Universidad Continental

FACULTAD DE DERECHO

Escuela Académico Profesional de Derecho

Tesis

Aplicación del Convenio de Budapest en la Ley de Delitos Informáticos del Perú, Cusco 2024

Ruth Stefanny Quincho Laura
Jose Fernando Aylas Dionicio
Joel Arcos Huayhua

Para optar el Título Profesional de Abogado

Cusco, 2025

Universidad Continental

INFORME DE CONFORMIDAD DE ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

A	:	Eliana Carmen Mory Arciniega. Decana de la Facultad de Derecho
DE	:	David Frank Molina Núñez. Asesor de trabajo de investigación
ASUNTO	:	Remito resultado de evaluación de originalidad de trabajo de investigación
FECHA	:	22 de mayo del 2025.

Con sumo agrado me dirijo a vuestro despacho para informar que, en mi condición de asesor del trabajo de investigación:

Título:
Aplicación del convenio de Budapest en la ley de delitos informáticos del Perú, Cusco 2024.

Autores:
1. Ruth Stefanny Quincho Laura – EAP. Derecho.
2. Jose Fernando Aylas Dionicio – EAP. Derecho.
3. Joel Arcos Huayhua – EAP. Derecho.

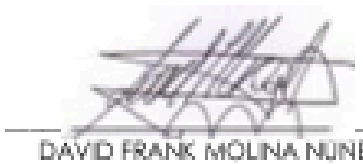
Se procedió con la carga del documento a la plataforma "Turnitin" y se realizó la verificación completa de las coincidencias resaltadas por el software dando por resultado 14 % de similitud sin encontrarse hallazgos relacionados a plagio. Se utilizaron los siguientes filtros:

- Filtro de exclusión de bibliografía — SI [X] NO [ ]
- Filtro de exclusión de grupos de palabras menores — SI [X] NO [ ]
  N° de palabras excluidas (20):
- Exclusión de fuente por trabajo anterior del mismo estudiante — SI [ ] NO [X]

En consecuencia, se determina que el trabajo de investigación constituye un documento original al presentar similitud de otros autores (citas) por debajo del porcentaje establecido por la Universidad Continental.

Recae toda responsabilidad del contenido del trabajo de investigación sobre el autor y asesor, en concordancia a los principios expresados en el Reglamento del Registro Nacional de Trabajos conducentes a Grados y Títulos – RENATI y en la normativa de la Universidad Continental.

Atentamente,



DAVID FRANK MOLINA NUÑEZ
Asesor de trabajo de investigación

AGRADECIMIENTO

Primero, a Dios, a nuestros padres, a todos quienes sacrificando un poco de su tiempo han permitido la realización de este esfuerzo colectivo.

DEDICATORIA

A quienes hicieron posible este logro.

A las familias, por ser los cimientos que sostienen cada uno de nuestros sueños, por su paciencia en los momentos de ausencia, y por celebrar con cada uno de nosotros los pequeños avances.

A nuestros compañeros de travesía académica, cómplices en noches de café y biblioteca, aliados en la decodificación de complejidades, testigos de esta metamorfosis intelectual.

A quienes lean estas líneas, que encuentren en estas páginas no solo conocimiento técnico, sino la huella de un esfuerzo mancomunado.

RESUMEN

La investigación se centró en comparar la aplicación del Convenio de Budapest y la Ley N° 30096 sobre delitos informáticos en Perú, con énfasis en los bienes jurídicos del patrimonio, fe pública, e indemnidad sexual en Cusco durante 2024, por tanto, el objetivo general de la investigación fue comparar la aplicación del convenio de Budapest con respecto a la ley de delitos informáticos del Perú para afrontar la ciberdelincuencia, Cusco 2024. La hipótesis planteada sugiere diferencias significativas entre ambos marcos normativos en cuanto a su alcance y efectividad. Metodológicamente, se empleó un enfoque mixto mediante cuestionarios dirigidos a expertos legales, y cualitativo a través de entrevistas semiestructuradas. La muestra incluyó a especialistas del Ministerio Público, la Policía Nacional del Perú y abogados penalistas de Cusco. Los instrumentos utilizados incluyeron encuestas para recoger datos estadísticos y entrevistas para obtener perspectivas interpretativas. Los resultados revelaron vacíos en la Ley N° 30096, como una limitada alineación con estándares internacionales y falta de herramientas procesales modernas. Por ejemplo, el fraude informático y la suplantación de identidad mostraron regulación insuficiente frente a las disposiciones del Convenio de Budapest. Asimismo, se identificó una implementación deficiente en áreas como la cooperación internacional y la preservación de pruebas digitales. Las conclusiones subrayan la necesidad de una reforma integral en la legislación peruana, priorizando la capacitación de operadores legales, la adopción de tecnologías avanzadas y el fortalecimiento de la cooperación transnacional. Además, se recomienda investigar más sobre las brechas específicas en la implementación del Convenio de Budapest para proponer estrategias concretas de mejora en el marco normativo nacional.

Palabras clave: Convenio de Budapest, delitos informáticos, Ley N° 30096, cooperación internacional, ciberdelincuencia, legislación peruana.

ABSTRACT

The research focused on comparing the application of the Budapest Convention and Law No. 30096 on cybercrime in Peru, with an emphasis on the legal rights of property, public faith, and sexual indemnity in Cusco during 2024. Therefore, the general objective of the research was to compare the application of the Budapest Convention with respect to the Peruvian cybercrime law to address cybercrime, Cusco 2024. The hypothesis posed suggests significant differences between both regulatory frameworks in terms of their scope and effectiveness. Methodologically, a mixed approach was used with quantitative analysis through questionnaires addressed to legal experts, and qualitative analysis through semi-structured interviews. The sample included specialists from the Public Prosecutor's Office, the National Police of Peru, and criminal lawyers from Cusco. The instruments used included surveys to collect statistical data and interviews to obtain interpretive perspectives. The results revealed gaps in Law No. 30096, such as limited alignment with international standards and a lack of modern procedural tools. For example, cyber fraud and identity theft were insufficiently regulated in light of the provisions of the Budapest Convention. Furthermore, deficient implementation was identified in areas such as international cooperation and the preservation of digital evidence. The findings underscore the need for comprehensive reform of Peruvian legislation, prioritizing the training of legal practitioners, the adoption of advanced technologies, and the strengthening of transnational cooperation. Furthermore, further research is recommended into specific gaps in the implementation of the Budapest Convention in order to propose concrete strategies for improving the national regulatory framework.

Keywords: Budapest Convention, computer crimes, Law No. 30096, international cooperation, cyber-delinquency, Peruvian legislation.

ÍNDICE DE CONTENIDO

AGRADECIMIENTO iv
DEDICATORIA v
RESUMEN vi
ABSTRACT viii
ÍNDICE DE CONTENIDO ix
ÍNDICE DE TABLAS xii
ÍNDICE DE FIGURAS xiii
INTRODUCCIÓN xv
CAPÍTULO I PLANTEAMIENTO DEL ESTUDIO 17
1.1. Planteamiento del Problema 17
1.2. Formulación del Problema 22
1.2.1. Problema general 22
1.2.2. Problemas específicos 22
1.3. Objetivos 23
1.3.1. Objetivo general 23
1.3.2. Objetivos específicos 23
1.4. Justificación e importancia 23
1.4.1. Justificación social 23
1.4.2. Teórica 25
1.4.3. Metodológica 26
1.5. Importancia de la Investigación 27
1.6. Limitaciones de la investigación 28
CAPÍTULO II MARCO TEÓRICO 30
2.1. Antecedentes de la Investigación 30
2.1.1. Antecedentes internacionales 30
2.1.2. Antecedentes nacionales 34
2.2. Bases Teóricas 42
2.2.1. Teorías de la delincuencia y el efecto tecnológico en el crimen 42
2.2.2. Tipificación de patrimonio, fe pública y la indemnidad e intangibilidad sexual en la actual legislación peruana 44
2.2.3. Delito informático 47

2.2.4. Tipos de delitos informáticos 48
2.2.5. Invasión de la privacidad y robo de identidad 48
2.2.6. Terrorismo cibernético 51
2.2.7. Pornografía infantil 52
2.2.8. Ciberacoso 52
2.2.9. La Convención de Budapest 53
2.2.10. Influencia del Convenio de Budapest en Perú 58
2.2.11. Marco común de derecho penal sustantivo 61
2.2.12. Estandarización de procesos penales 61
2.2.13. Cooperación Internacional 62
2.2.14. Dimensiones de la ciberdelincuencia 63
CAPÍTULO III HIPÓTESIS Y CATEGORÍAS 65
3.1. Hipótesis 65
3.1.1. Hipótesis general 65
3.1.2. Hipótesis específicas 65
3.1.3. Categorías de Estudio 66
CAPÍTULO IV METODOLOGÍA DEL ESTUDIO 67
4.1. Métodos, Tipo o Alcance de la Investigación 67
4.2. Diseño de Investigación 67
4.3. Población y Muestra de Estudio 68
4.3.1. Población 68
4.3.2. Muestra 68
4.3.2.1. Muestreo 68
4.3.2.2. Criterios de inclusión 68
4.3.2.3. Criterios de exclusión 69
4.4. Técnicas e Instrumentos de Recolección de Datos 69
4.5. Procedimiento para la Recolección de Datos 70
4.6. Técnicas de Análisis de Datos 70
4.7. Aspectos Éticos 70
CAPÍTULO V RESULTADOS 72
5.1. Análisis descriptivo 72
5.1.1. Objetivo general 72
5.1.2. Objetivo específico 1 74

5.1.3. Objetivo específico 2 84
5.1.4. Objetivo específico 3 93
CAPÍTULO VI DISCUSIÓN DE RESULTADOS 102
CONCLUSIONES 112
RECOMENDACIONES 115
REFERENCIAS BIBLIOGRAFICAS 117
ANEXOS 125
Anexo A. Matriz de Consistencia 125
Anexo B. Matriz de Operacionalización de Variables 128
Anexo C. Instrumentos 129
Anexo D. Declaración de Consentimiento Informado 132

ÍNDICE DE TABLAS

Tabla 1. Operacionalización de variables 66

ÍNDICE DE FIGURAS

Figura 1. ¿Considera usted que existen vacíos en la ley de delitos informáticos del Perú respecto al fraude informático? 79
Figura 2. ¿Considera usted que existen vacíos en el convenio de Budapest respecto al fraude informático? 80
Figura 3. ¿Considera usted que los policías y fiscales están totalmente preparados para combatir el fraude informático? 81
Figura 4. ¿Considera usted que es necesario capacitar en forma permanente a los policías y fiscales para combatir con mayor eficacia el fraude informático? 82
Figura 5. ¿Considera usted que existen vacíos en la ley de delitos informáticos del Perú, respecto a la suplantación de identidad? 88
Figura 6. ¿Considera usted que existen vacíos en el convenio de Budapest respecto a la suplantación de identidad? 89
Figura 7. ¿Considera usted que los policías y fiscales están totalmente preparados para combatir la suplantación de identidad? 90
Figura 8. ¿Considera usted que es necesario capacitar en forma permanente a los policías y fiscales para combatir con mayor eficacia la suplantación de identidad? 91
Figura 9. ¿Considera usted que existen vacíos en la ley de delitos informáticos del Perú, respecto a las proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos? 96
Figura 10. ¿Considera usted que existen vacíos en el convenio de Budapest respecto a las proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos? 97
Figura 11. ¿Considera usted que los policías y fiscales están totalmente preparados para combatir las proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos? 98
Figura 12. ¿Considera usted que es necesario capacitar en forma permanente a los policías y fiscales para combatir con mayor eficacia las proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos? 99

INTRODUCCIÓN

La ciberdelincuencia ha emergido como una de las principales amenazas de la era digital, abarcando una amplia gama de actividades ilegales que se cometen en línea. Desde el fraude informático hasta el terrorismo cibernético, estos delitos representan un desafío significativo para los sistemas legales y de seguridad a nivel mundial. En Perú, la Ley N° 30096 de Delitos Informáticos busca regular estas conductas delictivas, pero su alcance y efectividad han sido objeto de debate. Este panorama cobra mayor relevancia en un contexto global donde instrumentos como el Convenio de Budapest, que establece estándares internacionales para combatir el cibercrimen, han sido adoptados por numerosos países. En este marco, se evidencia la necesidad de analizar y comparar estas herramientas normativas para fortalecer la legislación peruana y enfrentar con mayor eficacia las complejidades de la ciberdelincuencia.

La presente investigación tiene como objetivo principal comparar la Ley N° 30096 con el Convenio de Budapest, evaluando su aplicación en tres bienes jurídicos protegidos: patrimonio, fe pública e indemnidad sexual. Desde una perspectiva teórica, se fundamenta en el análisis del derecho comparado y la criminología digital. Además, se sustenta en normativas internacionales y en la doctrina jurídica actual, buscando identificar vacíos legales y áreas de mejora en la legislación nacional para alinearla con estándares globales.

Metodológicamente, se utilizó un enfoque cualitativo. Se diseñaron cuestionarios dirigidos a expertos en derecho penal y ciberdelitos, complementados con entrevistas semiestructuradas. Este abordaje permitió contrastar la hipótesis general, que plantea diferencias significativas entre la Ley N° 30096 y el Convenio de Budapest, mediante análisis descriptivos y el razonamiento cualitativo basado en las

opiniones de los entrevistados. Los hallazgos resaltaron tanto coincidencias como discrepancias en la regulación de los ciberdelitos en ambos marcos normativos.

El trabajo se estructura en seis capítulos. El Capítulo I aborda el planteamiento del estudio, estableciendo el contexto y la problemática central. En el Capítulo II, se desarrolla el marco teórico, detallando conceptos clave como ciberdelincuencia y sus implicancias legales. El Capítulo III presenta las hipótesis y variables de la investigación. En el Capítulo IV, se describe la metodología empleada, mientras que el Capítulo V expone los resultados obtenidos, seguidos de conclusiones y recomendaciones en la última sección. Este enfoque integral busca contribuir al fortalecimiento del marco legal peruano frente a la ciberdelincuencia, promoviendo una mayor seguridad en el entorno digital.

CAPÍTULO I
PLANTEAMIENTO DEL ESTUDIO

I.1. Planteamiento del Problema

Dos cuestiones que no paran de aumentar en el tiempo son la tecnología y las manifestaciones de la delincuencia en todo tipo de modalidades, cualquiera que observe las manifestaciones actuales de la delincuencia no puede dejar de notar algunas de sus características peculiares, como su carácter indiscutiblemente global, su nivel de crecimiento sin precedentes y los constantes y rápidos avances tecnológicos asociados a ella (Statista, 2022). Debido a la variedad, omnipresencia y peligrosidad de los fenómenos delictivos que hoy amenazan nuestra seguridad, estamos asistiendo a una clara discontinuidad respecto a paradigmas anteriores de la amenaza. Por otro lado, la masiva utilización del internet, redes sociales e intercambio comercial sujeto a estas, han demostrado tener un ritmo de manejo similar o aún mayor que en el entorno físico. Hoy en día se puede hablar de cada cuestión y su símil en el entorno virtual que lo convierte en un mundo que conlleva sus beneficios y sus malestares (Coral Chalco, 2017; López, 2012; Miller et al., 2018).

Esta tendencia es claramente notoria en el manejo del internet en los últimos 30 años y han surgido una serie de incrementos dado los acontecimientos de cuarentena y la tendencia de jóvenes y adultos a hacer un uso muy alto de dispositivos móviles, así como sus efectos en la educación, salud (Amankwah-Amoah et al., 2021; Park et al., 2020; Quispe & Alecchi, 2021; Rodríguez & Sánchez, 2020) y como es usual, en el derecho, donde se han manifestado formas de sustituir de acciones que implican presencialidad como la visita de padres a hijos (Amick et al., 2022; Singer & Brodzinsky, 2020). No obstante, el avance del tiempo y de la tecnología no ha hecho más que hacer vulnerables a empresas que prestan servicios informáticos y a usuarios

que dando un click, pueden estar autorizando la usurpación, robo de información o robo monetario.

Es así como para el año 2016 en los Estados Unidos se tiene un valor de cerca de 2 mil millones de dólares en ciberdelincuencia, siendo este el primer delito reportado en la reguladora de telecomunicaciones de este país (Burnes et al., 2020). Del mismo modo se encuentran alrededor del mundo una serie de literatura que da cuenta de los problemas e implicancias de la cibercrimen, como por ejemplo, Europa Occidental y América del Norte (Davis, 2012; Wittes et al., 2016), pero también se tienen ejemplos en zonas donde el manejo de internet se asume limitado como Brasil (Booth, 2007) y países en África (Ibrahim, 2016), por lo que el tema del cibercrimen parece ser de tendencia global.

La ciberdelincuencia es un término colectivo que abarca una serie de actividades en línea depredadoras o perturbadoras, que incluyen: delitos de motivación económica, incluido el fraude (malware, ransomware, fraude de subastas en línea y correos electrónicos de phishing, por ejemplo), piratería, robo de identidad y distribución de pornografía ilegal y falsificación productos digitales, ciberterrorismo por motivos políticos y delitos por motivos psicológicos como la pornografía de venganza (Yar, 2019).

En el caso peruano, se han tenido una serie de esfuerzos académicos para poder establecer criterios para robustecer la ciberdelincuencia (o al menos parte de sus avances) en la ley de delitos informáticos (Congreso de la República del Perú, 2013). En este contexto se encuentran el delito de estafa básica (Vargas Miñan, 2022), el delito de phishing (Hidalgo Coronel & Solano Vidal, 2021; Sosa Umbo, 2022), así como esfuerzos por describir el problema desde el propio Ministerio de Justicia peruano (CONAPOC, 2020).

La llamada “gran aceleración” del COVID 19 para la digitalización (Amankwah-Amoah et al., 2021), también ha disparado en todo el mundo la ciberdelincuencia y cibercrimen, siendo que este proceso ha denotado la evidente debilidad de las leyes en el contexto informático. Es tan latente el problema que es conocido el caso de phishing de los bonos universales que el Estado Peruano otorgó durante la contingencia a esta pandemia (Sosa Umbo, 2022), demostrando que el gobierno como tal está muy rezagado y por ende, la población en general puede encontrarse expuesta a este tipo de delincuencia nueva con tan solo hacer un uso inadecuado de la computadora o de su celular.

Bajo lo expuesto, en la propuesta de la presente investigación se realizó un análisis comparativo entre los principales aspectos del cibercrimen entablados en la ley 30096, Ley de delitos informáticos, principal herramienta jurídica en el procesamiento de crímenes cibernéticos en la legislación peruana, pero que al no estar tipificado correctamente, el principio de legalidad los termina dirigiendo hacia modalidades más laxas de delitos, contribuyendo al clima de impunidad de los hechos delictivos. El problema radica en encontrar un cuerpo legal con el cual comparar la ley peruana, y este ejercicio se realizará con el convenio de Budapest, el cual es un documento supranacional que establece criterios clave para la ciberdelincuencia, pudiendo mejorar la legislación peruana en un ejercicio de derecho comparado. No obstante, este ejercicio implica el manejo de la literatura del derecho penal.

No obstante, este ejercicio implica el manejo de la literatura del derecho penal. Desde su promulgación hasta la actualidad la ley 30096 ha sufrido las siguientes modificatorias:

- Promulgación Original – 19 de agosto de 2013: La ley fue aprobada y promulgada en esta fecha, estableciendo el marco normativo para tipificar y sancionar delitos en el entorno digital.
- Primera Actualización Conceptual – 2015: En 2015 se introdujeron los primeros ajustes orientados a ampliar el espectro delictivo, incorporando nuevas conductas propias del entorno digital (como ciertas modalidades de fraude electrónico y suplantación de identidad) y modernizando definiciones tecnológicas. Estos cambios permitieron adecuar la norma a la rápida evolución del cibercrimen.
- Fortalecimiento de Sanciones y Procedimientos Probatorios – 2017: Durante 2017 se realizaron modificaciones que, además de endurecer las penas aplicables, incluyeron la actualización de los procedimientos de investigación y la admisión de evidencias digitales. Este cambio respondió a la necesidad de contar con herramientas legales que facilitasen la persecución penal de delitos cibernéticos en un contexto internacional.
- Ampliación en Protección de Datos y Delimitación del Catálogo Delictivo – 2019: A finales de 2019 se introdujeron cambios que vincularon de forma más directa la vulneración de datos personales con el ámbito de los delitos informáticos. Asimismo, se precisaron y ampliaron los tipos penales, incorporando delitos emergentes relacionados con el manejo indebido de información digital.
- Refuerzo en Cooperación Internacional y Actualización de Conceptos Tecnológicos – 2022: En 2022 se implementaron reformas destinadas a reforzar los mecanismos de cooperación transfronteriza en materia de

ciberseguridad, además de actualizar términos y definiciones para abarcar nuevas modalidades delictivas, tales como la ciber extorsión y el uso de tecnologías emergentes en actividades ilícitas.

Las modificaciones de la Ley 30096 han estado influenciadas por el Convenio de Budapest, ya que este instrumento internacional ha servido de referencia para armonizar la legislación en materia de delitos informáticos a nivel global. Por ejemplo, en las actualizaciones de 2015 y 2017, se observaron ajustes en las definiciones y procedimientos probatorios que reflejan las prácticas recomendadas por el Convenio, en cuanto a la adopción de herramientas para la investigación y el manejo de evidencias digitales. Además, las reformas de 2019 y 2022 fortalecieron la protección de datos y la cooperación internacional, elementos esenciales del Convenio de Budapest, que promueve el intercambio de información y la colaboración transfronteriza para combatir el cibercrimen. Estas adaptaciones responden a la necesidad de que la normativa nacional se mantenga actualizada frente a las dinámicas tecnológicas y delictivas, garantizando que el marco legal peruano esté en sintonía con los estándares internacionales en la lucha contra el delito informático.

Es así como, se propone en la presente investigación el elaborar una encuesta con especialistas en ciberdelincuencia que trabajen en instituciones como la Policía Nacional del Perú (PNP) y el Ministerio Público (MP) y abogados penalistas que conozcan de ciberdelitos de la ciudad de Cusco para realizar un análisis del derecho peruano con el convenio de Budapest en tres bienes jurídicos protegidos: el patrimonio, la fe pública y la intangibilidad sexual, en los delitos como el fraude informático, suplantación de identidad y proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos , en observancia al convenio de Budapest como instrumento legal para detallar la presencia o ausencia de aspectos importantes

en la ley de delitos informáticos en el Perú y específicamente en la ciudad del Cusco. A continuación, se establece la problemática que da pie a la investigación.

I.2. Formulación del Problema

I.2.1. Problema general

¿Se ha evidenciado la aplicación del convenio de Budapest con respecto a la ley de delitos informáticos del Perú, Cusco 2024?

I.2.2. Problemas específicos

- ¿Cuál ha sido el impacto de la implementación del convenio de Budapest con respecto a la ley de delitos informáticos del Perú 30096, con enfoque en el bien jurídico del patrimonio en el delito de fraude informático, Cusco 2024?
- ¿En qué medida se ha evidenciado la influencia del convenio de Budapest sobre la norma 30096, respecto del bien jurídico de la fe pública en el delito de suplantación de identidad, Cusco 2024?
- ¿Cómo se ha aplicado el convenio de Budapest con respecto a la ley de delitos informáticos del Perú, sobre el bien jurídico de la indemnidad e intangibilidad sexual en el delito de proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, Cusco 2024?

I.3. Objetivos

I.3.1. Objetivo general

Contrastar la aplicación del convenio de Budapest con respecto a la ley de delitos informáticos del Perú para afrontar la ciberdelincuencia, Cusco 2024.

I.3.2. Objetivos específicos

- Diagnosticar cómo se ha aplicado el convenio de Budapest con respecto a la ley de delitos informáticos del Perú, sobre el bien jurídico del patrimonio en el delito de fraude informático, Cusco 2024.
- Delimitar la influencia de la aplicación el convenio de Budapest con respecto a la ley de delitos informáticos del Perú, sobre el bien jurídico de la fe pública en el delito de suplantación de identidad, Cusco 2024.
- Establecer el impacto sobre la aplicación del convenio de Budapest con respecto a la ley de delitos informáticos del Perú, sobre el bien jurídico de la intangibilidad sexual en el delito de proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, Cusco 2024.

I.4. Justificación e importancia

I.4.1. Justificación social

En el ámbito social, la actualización de la ley que regula los delitos informáticos resulta una necesidad prioritaria para garantizar la seguridad de la población en el entorno virtual. En un contexto donde el avance tecnológico ha transformado casi todos los aspectos de la vida cotidiana, desde las relaciones interpersonales hasta las actividades económicas, cualquier debilidad en las normativas legales pone en peligro no solo a los individuos, sino también a las organizaciones y al propio Estado. El crecimiento exponencial de las interacciones virtuales, como el comercio electrónico,

la educación a distancia, las transacciones financieras y la comunicación digital, ha generado un entorno altamente vulnerable a actividades ilícitas como el fraude, el robo de identidad y la suplantación de datos personales. Estas amenazas, si no se enfrentan con herramientas legales adecuadas, pueden erosionar la confianza en los sistemas digitales y desincentivar su uso, afectando el desarrollo social y económico.

La existencia de leyes claras, modernas y efectivas en el ámbito de la ciberdelincuencia permite crear un entorno virtual seguro donde los ciudadanos pueden realizar sus actividades cotidianas con tranquilidad. Según Yar (2019), el marco normativo no solo debe centrarse en sancionar a los infractores, sino también en prevenir la ocurrencia de delitos mediante la implementación de medidas de protección adecuadas y la promoción de una cultura de ciberseguridad. Este enfoque no solo protege los derechos individuales, como el acceso a la privacidad y la seguridad de los datos, sino que también fomenta la estabilidad en las relaciones sociales y la confianza en las plataformas digitales.

Además, el impacto de una normativa desactualizada o insuficiente es particularmente grave en contextos donde la brecha tecnológica ya coloca a ciertos sectores en una situación de desventaja. La falta de regulación efectiva incrementa la exposición de los usuarios más vulnerables, como niños, adolescentes y personas mayores, a delitos como la explotación sexual, el ciberacoso y las estafas en línea. Por ello, el fortalecimiento de las leyes que regulan el entorno digital debe ir acompañado de campañas educativas y de concienciación que permitan a los usuarios identificar riesgos y adoptar medidas de autoprotección.

I.4.2. Teórica

Desde una perspectiva teórica, el derecho avanza a un ritmo considerablemente más lento que la tecnología, generando brechas normativas que pueden afectar

gravemente los derechos fundamentales de las personas. Los avances tecnológicos, al transformar las formas en que se desarrollan las interacciones sociales, económicas y culturales, han dado lugar a situaciones que no están adecuadamente reguladas en los marcos jurídicos tradicionales. Esta desincronización crea vacíos legales que son aprovechados por actores malintencionados para cometer delitos, tales como fraudes electrónicos, suplantaciones de identidad y otras formas de ciberdelincuencia. Vargas Miñan (2022) señala que este fenómeno plantea un desafío crítico para los sistemas legales, que deben adaptarse constantemente a un panorama cambiante para garantizar la protección de los derechos individuales y colectivos. En este contexto, la falta de legislación adecuada no solo dificulta la sanción de conductas ilícitas, sino que también pone en entredicho la capacidad de los Estados para ofrecer garantías de seguridad en un entorno digital cada vez más complejo. Los vacíos legales, que se originan en la incapacidad del derecho para anticiparse a las implicancias de las innovaciones tecnológicas, generan una sensación de incertidumbre jurídica que afecta tanto a los ciudadanos como a las empresas. Esta situación obliga a los sistemas legales a realizar esfuerzos significativos para cerrar dichas brechas, adoptando medidas que incluyan la actualización de normativas, la creación de leyes específicas y el fortalecimiento de mecanismos internacionales de cooperación jurídica. Asimismo, la armonización de las legislaciones a nivel internacional, como la promovida por instrumentos como el Convenio de Budapest, resulta esencial para enfrentar fenómenos transnacionales como la ciberdelincuencia.

I.4.3. Metodológica

La justificación metodológica de esta investigación radica en la combinación de técnicas estadísticas descriptivas y argumentos cualitativos, lo que permitió abordar la complejidad del tema desde una perspectiva integral y multidimensional. Las

estadísticas descriptivas se utilizaron para analizar y sintetizar los datos recopilados, permitiendo identificar patrones, tendencias y características principales relacionadas con la aplicación de la Ley N° 30096 y el Convenio de Budapest en el contexto de los ciberdelitos. Este enfoque estadístico proporcionó una base objetiva y clara para interpretar los aspectos medibles de las variables estudiadas, facilitando la comparación de indicadores y la evaluación de las diferencias entre los marcos normativos.

Por otro lado, los argumentos cualitativos complementaron el análisis numérico al permitir una comprensión más profunda y detallada de los aspectos normativos, sociales y legales involucrados. Mediante entrevistas semiestructuradas con expertos en derecho penal y ciberdelincuencia, se recogieron opiniones fundamentadas que aportaron un enfoque interpretativo al estudio. Estas perspectivas cualitativas enriquecieron el análisis al capturar matices y contextos que no podrían ser representados únicamente mediante datos estadísticos, proporcionando así una visión más completa de la problemática.

La combinación de estos enfoques metodológicos se justificó por la necesidad de contrastar la hipótesis general desde diferentes dimensiones: la estadística, que permitió encontrar diferencias significativas, y la cualitativa, que ofreció argumentos sólidos para contextualizar y sustentar los hallazgos. Este enfoque mixto garantizó la validez interna y externa de los resultados, al integrar datos objetivos y subjetivos que fortalecieron la interpretación y las conclusiones del estudio.

I.5. Importancia de la Investigación

La importancia de esta investigación radica en abordar un problema de creciente relevancia y complejidad en la era digital: la ciberdelincuencia y su regulación mediante marcos legales nacionales e internacionales. La tecnología y sus avances

constantes han transformado profundamente las dinámicas sociales y económicas, creando oportunidades y, a la vez, riesgos que afectan tanto a individuos como a instituciones. Como se plantea en la problemática, el carácter global y el rápido crecimiento de los delitos cibernéticos, combinados con la masificación del uso de internet y dispositivos móviles, generan un entorno propicio para actividades ilícitas como el fraude, la suplantación de identidad y la explotación sexual en línea. Estos fenómenos, si no se enfrentan con una legislación adecuada, perpetúan la inseguridad y la impunidad en el entorno digital.

El contexto peruano refleja estas vulnerabilidades. Aunque la Ley N° 30096 constituye un avance importante para regular los delitos informáticos, presenta vacíos legales que limitan su efectividad. Comparar esta normativa con el Convenio de Budapest, un instrumento internacional ampliamente reconocido, resulta crucial para identificar las áreas en las que la legislación peruana puede fortalecerse. Este análisis busca contribuir a la creación de un marco legal más robusto, que no solo sancione las conductas ilícitas, sino que también promueva la prevención y la protección de los derechos fundamentales en el entorno virtual.

Desde un enfoque metodológico, esta investigación combina técnicas cualitativas para proporcionar un análisis integral. El uso de estadísticas descriptivas permitió identificar tendencias y evaluar la efectividad de las normativas en cuestión, mientras que las entrevistas a expertos en derecho penal y ciberdelincuencia aportaron una perspectiva cualitativa enriquecedora. Este enfoque mixto asegura una comprensión más profunda de las implicancias normativas y sociales de los ciberdelitos, estableciendo bases sólidas para recomendaciones futuras.

En síntesis, la importancia de esta investigación radica en su capacidad para abordar una problemática de impacto global y local, contribuyendo al fortalecimiento

del marco legal peruano frente a los desafíos de la ciberdelincuencia. Esto no solo tiene implicancias directas en la seguridad y bienestar de los ciudadanos, sino que también fomenta la confianza en las instituciones y el desarrollo sostenible en un mundo cada vez más digitalizado.

I.6. Limitaciones de la investigación

Las limitaciones de esta investigación pueden clasificarse en tres categorías principales: económicas, contextuales y metodológicas. Desde el punto de vista económico, la investigación requirió recursos significativos para su implementación, tales como la organización de entrevistas con expertos, el acceso a bases de datos especializadas y la adquisición de literatura jurídica y estadística relevante. La carencia de financiamiento externo y el manejo de un presupuesto restringido limitaron la posibilidad de ampliar la muestra de participantes o realizar comparaciones internacionales más detalladas, lo que podría haber fortalecido los resultados obtenidos.

En el ámbito contextual, uno de los principales desafíos fue la dependencia de las opiniones de expertos, como fiscales, abogados penalistas y oficiales especializados en ciberdelincuencia. Aunque su perspectiva aporta un alto valor cualitativo, esta subjetividad puede influir en los hallazgos, ya que sus opiniones podrían estar condicionadas por sus experiencias individuales o el entorno en el que operan. Además, la concentración del estudio en Cusco puede limitar la generalización de los resultados a otras regiones del país con dinámicas diferentes en términos de legislación y aplicación de normativas.

Finalmente, desde un enfoque metodológico, el diseño mixto presenta retos inherentes. Por ejemplo, la integración de datos estadísticos con argumentos cualitativos requiere un alto nivel de consistencia en el análisis para evitar

interpretaciones sesgadas. Asimismo, las limitaciones en la disponibilidad de datos oficiales y actualizados sobre delitos informáticos en Perú restringieron la posibilidad de realizar análisis más robustos y comparaciones más amplias entre el Convenio de Budapest y la Ley N° 30096. Estas limitaciones subrayan la necesidad de futuras investigaciones que amplíen el alcance y profundidad del análisis en este campo.

CAPÍTULO II
MARCO TEÓRICO

II.1. Antecedentes de la Investigación

II.1.1. Antecedentes internacionales

a.) Spiezia (2022) realizó una investigación que lleva por título: “International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime”. El tema de las víctimas del ciberdelito se aborda aquí en el contexto de un análisis fundamental de las formas modernas de delincuencia transfronteriza. En el marco descrito, la cooperación judicial internacional sigue siendo, una vez más, un concepto clave en la implementación de estrategias efectivas y exitosas, también con miras a garantizar una mejor protección de quienes son víctimas de estas formas de delitos. La implementación del nuevo Protocolo, adoptado en 2021, del Convenio de Budapest de 2001 podría proporcionar un poderoso estímulo, cuyo innovador marco regulatorio también podría influir positivamente en el funcionamiento de las agencias europeas involucradas desde hace mucho tiempo en el sector, como Eurojust y Europol, en sus actividades de apoyo a las autoridades nacionales. Sus principales conclusiones son las de detallar que en efecto, el convenio de Budapest es un cuerpo jurídico que puede potencialmente mejorar la lucha contra la delincuencia en el marco del ciberespacio, siendo el inicio de un esfuerzo hacia un nuevo sistema de justicia criminal en los lugares donde se implemente.

b.) Campina y Rodrigues (2022) realizaron la investigación: “Cybercrime and the Council of Europe Budapes Convention: prevention, criminalization, and International Cooperation”. Describen que el Convenio de Budapest sobre Ciberdelincuencia prevé la tipificación como delito de la conducta; las facultades

procesales para la investigación penal; y la Cooperación Internacional como una de las más eficientes y policiales para prevenir y combatir el Cibercrimen. Los 77 Estados Participantes estrechan el trabajo con los Estados Observadores, dentro de la estrategia de Cooperación Internacional, en conexión con Gobiernos, autoridades policiales (nacionales e internacionales), Organismos e Instituciones Internacionales ha sido la (re)acción estratégica más rentable, impulsando la posición de cooperación a los retos emergentes, aunque el cibercrimen es uno de los más difíciles de afrontar. Entonces, hay una evolución en los instrumentos y estrategias para prevenir y combatir el Ciberdelito, pero urge una (re)solución legal y social efectiva, de lo contrario habrá impactos irreversibles en el mundo y en la humanidad. Finalmente, a partir de los desafíos de la ley y el delito cibernético, la estrategia se confirma en gran medida por la cooperación: el intercambio de a) información dentro de los marcos legales; b) la respuesta: operativa o táctica; c) las obras en la Darkweb; los movimientos del mercado, financieros y económicos frente al ciberdelito o para denunciar a los ciberdelincuentes; d) transparencia para prevenir la evolución e implementación del ciberdelito. Como conclusión se detalla que a partir de los desafíos de la ley y el delito cibernético, la estrategia se confirma en gran medida por la cooperación: el intercambio de información dentro de los marcos legales; la respuesta operativa o táctica; las obras en la Darkweb; los movimientos del mercado, financieros y económicos frente al ciberdelito o para denunciar a los ciberdelincuentes y la transparencia para prevenir la evolución e implementación del ciberdelito. Siendo estos alcances, un buen inicio para el procesamiento de cualquier delito que se encuentre en el entorno virtual.

c.) Nguyen, Truong y Lai (2022) realizaron la investigación: “Legal challenges to combating cybercrime: An approach from Vietnam”. Este documento explora los

desafíos legales de combatir el delito cibernético en Vietnam. Utilizamos un método de doctrina legal para revisar los marcos legales vietnamitas actualizados, que consisten en leyes sustantivas, procesales y preventivas sobre delitos cibernéticos. Luego combinamos el análisis de cuatro casos de delitos cibernéticos y entrevistas en profundidad de siete altos funcionarios policiales para analizar la aplicación de la ley de delitos cibernéticos. Los principales hallazgos revelan que, al actualizar su sistema legal, Vietnam ha mostrado una determinación para prevenir e interrumpir el delito cibernético. A pesar de los resultados positivos, la lucha de Vietnam contra el ciberdelito aún enfrenta desafíos legales, incluidos los tradicionales y los novedosos. Además, los enfoques activos y flexibles dentro de la gestión del ciberespacio de Vietnam pueden aumentar la eficacia de la lucha contra las actividades delictivas cibernéticas; sin embargo, pueden generar inquietudes a la hora de equilibrar el control del delito cibernético y la protección de los derechos humanos. Estos enfoques podrían entonces constituir un caso de estudio útil para otras situaciones similares.

d.) Elizalde, Flores y Castro (2021) realizaron una investigación titulada: “Los delitos cibernéticos en Chile, México y Colombia. Un estudio de Derecho Comparado”. El objetivo de este artículo fue investigar y analizar los delitos cibernéticos vigentes en Chile, México y Colombia, con el fin, primero, de estudiar sus ordenamientos jurídicos tendientes a regular estas nuevas formas delictivas; segundo, conocer cuáles son las semejanzas y diferencias que guardan los delitos cibernéticos en esos tres países; y, por último, determinar si en los inicios de la tercera década del siglo XXI, los tres países han adecuado su marco constitucional y legal a los términos establecidos en el Convenio sobre la Ciberdelincuencia 2001, celebrado en Budapest. Como conclusión, el estudio examinó la regulación de delitos cibernéticos en Chile, México y Colombia, analizando sus marcos constitucionales y

legales. Se compararon los avances de cada país, tomando como referencia los compromisos del Convenio de Budapest sobre ciberdelincuencia. Aunque los tres han progresado en la materia, Chile y México aún no han realizado las adecuaciones necesarias. Chile conformó una Comisión Mixta en octubre de 2021 para modernizar su legislación, y México no se ha adherido al convenio. Colombia ha incorporado algunos lineamientos desde 2009 y el convenio entró en vigor en julio de 2020, mostrando un avance parcial, además.

e.) Ortiz (2019) realizó la investigación de título: "Normativa Legal sobre Delitos Informáticos en Ecuador". El objetivo de la investigación es describir el avance tecnológico y la creciente accesibilidad al Internet que tienen las personas en todo el mundo ha sido de utilidad para la masificación en la creación y utilización de diferentes sitios web y APP (aplicaciones). Estas están diseñadas para satisfacer las necesidades de sus usuarios a través de dar tan solo un click; las necesidades suelen ser variadas, desde hacer transacciones bancarias complejas a nivel internacional a simplemente chatear con otra persona en un lugar remoto del planeta. Sin duda alguna, el uso de Internet facilita la vida de los usuarios, pero esos beneficios se tornan peligrosos cuando se infiltran entre los servicios del Internet programas maliciosos que de forma silenciosa pueden dañar no sólo los equipos tecnológicos sino también las finanzas de las personas, empresas y gobiernos. Los programas maliciosos son insertados en los sitios web o APP por delincuentes informáticos que han hecho de las Tecnologías de la Información y Comunicación (TIC) su nueva herramienta para cometer sus actos ilícitos. Cuáles son los tipos de delitos que se generan en la red, qué leyes existen para sancionar los delitos informáticos y cuáles son los problemas para combatir el mismo fueron las interrogantes que motivaron a desarrollar la presente revisión bibliográfica. Al concluir el trabajo pudo determinar

que existen dificultades para combatir los delitos informáticos por la transnacionalidad de los mismos y la incompatibilidad de las leyes a nivel mundial; considerando que en algunos países no existen Leyes para combatir los delitos informáticos y que son millonarias las pérdidas ocasionadas por este tipo de delitos.

f.) Sanmartin (2021) realizó una investigación acerca de: "Los delitos informáticos en el Código Orgánico Integral Penal y el Convenio Internacional de Budapest". Trabajo de investigación aborda el tema de los delitos informáticos en el Código Orgánico Integral Penal y el Convenio Internacional de Budapest, debido a que el Ecuador no se ha adherido al principal instrumento internacional sobre ciberdelincuencia que le permita tener una legislación completa y adecuada para mitigar los ataques de la cibercriminalidad. La investigación tuvo como propósito determinar las principales aportaciones que brindaría la adhesión al Convenio de Budapest en la regulación de delitos informáticos en el Ecuador. El desarrollo de la perspectiva teórica se sustenta en la revisión de documentación teórica y académica. El análisis se llevó a cabo mediante una metodología con enfoque cualitativo, de alcance descriptivo a través del método histórico, analítico y comparativo; asimismo, se realizó entrevistas a profesionales del derecho especializados en derecho informático, lo cual, permitió construir criterios a cerca de la factibilidad que presentaría la adhesión de Ecuador al Convenio de Budapest, llegando a la conclusión de que los principales aportes son: el catálogo de delitos, las normas procesales de investigación y las normas de cooperación internacional que permitirán concretar una política penal similar y armonizar la cooperación internacional entre los países que han ratificado el Convenio de Budapest.

II.1.2. Antecedentes nacionales

Huaman (2020) realizó una investigación denominada: “Los delitos informáticos en Perú y la suscripción del Convenio de Budapest”, que fue realizada a partir de observar una realidad en la que los delitos informáticos van tomando mayor presencia y de conocer la postura que asume nuestro Estado para hacer frente a estos delitos; una de ellas es la suscripción del Convenio de Budapest o Convenio de Ciberdelincuencia y lo que se analiza, es la manera en que la suscripción del mencionado convenio influye en el tratamiento de los delitos informáticos, que lleva a plantear las siguientes interrogantes: ¿De qué manera la suscripción del convenio de Budapest influye en el tratamiento de los delitos informáticos? como pregunta general, y como preguntas específicas, ¿Cuál es el desarrollo legislativo de los delitos informáticos en el Perú? ¿Cuál es la problemática actual generada por los delitos informáticos en el Perú? ¿Cómo es la legislación de delitos informáticos en países sudamericanos que suscribieron el convenio de Budapest? ¿Cuáles son los efectos que produce la suscripción del convenio de Budapest?, cada una de ellas con sus respectivos objetivos. En el Marco teórico, se pone especial énfasis en el desarrollo de nuestras categorías de estudio, siendo la primera categoría “Los Delitos Informáticos” y la segunda categoría “El Convenio de Budapest”. En el diseño metodológico se ha considerado: El enfoque de investigación cualitativo, por cuanto se orienta a la revisión y obtención de datos de carácter teórico y legislativo antes que a la obtención de datos estadísticos; como tipo de investigación: Descriptiva Jurídica y Comparativa; y el nivel de investigación: Investigación básica, al estar orientada a la revisión de conocimientos teóricos que se verán ampliados. Así como técnicas e instrumentos que han permitido obtener información doctrinaria, legislativa y de casos. Todo ello ha permitido arribar a las siguientes conclusiones: PRIMERA: La suscripción del Convenio de Budapest, influye de manera relativa en el tratamiento de los delitos

informáticos, al centrarse en la adecuación de nuestra normatividad a la prevista en el mencionado Convenio, como es establecer un catálogo de delitos, establecer normas procesales orientadas a salvaguardar las evidencias digitales y recurrir a la cooperación internacional para investigar la comisión de este tipo de delitos; y la principal característica que es la cooperación internacional para investigar casos trascedentes ha tenido mínima aplicación desde su suscripción. SEGUNDA: El desarrollo legislativo de los delitos informáticos en el Perú ha sido progresivo y rápido en un periodo de 30 años que comienza en 1991 con la tipificación de estos delitos en el artículo 207 del Código Penal, pero, sobre todo desde el año 2013 con la promulgación de la ley 30096 y las modificaciones realizadas en con la Ley 30171, hasta la suscripción del Convenio en mención, permitiendo contar en la actualidad con legislación equiparable a la legislación comparada de delitos informático. TERCERA: La problemática actual causada por la comisión de delitos informáticos en el Perú es creciente; obedece al acceso y uso de diversos y novedosos medios tecnológicos por parte de los ciberdelincuentes, situación que hace difícil su identificación y ubicación. En América Latina en el año 2017 el Perú ha sido el más afectado con los programas ransomware con un 25.1% del total de casos presentado; para el 2019, nuestro país era el tercer país en América latina más afectados con programas Spyware; el mismo años se presentaron 3012 denuncias por fraude informático y 247 denuncias sobre suplantación de identidad en la Divindat); se suma a ello, el escaso presupuesto destinado a contar con tecnología de alta gama para la persecución de este tipo de delitos. CUARTA: La legislación sobre delitos informáticos de países sudamericanos que suscribieron el convenio de Budapest es uniforme y permite una integración generada a partir de la cooperación internacional promovida por dicho Convenio. QUINTA: Los efectos de suscribir el Convenio de

Budapest, son positivos a nivel legislativo, porque permite contar con un catálogo integral de delitos informáticos, sin embargo, se requieren de políticas orientadas a destinar recursos económicos para el equipamiento de la tecnología informativa que permita hacer frente a los delitos informáticos.

Alatrista y Magariño (2021) realizaron la investigación: "Ciberbullying: análisis de su regulación normativa en el marco de los derechos fundamentales de los menores de edad". Investigación que tuvo como objetivo principal, determinar si el cyberbullying vulnera los derechos fundamentales de los menores de edad en cuanto al honor, la buena reputación y la intimidad personal. Se revisó el ordenamiento jurídico nacional en búsqueda de aquellas normas de protección al menor y cuáles han sido los avances legislativos en este tema, revisamos y analizamos las diferencias y similitudes de otros ordenamientos jurídicos internacionales con el fin de promover y hallar mejores soluciones a la legislación nacional, usando la metodología de análisis documental, que permitió recoger conceptos, doctrinas, normativas y jurisprudencia nacional e internacional con la finalidad de conocer y analizar nuevas informaciones. El resultado final se enfoca en promover una alerta de urgencia a nuestras autoridades y sociedad en general para que puedan tomar conciencia sobre este fenómeno ya tipificado como delito por otros ordenamientos jurídicos, y de esa manera proteger a los menores de edad contra el ciberbullying. Finalmente se concluyó la investigación verificando que existe una falta de normativa única y expresa y en igual manera una falta de interés de parte de los legisladores en legislar una normativa acorde al tiempo y necesidad para afrontar, prevenir y detener este grave problema y no quedarse a lamentar fatales desenlaces como simples observadores.

Pereyra y Turpo (2020) realizaron la investigación: "Instrumentos normativos que se deben adecuar en nuestra legislación según el marco del Convenio de Budapest

como mecanismo legal de protección a la intimidad personal frente a las TICS". El trabajo de investigación se basa en un análisis jurídico de resultados sobre la adecuación de ciertas normas del Convenio de Budapest, en la normativa vigente en Perú, respecto del Derecho de protección a la intimidad personal frente a la utilización de las tecnologías de la comunicación social, en adelante TICs, debido a la reciente adhesión de nuestro país al mencionado Convenio FEB2019. El objetivo general será determinar si la adecuación de los instrumentos normativos de nuestra legislación según el marco del Convenio de Budapest, resultarían eficaces. En cuanto a los objetivos específicos se analizará la relación que existe entre la normativa legal de Protección a la intimidad personal vigente en el Perú y el Convenio de Budapest y la identificación de los efectos de la modificación de nuestra legislación en la adecuación al marco legal del Convenio de Budapest, ello, como mecanismo legal de protección a la intimidad personal frente a las TICs. Dicha investigación se sustenta en una metodología mixta con preponderancia cualitativa, realizada mediante cálculos estadísticos de información obtenida en el campo, «data cruda», en cuanto a las variables de estudio y los resultados, ello, coadyuvaran a determinar las conclusiones del presente trabajo, al cual se integrará investigaciones académicas, manuscritos, información de libros, documentos virtuales, doctrina, jurisprudencia, y el aporte sustancial de los especialistas entrevistados en la materia. Entre sus principales conclusiones se tiene que la protección a la intimidad personal en el Perú, debido al avance de las TICs, ha sido últimamente vulnerada de diferentes modalidades (nuevas conductas delictuales), ello, necesita ser protegido eficazmente mediante mecanismos legales adecuados en nuestra legislación, a fin de reducir en lo posible las estadísticas de denuncias contra este derecho fundamental de toda persona.

Villareal (2020) realizó la investigación: “Innovaciones en la tipificación de delitos con la ratificación del convenio contra el cibercrimen, en el Perú el año 2019”. Dicha investigación tuvo como objetivo determinar las modificaciones en la tipificación de delitos que incorpora el Convenio contra el cibercrimen de Budapest en Perú el año 2019. El tipo de estudio fue Básica Descriptiva; el Diseño No experimental, descriptivo, correlacional, transversal. Método: La población es finita, al estar compuesta por el estudio de la tipificación de delitos por medios informáticos en tres documentos legales que son el Convenio contra el Cibercrimen de Budapest, la Ley de Delitos Informáticos y el Código Penal. La muestra corresponde al 100% de la población, centrando el estudio en los aspectos pertinentes de los tres dispositivos legales antes enunciados. Resultados: Se ha podido determinar que el Convenio contra el cibercrimen de Budapest, ratificado por el Perú el año 2019, existe un 57.14% de coincidencia, haciendo necesario modificar su tipificación del Art 4° de la Ley de Delitos Informáticos, pues la misma no incluye la totalidad de elementos objetivos que propone la Convención y respecto al delito de Falsificación Informática, hallamos un 0% de coincidencia, haciendo necesario implementar su regulación debido a que no se encuentra tipificado ni en el Código Penal ni en la Ley de Delitos Informáticos. Conclusión: Finalmente se ha podido verificar que es necesario la modificación del Art 4° “Atentado contra la integridad de sistemas informáticos” y la incorporación del delito informático de Falsificación Informática en el Capítulo referido a delitos contra la fe pública en la Ley N°30096 Ley de Delitos Informáticos.

Vitteri (2022) realizo la investigación: “Mecanismos jurídicos para implementar la Ley 30096 en los Delitos Informáticos contra el patrimonio frente a las nuevas Tecnologías Informáticas”, investigación que tuvo como finalidad determinar los mecanismos jurídicos para implementar en la Ley No 30096 de delitos informáticos

contra el patrimonio frente a las nuevas modalidades que existen hoy en día. Como fuente principal la creación de una fiscalía especializada en este delito, así también, en las demás modalidades que existen en nuestro ordenamiento y las que van surgiendo día a día, toda vez que genera una inseguridad jurídica en nuestra justicia y de tal modo que es ineficaz para poder demostrar la autoría o participación en una etapa preliminar, por lo que no se logra una efectiva sanción en este tipo penal. En esta investigación se logró efectuar y aplicar el método inductivo, porque propondremos nuevos instrumentos necesarios para combatir la ciberdelincuencia que ocurre en este momento con mayor frecuencia. Así mismo esta investigación busca como objetivo general determinar los mecanismos jurídicos para implementar la Ley N° 30096 de Delitos informáticos contra el patrimonio frente a las nuevas tecnologías informáticas. Con esta investigación se propone la creación de una fiscalía especializada en delitos informáticos para combatir la ciberdelincuencia que viene evolucionando de una manera constante en nuestra sociedad y en el mundo

Fuentes (2021) realizó la investigación: “Modificación de la ley 30096 para incorporar los delitos de phishing, pharming y carding como delitos penalizables con prisión, para reducir la ciberdelincuencia, Lima 2019”. Investigación que tuvo como objetivo principal justificar por qué los delitos de Phishing, Pharming y Carding deben ser incorporados a la Ley N°30096 como delitos penalizables con penas privativas de la libertad, para ello debe tenerse en consideración que investigar el delito desde cualquier ámbito es hoy en día una actividad muy compleja. Actualmente el auge de la cibercriminalidad va en aumento, generando los llamados delitos informáticos ya que para su consumación se requiere emplear medios electrónicos, ejemplo de estos delitos son: el hacking, propaganda maliciosa de un virus, pornografía infantil y agresión a proveedores de Internet son los delitos informáticos

más y más comunes en nuestro país. Por ello, el Parlamento Peruano promulgó la Ley N°30096, denominada Ley de Delitos Informáticos, modificada posteriormente por la Ley N°30171, la misma que describe que, con tan solo tener acceso a Internet, muchos de los usuarios están expuestos a una cadena de delitos que se cometen incorporando las nuevas tecnologías y avances digitales, según la ley violando la confidencialidad, integridad y la información; asimismo, la citada norma incorporó una serie de delitos informáticos, dentro de los que se encuentran interceptación de información, suplantación de identidad, entre otros, a estos tipos penales se les establecieron sanciones penales con la finalidad de contrarrestar su consumación, razón por la cual es imprescindible que también se incorporen a esta gama de delitos las modalidades delictivas de Phishing, Pharming y Carding como delitos penalizables con prisión, a fin de reducir la ciberdelincuencia en la ley N°30096.

Ayma (2020) realizó la investigación: “Delitos informáticos y su relación con el proceso de investigación preliminar en el distrito fiscal de Lima norte año 2019”. Tuvo como finalidad examinar los datos bibliográficos y los datos estadísticos, respecto a los delitos informáticos, en tal sentido, los resultados obtenidos al respecto dan cuenta, que en el ministerio público de cono norte, viene aplicando de manera incorrecta la norma jurídica respecto al delito informático, dañando de esta manera los derechos fundamentales de personas procesadas, en algunos casos del estado. La informática es imperiosa para desarrollar las organizaciones dentro de la sociedad, en tal sentido es importante ponderar su uso correcto, para no afectar los derechos individuales y colectivos. En sus conclusiones se evidencian que las autoridades deben capacitar a los operadores del ministerio público en la valoración correcta de las pruebas, con evaluaciones precisas para no cometer excesos ni omitir los datos de sistemas informáticos, sobre todo de aquellas que han sido obtenidos de manera

ilegal, cuya valoración será evaluada excepcionalmente por el organismo competente. Finalmente se concluye que las evidencias dan cuenta que los procedimientos jurídicos referido al tratamiento penal, respecto delitos informáticos para preservar los bienes patrimoniales del estado, son deficientes. El cual genera desorden, porque al no aplicar la norma correctamente sobre el delito informático, se comete omisión en desmedro del estado. Las fiscalías especializadas en esta materia deben asumir su competencia con ponderación, promoviendo actualizaciones académicas permanentes en convenio con las instituciones académicas. Que la aparición de la informática ha creado un desafío y nuevos paradigmas para la ciencia del derecho, que ha tenido que cambiar sus paradigmas para poder describir los usos y costumbres y las conductas sociales de pobladores. El derecho ha tenido que modernizar sus herramientas jurídicas acorde con los entornos digitales para poder valorar las evidencias.

II.2. Bases Teóricas

II.2.1. Teorías de la delincuencia y el efecto tecnológico en el crimen

Ante la pregunta simple de por qué la gente comete crímenes, se abren múltiples horizontes de análisis que buscan explicar las raíces de la conducta delictiva. Dos enfoques fundamentales en este debate son la teoría de la elección racional y la teoría del aprendizaje social. La primera postula que los individuos actúan de forma deliberada, evaluando minuciosamente los costos y beneficios de sus actos, mientras que la segunda destaca la influencia del entorno social y la imitación de modelos. Ambos marcos teóricos se ven potenciados por el avance tecnológico, que facilita el acceso a herramientas y redes que pueden influir en el proceso decisorio y en la normalización de conductas delictivas.

La Teoría de la Elección Racional se fundamenta en la premisa de que los individuos deciden delinquir mediante un proceso de evaluación de los costos y

beneficios asociados a sus acciones. Becker (1968) estableció que, al igual que en cualquier otra actividad, la toma de decisiones delictivas se realiza de forma lógica y calculada, considerando la ganancia potencial y el riesgo de ser sancionado. Esta perspectiva asume que la delincuencia es, en esencia, el resultado de un análisis racional en el que el actor opta por el delito si percibe que los beneficios superan los costos.

La introducción de nuevas tecnologías ha modificado sustancialmente este balance costo-beneficio. Según Cornish y Clarke (1986), el avance tecnológico ha permitido reducir la percepción del riesgo en la comisión de delitos, pues las herramientas digitales facilitan el anonimato, la planificación remota y la ejecución de actos ilícitos sin presencia física. Así, la tecnología actúa como un potenciador de la capacidad del delincuente para minimizar las barreras que tradicionalmente hubieran frenado sus conductas delictivas.

En consecuencia, el entorno digital ha transformado la práctica del delito al proporcionar métodos más sofisticados y menos detectables para la realización de actividades ilegales. Becker (1968) y Cornish y Clarke (1986) coinciden en que esta optimización de los mecanismos delictivos mediante la tecnología incrementa la rentabilidad percibida de cometer delitos, lo cual se traduce en un aumento potencial en la incidencia de delitos informáticos y otras actividades ilícitas facilitadas por las innovaciones tecnológicas.

La Teoría del Aprendizaje Social plantea que las conductas delictivas se adquieren a través de la observación e imitación de modelos presentes en el entorno social. Bandura (1977) estableció que los comportamientos se aprenden en un contexto social, en el que la exposición a modelos que refuerzan o premiar la conducta delictiva puede fomentar su adopción. Este marco teórico destaca la

importancia de los procesos de socialización y la influencia de pares y medios de comunicación en la formación de hábitos y actitudes respecto al delito.

La tecnología ha amplificado el impacto de estos procesos sociales al facilitar el acceso a redes de información y comunidades en línea donde se difunden conductas delictivas. Akers (1998) argumenta que, en la era digital, las plataformas de comunicación y las redes sociales permiten que los individuos compartan y aprendan técnicas delictivas de manera inmediata y global, lo que acelera el proceso de aprendizaje y normalización de estos comportamientos. Este intercambio de información reduce las barreras tradicionales de la transmisión cultural y crea espacios donde las conductas ilegales son incluso incentivadas.

Finalmente, la tecnología no solo incrementa la velocidad y el alcance de la socialización de conductas delictivas, sino que también modifica la percepción de la gravedad de dichas acciones. Bandura (1977) y Akers (1998) sostienen que la exposición continua a modelos que validan o glorifican el delito puede debilitar las inhibiciones sociales y morales que, de otra forma, limitarían la incidencia delictiva. Este fenómeno resalta la necesidad de adaptar estrategias de prevención e intervención social que consideren la influencia de la tecnología en la propagación de conductas delictivas.

II.2.2. Tipificación de patrimonio, fe pública y la indemnidad e intangibilidad sexual en la actual legislación peruana

La tipificación de los delitos contra el patrimonio en la legislación penal peruana se encuentra regulada en el Título V del Código Penal, el cual abarca una serie de conductas que atentan contra los bienes materiales o inmateriales de una persona, ya sea física o jurídica. Entre los principales delitos contra el patrimonio destacan el hurto (artículo 185), el robo (artículo 188), la estafa (artículo 196) y la

apropiación ilícita (artículo 190). El elemento común de estas figuras penales es la afectación o puesta en peligro del derecho de propiedad o posesión legítima, ya sea mediante la sustracción, la violencia, el engaño o la disposición indebida de los bienes ajenos. Así, el hurto se caracteriza por la sustracción sin empleo de violencia, mientras que el robo añade el uso de fuerza o intimidación contra la víctima. Por su parte, la estafa involucra un ardid o engaño para inducir a error a la víctima, y la apropiación ilícita se configura cuando alguien, teniendo posesión legítima de un bien ajeno, decide apropiárselo indebidamente. Estas tipificaciones buscan salvaguardar la seguridad jurídica de los ciudadanos y, de manera más amplia, la estabilidad económica y social, garantizando que los bienes y recursos sean protegidos de conductas ilícitas que puedan despojar a los propietarios de su legítima tenencia.

En el caso de los delitos contra la fe pública, su tipificación se encuentra en el Título X del Código Penal, abarcando conductas que menoscaban la confianza colectiva depositada en documentos, actos o símbolos que acreditan la veracidad o autenticidad de ciertos hechos o declaraciones. Entre estas conductas destacan la falsificación de documentos (artículos 427 al 431), la falsificación de sellos y timbres (artículos 433 y 434) y la falsificación de moneda (artículos 437 y 438). El elemento clave radica en la generación de perjuicios a la confianza social, dado que la veracidad de documentos oficiales, monedas y otros instrumentos de validación resulta fundamental para el correcto funcionamiento de las relaciones civiles y comerciales. Así, la ley sanciona tanto a quienes elaboran documentos falsos como a quienes, a sabiendas de su inautenticidad, los utilizan para generar ventajas indebidas o perjudicar a terceros. De este modo, el derecho penal peruano protege la fe pública como un bien jurídico de gran relevancia, puesto que la credibilidad y la certeza en la

documentación oficial y los medios de pago constituyen pilares esenciales para el ordenamiento jurídico y la convivencia pacífica de la sociedad.

La indemnidad e intangibilidad sexual, por su parte, se protegen en el Título IV del Código Penal peruano, bajo la denominación de "Delitos contra la libertad e indemnidad sexuales". Este conjunto de normas abarca una amplia gama de conductas que atentan contra la dignidad y la libertad sexual de las personas, tutelando principalmente a los menores de edad y a quienes, por su condición, no pueden prestar un consentimiento válido o libre. Dentro de este grupo se encuentran delitos como la violación sexual (artículos 170 y 173), el acto contra el pudor (artículo 176), la violación de personas en incapacidad de resistir (artículo 171) y el hostigamiento sexual (artículo 176-B), entre otros. La noción de indemnidad sexual hace referencia a la protección absoluta de la esfera sexual de los menores de edad, mientras que la libertad sexual se vincula con el derecho de todo individuo a decidir libremente sobre su vida sexual sin ser coaccionado o forzado por terceros. Así, la legislación peruana establece sanciones severas para quienes infrinjan estos derechos, especialmente cuando las víctimas son personas especialmente vulnerables, como los niños, adolescentes o personas con discapacidad mental.

Dentro de esta misma categoría se encuentra la protección de la llamada "intangibilidad sexual", entendida como la salvaguarda de la dignidad y el libre desarrollo de la sexualidad, sin que exista injerencia violenta, engañosa o abusiva por parte de terceros. Por ejemplo, la violación sexual contempla circunstancias agravantes cuando el agresor abusa de una posición de confianza o autoridad, o cuando la víctima se encuentra en una situación de indefensión física o psicológica. En el caso de menores de edad, la legislación adopta un enfoque de protección reforzada, presumiendo la inexistencia de consentimiento válido y castigando de

forma más drástica las conductas que vulneran su indemnidad sexual. Estas tipificaciones reflejan la voluntad del Estado peruano de proteger bienes jurídicos tan fundamentales como la libertad, la integridad y el normal desarrollo de la personalidad de cada individuo. Asimismo, se busca evitar la cosificación de la persona y combatir la violencia de género y otras formas de discriminación que atenten contra la dignidad humana. En síntesis, la regulación de los delitos contra la indemnidad e intangibilidad sexual en la legislación peruana responde a la necesidad de salvaguardar los derechos más básicos de la víctima, reconociendo la especial relevancia que reviste la libertad sexual en el contexto de los derechos humanos y la convivencia social.

II.2.3. Delito informático

Para satisfacer sus necesidades, las personas recurren a mecanismos tanto lícitos como ilícitos. Estos últimos violan indiscutiblemente las libertades y derechos de propiedad de los demás. Con los avances tecnológicos, una modalidad emergente es el delito cibernético, que no es una categoría antigua en el mundo delictivo. Se define como cualquier actividad ilegal que se lleva a cabo utilizando computadoras, Internet u otras tecnologías reconocidas por las leyes pertinentes (Congreso de la República del Perú, 2013). El cibercrimen es el delito más común, jugando un rol crucial en las estafas derivadas del desconocimiento y las brechas tecnológicas a las que las personas están expuestas. Los delincuentes no solo causan grandes pérdidas a la sociedad y al gobierno, sino que también pueden ocultar su identidad en gran medida. Existe una variedad de actividades ilegales que se cometen en Internet por individuos técnicamente calificados. Con una interpretación más amplia, se puede afirmar que el delito cibernético abarca cualquier actividad ilegal donde la computadora o Internet son herramientas, objetivos o ambos.

A pesar de los beneficios que nos brinda Internet, también tiene sus aspectos negativos. Algunos de los delitos cibernéticos más recientes incluyen la estafa en línea, el acoso cibernético, el terrorismo digital, la suplantación de identidad por correo electrónico, el bombardeo de correos electrónicos, la pornografía en línea y la difamación cibernética, entre otros. Algunos delitos tradicionales también pueden clasificarse como cibercrímenes si se cometen mediante computadoras o Internet (Arifin et al., 2020). En el caso peruano, se registraron poco más de 3,000 casos de delitos informáticos en 2019 (ANDINA, 2020).

II.2.4. Tipos de delitos informáticos

Para detallar estos delitos, es esencial resaltar los aportes de organizaciones multilaterales como la Organización de Naciones Unidas (ONU), quienes consideran los fraudes a través de computadoras, la manipulación y falsificación, el daño con software y el acceso no autorizado a hardware y servicios informáticos. Por otro lado, el convenio de Budapest se enfoca en el acceso ilegal, la interceptación ilícita, los ataques a la integridad de sistemas informáticos, así como de datos y el abuso de dispositivos. También destaca la falsificación y el fraude informáticos. Además, se abordan temas como la pornografía infantil y los delitos contra la propiedad intelectual y cuestiones afines. En este contexto, los delitos informáticos se pueden clasificar en grandes categorías, tal como lo sostiene la literatura del derecho norteamericano:

II.2.5. Invasión de la privacidad y robo de identidad

Dada la naturaleza altamente digitalizada de la recopilación y almacenamiento de datos, la información personal de los ciudadanos está más en riesgo que nunca. Usando datos almacenados en bases de datos nacionales, los individuos reciben un

número de Seguro Social en lugar de un número de identidad. Este sistema de identificación se utiliza en impuestos, atención médica, educación y documentación de empleados en algunas organizaciones privadas (Sharma & Gaherwal, 2017). El robo de identidad es altamente factible, ya que acceder al número de Seguro Social de una persona puede revelar gran cantidad de información sobre su ciudadanía y facilitar la usurpación de su identidad. Sin embargo, esta forma de ciberdelito no se limita al sistema de Seguridad Social, sino que también incluye el acceso y robo de datos de tarjetas de crédito digitalizadas (Al-Khater et al., 2020). La adquisición de datos de tarjetas de crédito o información de la Seguridad Social puede tener múltiples propósitos perjudiciales, desde generar grandes facturas a nombre de víctimas desprevenidas hasta vender la información con fines lucrativos. La relevancia multinacional del robo de identidad lo convierte en una de las formas más comunes de ciberdelincuencia.

Cuando tiene éxito, el robo de identidad puede vincularse con otras formas de ciberdelincuencia definidas de manera independiente o causar estos delitos directamente. Algunos ejemplos incluyen la piratería, el fraude en cajeros automáticos, el fraude electrónico, el intercambio de archivos y la piratería (Marcum & Higgins, 2019). El riesgo de robo de identidad en computadoras o redes digitales se puede identificar si un usuario recibe solicitudes de información confidencial (número de seguro social, detalles de la tarjeta de crédito, nombre de usuario, contraseña y PIN de aplicaciones financieras móviles, detalles de cuentas de ahorros) por correo electrónico o plataformas de redes sociales. Es importante tener en cuenta que las organizaciones que legítimamente necesiten dicha información (un empleador, un proveedor médico, una escuela, un banco o una agencia tributaria) rara vez, o nunca, utilizan estos canales para solicitarla (Al-Khater et al., 2020). Otros métodos de

detección incluyen el seguimiento de facturas para saber si se ha cambiado una dirección de facturación y cuándo; la revisión frecuente de facturas y cuentas bancarias para identificar cargos por compras no realizadas (Jahankhani et al., 2014); la revisión de informes crediticios para detectar cuentas a nombre extranjero; y la adquisición de programas de software sofisticados para la protección de contraseñas robustas y la detección de infiltraciones no autorizadas en la red (Marcum & Higgins, 2019).

En este contexto, se puede detallar una modalidad delictiva conocida como phishing, que se basa en obtener datos privados de los usuarios a través de internet, especialmente para acceder a sus cuentas o información bancaria. Estos se pueden clasificar en:

- Sitios web falsos y alertas de seguridad por correo electrónico: Los estafadores crean páginas web que aparentan ser legítimas, pero son una parodia. El objetivo de estos sitios es inducir al usuario a ingresar información personal, la cual es utilizada posteriormente para acceder a cuentas comerciales y bancarias.
- Correos electrónicos falsos de virus: Muchas advertencias enviadas por correo electrónico sobre virus son engaños, diseñados únicamente para causar preocupación y disrupción en los negocios.
- Fraudes de lotería: Son correos electrónicos que informan al destinatario que ha ganado un premio en una lotería. Para obtener el dinero, el destinatario debe responder. Luego, se recibe otro correo solicitando información bancaria para transferir directamente el dinero. Además, se solicita una tarifa de procesamiento/manejo. Evidentemente, el dinero

nunca se transfiere, la tarifa de procesamiento es estafada y los datos bancarios se utilizan para otros fraudes.

- Transacciones en línea fraudulentas con tarjetas de crédito: Proporcionar información de la tarjeta de crédito a través de internet, consciente o inconscientemente, puede resultar problemático. Si las transacciones electrónicas no están protegidas, los hackers pueden robar los números de la tarjeta de crédito y hacer un uso indebido de esta tarjeta, haciéndose pasar por el propietario.

II.2.6. Terrorismo cibernético

El terrorismo cibernético se refiere al uso, implementación u objetivo de computadoras y redes para difundir información o incitar miedo, ansiedad y violencia (Marsili, 2019). Al igual que las formas tradicionales de terrorismo, el terrorismo cibernético no solo es común, sino que sus impactos pueden ser graves. La difusión de propaganda cuidadosamente formulada a través de tecnologías de Internet y redes sociales puede afectar negativamente la credibilidad y disponibilidad de información en un área específica, facilitar el sabotaje político, cambiar la opinión pública, alterar la ley y el orden, dañar la infraestructura y causar la muerte (Jahankhani et al., 2014; Marsili, 2019). La detección del terrorismo cibernético es compleja, ya que la intención detrás de este generalmente se materializa antes de ser detectada. De hecho, el terrorismo cibernético a menudo pasa desapercibido para sus víctimas (Zhang, 2008). La clasificación de esta forma de delito cibernético a menudo recae en profesionales, generalmente empleados por el gobierno, que poseen los recursos psicológicos y analíticos necesarios para identificar información falsa que circula en el ciberespacio (Marcum & Higgins, 2019). En la superficie, uno puede equiparse para detectar y prevenir los efectos del terrorismo cibernético identificando

información en línea que ha sido sacada de contexto o que incita irracionalmente a la audiencia a tomar medidas drásticas. En esta investigación, no se profundiza en este punto, ya que no es el enfoque principal de la investigación debido a que no es un problema prevalente en la realidad latinoamericana y peruana en particular.

II.2.7. Pornografía infantil

La pornografía infantil, como forma de delito cibernético, consiste en la difusión de grabaciones digitales (videos, imágenes y archivos de audio) de niños y menores vestidos inapropiadamente, ligeros de ropa o desnudos; posando o hablando de manera sexualmente provocativa (Sae-Bae et al., 2014). A pesar de las diferencias sociológicas, la difusión de pornografía infantil es un delito grave a nivel mundial (Vyawahare & Chatterjee, 2020). Los impactos de la pornografía infantil en un menor incluyen daños permanentes a la autoimagen, desarrollo de trastornos psicológicos, problemas de socialización y alteraciones en el desarrollo sexual (Bada & Nurse, 2020). La detección de pornografía infantil no es un proceso sencillo, ya que identificar contenido digital que retrata a personas que parecen menores de edad en posiciones sexuales puede no ser completamente fiable. Esto se debe a que la edad de la mayoría en ciertas políticas puede ser tan baja como 18 años; una edad en la que los adultos legales pueden parecer fácilmente menores de edad (Sae-Bae et al., 2014). No obstante, este sigue siendo el mejor método para detectar la pornografía infantil en el contenido digital. En un nivel más alto de cumplimiento legislativo, los productores de contenido digital para adultos deben mostrar una certificación de que los actores, actrices y modelos en sus producciones son mayores de edad (Dragan, 2018). En la presente investigación, no se profundiza en este punto, ya que no es el enfoque principal de la investigación, dado que se ha hecho mucho esfuerzo a nivel nacional

para su estandarización global y erradicación, por lo que no comprende los tópicos detallados en la investigación.

II.2.8. Ciberacoso

El ciberacoso implica el uso de coerción, fuerza, amenazas y/o burlas para intimidar, abusar y/o dominar a otra persona a través de redes informáticas, Internet o plataformas de redes sociales (Ali et al., 2018; Perera & Fernando, 2021). El auge de las tecnologías de redes sociales ha sido parte integral del advenimiento y evolución del ciberacoso, ya que el crecimiento perpetuo en la cantidad de usuarios de diferentes grupos sociales ha generado un caldo de cultivo para comportamientos sociales no deseados en estas plataformas. Los adolescentes y las mujeres están sobrerrepresentados en la población víctima de ciberacoso (Vyawahare & Chatterjee, 2020). Las diversas formas que puede tomar el acoso cibernético incluyen, entre otras, el abuso cibernético (ataques verbales en las redes sociales); morphing (adquisición y difusión no autorizada de la información digital de una víctima con fines pornográficos) (Bada & Nurse, 2020); difamación cibernética (difusión de información falsa o increíble sobre un individuo o sus intereses en línea); y chantaje cibernético (uso ilegal de la información personal de un individuo para coaccionarlo e intimidarlo a conceder favores) (Dragan, 2018). La detección del ciberacoso sigue procesos similares a los de la detección del ciberterrorismo. Aquí, un usuario (o un padre) puede detectar el acoso cibernético buscando instancias de ataques verbales en las redes sociales, adquisición y difusión no autorizada de información digital (de su hijo) con fines pornográficos, difusión de información falsa o increíble sobre ellos o sus hijos, y el uso ilegal de información personal para coaccionarlos e intimidarlos a conceder favores políticos, sexuales o financieros (Dragan, 2018). Es importante comprender que el ciberacoso suele ser repetitivo y afecta principalmente a

adolescentes y mujeres. Estas variables son cruciales en la detección de posibles casos de esta forma de ciberdelito.

II.2.9. La Convención de Budapest

Los estados que forman parte de la Convención Internacional sobre Delitos Cibernéticos han identificado que las tecnologías modernas de comunicación y procesamiento de datos representan un desafío considerable en la lucha contra los delitos informáticos y cibernéticos (Federal Supreme Court of Switzerland, 2014). Esto se debe, en gran medida, a la naturaleza transnacional inherente de la tecnología subyacente (Clough, 2014). En muchos casos, resulta extremadamente difícil determinar la ubicación exacta donde se ha cometido un acto delictivo, dado que los datos pueden haberse cargado en un país, alojado en un segundo, mientras la víctima reside en un tercer país, y los datos robados pueden ser enviados a una cuarta jurisdicción (Weissbrodt, 2013). Esta complejidad geográfica y jurisdiccional añade una capa adicional de dificultad en la persecución y resolución de estos delitos.

El Convenio sobre Ciberdelincuencia del Consejo de Europa, comúnmente conocido como el Convenio de Budapest (Council of Europe, 2001b), es el primer instrumento internacional vinculante que aborda este tema (Clough, 2014). El preámbulo del Convenio de Budapest establece su objetivo como una "política criminal común dirigida a la protección de la sociedad contra el ciberdelito", y su intención es "disuadir las acciones dirigidas contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, las redes y datos, así como el uso indebido de dichos sistemas, redes y datos al prever la penalización de dicha conducta" (Council of Europe, 2001b). Este convenio busca armonizar las leyes nacionales para facilitar una cooperación internacional más efectiva en la lucha contra la ciberdelincuencia.

Acceso ilegal (art. 2 CCC)

El artículo 2 del Convenio de Budapest exige que cada país miembro adopte las medidas legislativas necesarias para criminalizar el acceso no autorizado e intencional a todo o parte de un sistema informático. Además, permite que un país exija que el delito se cometa infringiendo medidas de seguridad (Council of Europe, 2001a). Esta disposición es coherente con el artículo 5 lit. f del GDPR, que establece estándares para la protección adecuada de datos (Buchholtz & Stentzel, 2018). Este tipo de delito es análogo al allanamiento de morada, en el que se obtendría una llave para abrir una puerta sin permiso. La intención detrás de esta legislación es asegurar que los sistemas informáticos estén protegidos contra accesos no autorizados que puedan comprometer la integridad y seguridad de los datos y sistemas.

Interceptación ilegal (art. 3 CCC)

El artículo 3 del Convenio requiere que cada país tipifique como delito la interceptación no autorizada de transmisiones no públicas de datos informáticos hacía, desde o dentro de un sistema informático, incluyendo emisiones electromagnéticas. Esta medida pretende proteger la privacidad de los datos, de manera similar a cómo las escuchas telefónicas violan la privacidad en el mundo físico (Dine, 2020). La interceptación ilegal implica que el flujo de datos entre el remitente y el destinatario es interrumpido o desviado, lo que puede resultar en la obtención de información privada sin el consentimiento de las partes involucradas. Este tipo de vigilancia ilegal puede tener consecuencias graves para la privacidad y la seguridad de la información personal y comercial.

Interferencia de datos (art. 4 CCC)

El artículo 4 del Convenio de Budapest establece que cada país debe tipificar como delito la alteración, daño, supresión o deterioro intencional y no autorizado de

datos informáticos. Es fundamental que estas acciones se realicen "sin derecho" e "intencionalmente" (Council of Europe, 2001a), ya que los operadores del sistema podrían interferir con los datos de manera negligente, pero con derecho a hacerlo. Un ejemplo común de interferencia de datos es la instalación de ransomware, que cifra archivos para extorsionar al propietario legítimo (Kansagra et al., 2015). Esta modalidad delictiva puede causar interrupciones significativas en las operaciones de una organización, así como pérdidas financieras y de reputación. La intencionalidad y la falta de autorización son elementos clave para distinguir entre una interferencia legítima y un acto delictivo.

Interferencia del sistema (art. 5 CCC)

El artículo 5 del Convenio obliga a cada país a criminalizar la obstaculización intencional y no autorizada del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro o alteración de datos informáticos. Este artículo se centra en la funcionalidad del sistema más que en la disponibilidad e integridad de los datos (Council of Europe, 2001a). Ambas disposiciones reconocen el uso de ransomware como una herramienta típica para llevar a cabo actividades ilegales, aunque la extorsión no es un requisito para que se considere un delito. La interferencia en el sistema puede causar interrupciones operativas graves, afectando la capacidad de las organizaciones para llevar a cabo sus actividades diarias y comprometiendo la seguridad de la información.

Uso indebido de dispositivos (art. 6 CCC)

El artículo 6 del Convenio de Budapest establece que cada país debe tipificar como delito la producción, venta, adquisición para uso, importación, distribución o puesta a disposición de dispositivos, incluidos programas informáticos, diseñados principalmente para cometer delitos establecidos en los artículos 2 a 5. Además, la

posesión de tales dispositivos con la intención de cometer delitos también debe ser penalizada (Council of Europe, 2001a). Con el auge del "Internet de las cosas", el mal uso de dispositivos se ha vuelto aún más relevante de lo que se anticipó inicialmente. Los dispositivos conectados a internet, como electrodomésticos inteligentes y sistemas de automatización del hogar, pueden ser explotados por ciberdelincuentes para obtener acceso no autorizado a redes y datos, presentando nuevos desafíos para la seguridad cibernética.

Falsificación informática (art. 7 CCC)

El artículo 7 del Convenio exige que cada país tipifique como delito la introducción, alteración, supresión o eliminación intencional y no autorizada de datos informáticos, resultando en datos no auténticos, con la intención de que se consideren auténticos a efectos legales (Council of Europe, 2001a). Este artículo llena un vacío en el derecho penal relacionado con la falsificación tradicional, aplicando la misma lógica a los datos digitales. La falsificación informática puede tener graves consecuencias, ya que los datos no auténticos pueden ser utilizados para engañar a entidades legales y comerciales, resultando en fraudes y otras actividades delictivas.

Fraude informático (art. 8 CCC)

El artículo 8 del Convenio establece que cada país debe tipificar como delito la pérdida de propiedad de otra persona mediante la alteración, supresión o eliminación de datos informáticos o la interferencia en el funcionamiento de un sistema informático, con intención fraudulenta o deshonesta para obtener un beneficio económico (Council of Europe, 2001a). Los correos de phishing son un ejemplo común de fraude informático, donde los delincuentes simulan ser remitentes legítimos para solicitar transferencias de dinero. Este tipo de fraude puede causar pérdidas significativas a las víctimas, tanto en términos de dinero como de confianza, y

representa una amenaza constante para la seguridad de la información y las transacciones financieras.

Conservación acelerada de datos informáticos almacenados (art. 29 cif. 1 CCC) El artículo 29 del Convenio permite que un país solicite a otro que conserve rápidamente los datos almacenados mediante un sistema informático en su territorio, con la intención de presentar una solicitud de asistencia mutua para búsqueda, acceso, incautación o divulgación de datos (Council of Europe, 2001a). Esto es esencial para evitar que los datos se modifiquen, eliminen o destruyan durante la preparación, transmisión y ejecución de una solicitud de asistencia judicial recíproca (Isenring et al., 2019). La conservación rápida de datos es crucial en la lucha contra el ciberdelito, ya que garantiza que las pruebas digitales se mantengan intactas y disponibles para las investigaciones y procesos judiciales.

II.2.10. Influencia del Convenio de Budapest en Perú

El Convenio de Budapest puede contribuir significativamente a los países miembros al fomentar una política común en el derecho penal aplicada a la ciberdelincuencia. Este tratado permite la adopción de una legislación específica para abordar este tipo de delitos y su evolución constante. Su finalidad incluye la capacidad preventiva mediante el uso de herramientas acordadas en el Convenio de Budapest, especialmente aquellas relacionadas con los datos informáticos, y el establecimiento de una red cooperativa para mejorar las capacidades de detección e investigación de delitos. En otras palabras, busca una mayor visibilidad y comprensión de los delitos cibernéticos a medida que la tecnología avanza, conforme a los artículos del capítulo II del Acuerdo.

La incorporación del Convenio de Budapest en la legislación peruana se ha reflejado en diversos ajustes normativos que buscan robustecer la respuesta penal

frente a los delitos informáticos, especialmente durante las reformas de 2019 y 2022. A finales de 2019, la Ley 30096 experimentó modificaciones que reforzaron la protección de datos personales y precisaron el catálogo delictivo, alineándose con los principios establecidos por dicho convenio. El Convenio de Budapest, reconocido como el primer instrumento internacional vinculante en materia de ciberdelincuencia, obliga a los Estados firmantes a tipificar conductas como el acceso ilícito a sistemas informáticos, la interferencia en datos y la utilización indebida de dispositivos.

En consecuencia, la normativa peruana amplió el ámbito de la protección penal para abarcar con mayor detalle la vulneración de datos personales y la explotación indebida de información digital. Esta armonización se tradujo en la inclusión de nuevos tipos penales que sancionan la captura, interceptación y difusión de información, además de endurecer las penas cuando estas conductas afectan de manera grave la integridad de datos o sistemas informáticos. Dichas reformas reflejan el interés de Perú por acoplarse a los estándares internacionales, fortaleciendo la salvaguarda de los derechos fundamentales en el entorno digital y participando de forma efectiva en la persecución del ciberdelito a nivel global. Asimismo, las modificaciones de 2019 contemplan la adopción de herramientas procesales que permiten a las autoridades recabar y preservar evidencia digital con mayor eficiencia, en consonancia con las directrices sobre cooperación y recolección de pruebas electrónicas que promueve el Convenio de Budapest. De esta forma, Perú se aproxima a la construcción de un marco legal moderno y sólido que responda a los desafíos crecientes de la delincuencia en línea, garantizando una mayor protección de la privacidad y los datos personales en la era digital.

Las reformas introducidas en 2022 consolidaron los avances previos al fortalecer los mecanismos de cooperación internacional y actualizar los conceptos

tecnológicos recogidos en la legislación nacional. Esta orientación se sustenta en la esencia del Convenio de Budapest, que impulsa la colaboración entre Estados para enfrentar la naturaleza transnacional de la ciberdelincuencia. A través de estas disposiciones, se han implementado protocolos de intercambio de información y asistencia judicial más ágiles, además de establecer canales de comunicación seguros entre las autoridades competentes. Por otro lado, se incorporaron nuevas figuras delictivas, como la ciber extorsión y el uso indebido de tecnologías emergentes, atendiendo la exigencia de mantener la legislación en sintonía con los vertiginosos cambios tecnológicos que caracterizan al entorno digital.

Con ello, se busca no solo lograr una armonización normativa a escala global, sino también dotar a las instituciones peruanas de herramientas más eficaces para investigar y perseguir delitos cibernéticos. El perfeccionamiento de la legislación incluye metodologías especializadas en ciberseguridad y la adopción de estándares técnicos internacionales que facilitan el rastreo e identificación de actividades ilícitas en la red. Simultáneamente, se promueve la participación de Perú en redes de intercambio de información sobre incidentes de ciberseguridad, fortaleciendo la cooperación con otros países signatarios o afines al Convenio de Budapest. De esta manera, la evolución constante de las leyes peruanas en materia de delitos informáticos no solo responde a la necesidad de proteger a la ciudadanía frente a amenazas digitales cada vez más sofisticadas, sino también al compromiso de integrarse a una estrategia internacional coordinada para combatir el cibercrimen. En suma, la armonización con los lineamientos del Convenio de Budapest se erige como pilar esencial para la eficacia de las políticas criminales en un escenario crecientemente globalizado y digitalizado.

II.2.11.Marco común de derecho penal sustantivo

La firma del Pacto de Budapest ha llevado a la tipificación de leyes específicas en los países signatarios. En Perú, los ciberdelitos se definen como aquellos realizados "deliberada e ilegítimamente". La legislación peruana sobre delitos informáticos ha avanzado en la inclusión de comportamientos no contemplados en el Convenio, tales como el grooming, la interferencia telefónica y la discriminación, integrándolos en el código penal. Sin embargo, una de las dificultades para establecer un marco común radica en la definición de "delitos informáticos", ya que es complejo limitarla únicamente a aquellos donde el bien jurídico es la información o el bien informático, excluyendo otros delitos cometidos mediante medios tecnológicos.

Aún no se puede afirmar que Perú ha alcanzado el estándar del Convenio de Budapest, ya que la aplicación por parte de los operadores jurídicos es limitada e incierta. No se conoce el número total de casos no denunciados, aquellos que pasan por la investigación policial y cuántos se convierten en casos penales y son sentenciados. Esto implica una falta de jurisprudencia desarrollada, lo que limita a los operadores de justicia en sus procesos. Además, se observan iniciativas ejecutivas y legislativas descoordinadas, como el Decreto Legislativo N° 1182 (acceso policial a las comunicaciones) y la Ley de Delitos Informáticos (Ley N° 30096).

II.2.12. Estandarización de procesos penales

El Convenio de Budapest establece criterios para la persecución de delitos en el fuero penal y la recolección de pruebas para demostrar los delitos, además de proporcionar un marco legal común para el ámbito penal. Incluye la obligatoriedad de la preservación de datos informáticos y establece formas para la retención y confiscación de estos datos. Aunque gran parte de la legislación peruana está alineada con el Convenio de Budapest, no está plenamente integrada en los procesos judiciales peruanos. Mientras que el Convenio establece medidas procesales, garantías y

jurisdicción aplicable, estas no aparecen en el código penal peruano con las particularidades del delito cibernético y solo se alinean con la normativa usual para delitos comunes. Además, la legalidad de la obtención y uso de pruebas, el debido proceso y la competencia territorial son áreas que necesitan mayor desarrollo.

Con las innovaciones del artículo 230 del código penal vigente, se han mejorado los detalles sobre el tráfico y conservación de la información, pero no se ha desarrollado un procedimiento claro para actuar conforme a esta normativa. Esto se contradice con la obligación de conservar la información de los aparatos geolocalizados, una norma vigente desde 2015. La falta de claridad y desarrollo en estos procedimientos impide una aplicación efectiva y coherente de las leyes, lo que subraya la necesidad de una mayor integración y alineación con los estándares internacionales establecidos por el Convenio de Budapest.

II.2.13. Cooperación Internacional

En temas de extradición, asistencia recíproca y la creación de mecanismos de respuesta a emergencias, el Convenio de Budapest proporciona directrices claras para la coordinación y cooperación entre sus miembros. En el contexto peruano, aún no se ha implementado plenamente esta disposición para fortalecer los lazos con los miembros del convenio, lo cual representa una oportunidad de mejora significativa. Este proceso puede mejorarse mediante acuerdos multisectoriales que involucren al Ministerio del Interior, el Ministerio de Defensa, el Ministerio de Relaciones Exteriores y el Ministerio de Transportes y Comunicaciones.

Los objetivos de esta cooperación internacional incluirían la protección del país contra ciberataques de gran escala, como el terrorismo digital, facilitando el manejo judicial de bandas internacionales que operen o afecten al país. Además, participar en capacitaciones organizadas por los países miembros y estar preparados para ataques

cibernéticos en escenarios de alta demanda de servicios digitales, como ocurrió durante la pandemia de COVID-19, cuando la presencia digital de la población aumentó significativamente, haciéndola más vulnerable a la ciberdelincuencia.

II.2.14. Dimensiones de la ciberdelincuencia

En un artículo reciente, Tsakalidis y Vergidis (2019) adoptan la Taxonomía de la Convención sobre Ciberdelincuencia (Council of Europe, 2001a) para respaldar su nuevo marco de clasificación. La taxonomía propuesta por Tsakalidis y Vergidis (2019) refleja fielmente la clasificación del Consejo de Europa, con algunas modificaciones clave. Las dimensiones utilizadas son las siguientes:

- Delitos contra la Confidencialidad, Integridad y Disponibilidad de los Datos y Sistemas Informáticos: Esta categoría incluye acceso ilegal (piratería, cracking), adquisición ilegal de datos (espionaje de datos), interceptación ilegal, interferencia de datos, interferencia del sistema y mal uso de dispositivos.
- Delitos relacionados con la informática: Se dividen en falsificación informática, fraude informático y robo de identidad.
- Delitos relacionados con el contenido: Esta dimensión abarca material pornográfico, abuso sexual infantil, explotación sexual infantil, ofensas religiosas, ciberacoso, apuestas ilegales y juegos en línea, spam y amenazas relacionadas, racismo y discurso de odio en internet.
- Delitos relacionados con infracciones de derechos de autor y derechos conexos: Aquí se incluyen los delitos relacionados con los derechos de autor y marcas registradas.

- Delitos combinados relacionados con la identidad, la seguridad y la ofensa: Incluyen suplantación de identidad, lavado cibernético, guerra cibernética y uso terrorista de internet.

Estas modificaciones incluyen la adición de 'Adquisición ilegal de datos' en los delitos de Tipo A (o 'Dimensión 1'), 'Identidad urbana' en los delitos de Tipo B (o 'Dimensión 2'), 'Delitos relacionados con marcas comerciales' en el Tipo D (o 'Dimensión 4') y 'Racismo e incitación al odio en Internet' en los delitos de Tipo C (o 'Dimensión 3'), en lugar de separarlos como una dimensión individual. Tsakalidis y Vergidis (2019) han expandido significativamente los delitos de Tipo C (o 'Dimensión 3'), agregando seis nuevos delitos relacionados con el contenido: material pornográfico, delitos religiosos, ciberacoso, apuestas ilegales y juegos en línea, spam y amenazas relacionadas, y racismo y discurso de odio en internet. Además, proponen la adición de un Tipo E o “Delitos combinados” para incluir “actos que combinan varios delitos diferentes en actos únicos” (Tsakalidis & Vergidis, 2019, p. 716).

CAPÍTULO III
HIPÓTESIS Y CATEGORÍAS

III.1. Hipótesis

III.1.1. Hipótesis general

Existe una diferencia significativa entre la ley de delitos informáticos del Perú y el convenio de Budapest acerca de la ciberdelincuencia, Cusco 2024.

III.1.2. Hipótesis específicas

- Existe una diferencia significativa entre la ley de delitos informáticos del Perú y el convenio de Budapest acerca del bien jurídico del patrimonio en la modalidad de fraude informático, Cusco 2024.
- Subsiste una brecha de aplicación entre la ley de delitos informáticos del Perú y el convenio de Budapest en cuanto al bien jurídico de la fe pública en la modalidad de la suplantación de identidad Cusco 2024.
- Resulta por el momento inaplicable el cumplimiento cabal del convenio de Budapest en la normativa peruana de delitos informáticos respecto del bien jurídico de la libertad e intangibilidad sexual en la modalidad de proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, Cusco 2024.

III.1.3. Categorías de Estudio

Tabla 1.
Operacionalización de variables

	Categoría 1: Convenio de Budapest
Definición Conceptual	**Instrumento internacional que busca armonizar las leyes nacionales para combatir el ciberdelito mediante la cooperación internacional y la tipificación específica de delitos cibernéticos.**
Definición Operacional	Evaluación de la implementación del Convenio de Budapest en el marco legal peruano sobre ciberdelitos.
Dimensiones	Tipificación de delitos cibernéticos
Indicadores	Inclusión de delitos específicos como fraude informático y suplantación de identidad; Obligación de preservar datos; Aplicación práctica en procesos penales.
Instrumentos	Encuestas y entrevistas a juristas y especialistas en ciberdelitos; análisis documental del marco legal.
	Categoría 2: Ley de Delitos Informáticos del Perú (Ley N° 30096)
Definición Conceptual	**Normativa nacional que regula los delitos cibernéticos en Perú, enfocada en la protección de bienes jurídicos como el patrimonio, la fe pública y la indemnidad sexual.**
Definición Operacional	Análisis de la eficacia y limitaciones de la Ley N° 30096 frente a los delitos cibernéticos más comunes.
Dimensiones	Protección del patrimonio
Indicadores	Regulación de fraude informático; sanciones por suplantación de identidad; medidas contra proposiciones sexuales en línea.
Instrumentos	Encuestas a operadores del sistema de justicia; entrevistas a legisladores; revisión de casos judiciales.

Fuente: Elaboración propia

CAPÍTULO IV
METODOLOGÍA DEL ESTUDIO

IV.1. Métodos, Tipo o Alcance de la Investigación

Este estudio adoptó el método científico, caracterizado por un enfoque sistemático y objetivo para la investigación y recopilación de datos, con el fin de comprender y explicar fenómenos sociales. Se utilizó el método comparativo, que permite analizar similitudes y diferencias entre sistemas legales para identificar patrones, vacíos y elementos relevantes. Este enfoque se complementó con el método hipotético-deductivo, que parte de teorías generales para formular proposiciones específicas que se verifican mediante observaciones empíricas o análisis estadísticos (Hernández Sampieri & Mendoza Torres, 2018).

El tipo de investigación fue aplicado, ya que busca generar conocimiento de ventaja para la fines teóricos y prácticos para optimizar la legislación peruana en ciberdelitos tomando como referencia el Convenio de Budapest. Esta investigación también tuvo un nivel descriptivo, al detallar la tipificación de delitos informáticos y su relación con el marco legal nacional, utilizando herramientas de estadística descriptiva e inferencial.

IV.2. Diseño de Investigación

El diseño cualitativo. Se analizó los datos obtenidos mediante cuestionarios y un enfoque cualitativo para interpretar aspectos legales, vacíos normativos y opiniones de expertos (Hernández-Sampieri & Mendoza, 2018). Al tratarse de un diseño no experimental, no se manipularon intencionadamente las variables, sino que se observaron los fenómenos en su contexto natural, lo que permitió evaluar la relación entre el Convenio de Budapest y la Ley de Delitos Informáticos (Ley N.º 30096).

IV.3. Población y Muestra de Estudio

IV.3.1. Población

La población incluyó a profesionales del derecho penal y agentes policiales de la ciudad de Cusco que participaron en casos de ciberdelitos. Esta población incluyó fiscales, jueces, abogados penalistas y miembros de la Policía Nacional del Perú.

IV.3.2. Muestra

Se seleccionó una muestra de 15 profesionales mediante un muestreo no probabilístico por criterio, dado que su participación dependía de su experiencia en investigación y judicialización de ciberdelitos.

IV.3.2.1. Muestreo

El tamaño de muestra se realizó a través de un muestreo no probabilístico, que es una técnica de muestreo en la que cada miembro de la muestra se elige de manera arbitraria (Hernández-Sampieri & Mendoza, 2018).

IV.3.2.2. Criterios de inclusión

- Profesionales del derecho que trabajen en el Ministerio Público o ejerzan como litigantes en casos de ciberdelincuencia.
- Policías con experiencia en la investigación de ciberdelitos.
- Experiencia comprobable en procesos relacionados con el Convenio de Budapest y la Ley de Delitos Informáticos.

IV.3.2.3. Criterios de exclusión

- Profesionales o agentes sin experiencia en ciberdelitos.
- Personas que no aceptaron participar en el estudio o no firmaron el consentimiento informado.

IV.4. Técnicas e Instrumentos de Recolección de Datos

Se utilizó la técnica de la encuesta como herramienta principal, y el cuestionario estructurado como instrumento de recolección de datos, además de que se aplicaron entrevistas semi estructuradas dentro de la aplicación del mismo cuestionario. Este cuestionario se basó en las dimensiones propuestas por Tsakalidis y Vergidis (2019) para el Convenio de Budapest, adaptándose a las especificaciones de la Ley N.º 30096. Además, se incorporaron indicadores desarrollados por Vargas (2022) para identificar vacíos normativos y prácticas judiciales.

El instrumento incluyó dimensiones normativas (tipificación de ciberdelitos, pluralidad de agentes, adaptación a tecnologías emergentes) y aspectos operativos (capacidades de investigación, capacitación de personal). La validez del instrumento fue confirmada mediante juicio de expertos, mientras que su confiabilidad se evaluó con el coeficiente alfa de Cronbach, obteniéndose un valor esperado mayor a 0.70. Para la parte cualitativa, se realizaron entrevistas semiestructuradas a la par del cuestionario, dirigidas a obtener información detallada sobre las percepciones y experiencias de los participantes respecto a los vacíos normativos y la aplicación del Convenio de Budapest en el contexto peruano. En el caso del instrumento cualitativo, la validez se aseguró mediante la triangulación de informantes.

IV.5. Procedimiento para la Recolección de Datos

Se obtuvo el consentimiento informado de los participantes, así como las autorizaciones institucionales necesarias para aplicar las encuestas a fiscales, jueces y policías en Cusco. Las encuestas se llevaron a cabo tanto de manera presencial como digital, garantizando la confidencialidad y anonimato de las respuestas. Posterior a eso, se exportaron los resultados a programas como el Excel 2019 y el Programa estadístico en ciencias sociales (SPSS por sus siglas en inglés) v. 26. En este último se llevaron a cabo análisis estadísticos avanzados esenciales para el examen de las teorías. Los instrumentos se realizaron en formato presencial y virtual, utilizando preguntas abiertas que permitieron explorar aspectos profundos del tema investigado.

IV.6. Técnicas de Análisis de Datos

El análisis de datos combinó enfoque a uno mixto de incidencia cualitativa. Los datos recolectados fueron analizados mediante estadística descriptiva e inferencial. Inicialmente, se realizó una prueba de normalidad para determinar si se debían aplicar pruebas paramétricas o no paramétricas. Posteriormente, se emplearon tablas y figuras para la contestación de las preguntas clave de la investigación a través de las respuestas obtenidas en los cuestionarios.

En el análisis cualitativo, se utilizó la codificación temática para identificar patrones y categorías emergentes en las respuestas de los instrumentos. Este análisis permitió contextualizar y complementar los hallazgos.

IV.7. Aspectos Éticos

Para garantizar el cumplimiento de principios éticos, se implementaron las siguientes medidas:

Obtención del consentimiento informado.

Resguardo del anonimato y la confidencialidad de los datos.

Uso exclusivo de los datos para fines académicos.

El respeto a la dignidad de los participantes y la fiabilidad de los resultados fueron pilares fundamentales del estudio. Estas acciones estuvieron alineadas con los lineamientos éticos de la Universidad Continental y las buenas prácticas investigativas descritas por Ríos Cataño (2020).

CAPÍTULO V
RESULTADOS

V.1. Análisis descriptivo

V.1.1. Objetivo general

El análisis evidencia múltiples desafíos en la legislación peruana y el Convenio de Budapest frente a los delitos informáticos. En términos generales, los entrevistados coinciden en señalar que la normativa actual no se ajusta a la velocidad con la que evolucionan las tecnologías y las modalidades delictivas. La falta de precisión y adaptabilidad en las leyes, así como la ausencia de definiciones claras, dificulta la persecución y sanción efectiva de los delitos como el fraude informático, la suplantación de identidad y las proposiciones sexuales a menores. Esto genera una percepción de impunidad y expone la necesidad urgente de una reforma integral.

La evaluación de la legislación peruana y el Convenio de Budapest respecto a delitos informáticos evidencia una percepción generalizada de insuficiencia en el marco normativo y en las capacidades institucionales para enfrentar estos desafíos. En cuanto al fraude informático, el 93% de los encuestados considera que la normativa peruana presenta vacíos significativos, resaltando la necesidad de una actualización que contemple modalidades delictivas emergentes y mecanismos efectivos de prevención y sanción. Respecto al Convenio de Budapest, el 53% identifica insuficiencias, lo que subraya la urgencia de adaptarlo a la evolución de las amenazas digitales y a las necesidades nacionales específicas.

La suplantación de identidad, otro tema central, refleja vacíos similares. El 73% de los encuestados señala deficiencias en la legislación peruana, mientras que el 67% percibe que el Convenio de Budapest no aborda suficientemente este delito. Esto resalta la importancia de desarrollar definiciones legales más claras y mecanismos

específicos de cooperación internacional. Asimismo, la falta de preparación de policías y fiscales es un problema recurrente, con el 80% considerando que no están capacitados para manejar casos de suplantación de identidad y el 93% respaldando la necesidad de una capacitación continua.

Por último, en delitos relacionados con proposiciones sexuales a menores, el 87% identifica vacíos normativos en la legislación peruana, y el 73% considera que el Convenio de Budapest no cubre adecuadamente estos delitos. Esta percepción refuerza la necesidad de marcos legales y operativos más robustos, con un enfoque integral que incluya formación especializada, cooperación internacional y herramientas tecnológicas avanzadas.

En conjunto, estos hallazgos resaltan la necesidad de reformas legislativas, fortalecimiento institucional y actualización del Convenio de Budapest para enfrentar de manera efectiva los desafíos de la ciberdelincuencia, priorizando la protección de los derechos fundamentales de los ciudadanos y la seguridad digital en un entorno tecnológico en constante evolución.

Aunque constituye un marco relevante para la cooperación internacional, presenta limitaciones importantes para abordar las particularidades nacionales y los delitos emergentes. La desconexión entre las disposiciones internacionales y la realidad local peruana limita su implementación práctica y su capacidad para ofrecer soluciones efectivas. Asimismo, las empresas internacionales y locales son señaladas por su falta de cooperación en las investigaciones, lo que retrasa y complica aún más la acción legal.

Otro aspecto crítico identificado es la insuficiencia en la preparación de las autoridades, como policías y fiscales, para abordar la creciente complejidad de los delitos informáticos. La falta de formación continua y de acceso a herramientas

tecnológicas avanzadas es un obstáculo significativo para enfrentar estas amenazas. Los entrevistados enfatizan la necesidad de implementar programas de capacitación especializada que aborden no solo las técnicas actuales de investigación, sino también las dinámicas cambiantes del entorno digital.

En el caso de los delitos contra menores, como las proposiciones sexuales a través de medios tecnológicos, se subraya la ausencia de normativas específicas y protocolos claros que protejan eficazmente a esta población vulnerable. La falta de regulación en plataformas digitales, redes sociales y aplicaciones de juegos en línea es un factor agravante, lo que facilita la proliferación de delitos como el grooming y otras formas de explotación.

En conjunto, estos hallazgos resaltan la necesidad de fortalecer el marco normativo peruano, actualizar el Convenio de Budapest y establecer mecanismos sólidos de cooperación internacional. Los entrevistados abogan por un enfoque integral que combine la reforma legislativa, la capacitación continua de las autoridades y la colaboración efectiva de las empresas privadas para enfrentar de manera eficiente los desafíos de la ciberdelincuencia.

V.1.2. Objetivo específico 1

El marco normativo actual no está diseñado para abarcar los delitos informáticos que se desarrollan rápidamente con el avance tecnológico. Según los entrevistados, “el marco normativo actual no comprende la rapidez con la que evoluciona la tecnología”, lo que crea una desconexión evidente entre las leyes y las amenazas emergentes. Esta brecha facilita que los delincuentes adapten sus estrategias a vacíos legales, generando una sensación de impunidad. Además, se destacó que “el ordenamiento jurídico debe adaptarse a la delincuencia delictiva, ya que existen diversos delitos que no están identificados adecuadamente”. Esto sugiere que las

normativas carecen de flexibilidad y previsión para incorporar nuevas modalidades delictivas, como las vinculadas al fraude informático y a la suplantación de identidad. La legislación debería no solo responder a los problemas actuales, sino anticiparse a posibles amenazas en el entorno digital.

Por otro lado, el reducido porcentaje que no considera necesaria la capacitación permanente podría deberse a una percepción errónea de suficiencia en los conocimientos actuales o una subestimación del impacto del fraude informático. Sin embargo, la clara mayoría que aboga por la capacitación destaca una necesidad crítica: invertir en el desarrollo de competencias especializadas como una estrategia preventiva y reactiva frente a este tipo de criminalidad.

Otro aspecto importante mencionado es que "la persecución y la acción frente a la sanción de los delitos informáticos no existen debido a la falta de formalización de la investigación preparatoria". Esto implica que, incluso en casos donde las leyes son claras, la ausencia de procedimientos formales para investigar y sancionar delitos limita la capacidad del sistema legal para responder eficazmente.

Además, se señala que "ya que no precisa todas las modalidades de fraude informático", las normativas actuales requieren una reforma integral para incluir variantes específicas de delitos digitales. Esto permitiría abordar de manera más efectiva las conductas ilícitas que afectan tanto a individuos como a organizaciones, reduciendo significativamente los vacíos legales existentes.

La ausencia de definiciones claras y específicas en las normativas es una barrera importante en la lucha contra los delitos informáticos. Los entrevistados indicaron que "no están bien definidas las conductas delictivas", lo que complica su identificación y clasificación durante las investigaciones. Esto no solo afecta el proceso judicial, sino que también dificulta la comprensión por parte de los operadores legales.

Asimismo, se mencionó que “la ley no define claramente el bien jurídico protegido ni los ámbitos de competencia respecto al lugar donde se comete el delito”. Este vacío es especialmente problemático en el contexto de delitos transnacionales, donde las jurisdicciones se superponen y las investigaciones se ven obstaculizadas por la falta de criterios claros. La falta de precisión en las normativas permite que los delincuentes aprovechen estas ambigüedades.

Otro punto relevante es que “por no haberse considerado todas las modalidades de fraude informático, las leyes actuales no cubren los delitos emergentes”. Esto refleja una insuficiencia en la cobertura legal, dejando fuera de regulación conductas que afectan gravemente la seguridad digital. La creación de normativas más amplias y específicas podría cerrar estas lagunas y mejorar la capacidad del sistema legal para abordar nuevas amenazas.

En palabras de los entrevistados, “en vista de que algunas leyes no están sujetas a la realidad de la sociedad del país, es fundamental que las normativas sean más específicas y adaptadas”. Esto sugiere que un enfoque más localizado y realista podría aumentar la efectividad de las leyes en contextos específicos, como el de Perú, donde las dinámicas sociales y tecnológicas tienen particularidades únicas.

El Convenio de Budapest es reconocido como un marco internacional importante, pero los entrevistados señalaron que “el convenio desde un punto de vista no se ajusta de manera suficiente a todos los diferentes delitos que vienen apareciendo en sus modificaciones”. Esto refleja una percepción de que el convenio no ha evolucionado al mismo ritmo que las amenazas cibernéticas, dejando fuera de su alcance varias conductas emergentes.

También se señaló que “considero que debería ser más específico y no está sujeto a las leyes peruanas”. Esto pone en evidencia una desconexión entre las

disposiciones internacionales y las necesidades locales, lo que reduce la efectividad del convenio en contextos como el peruano. La falta de alineación con las normativas nacionales limita su aplicación práctica y su impacto.

Otro aspecto resaltado es que "el Perú como país ingresó muy tarde al Convenio de Budapest". Este retraso ha impedido que el país adapte el convenio a tiempo y desarrolle capacidades suficientes para implementarlo. La integración tardía también ha dificultado el establecimiento de mecanismos efectivos de cooperación internacional.

En términos de cooperación, los entrevistados expresaron que "más información y colaboración entre empresas privadas y estatales es esencial para que el convenio funcione". Esto indica que el éxito del convenio no solo depende de su diseño, sino también de la participación de los actores clave, tanto nacionales como internacionales, para garantizar su efectividad.

La colaboración limitada de las empresas privadas es un problema recurrente en la lucha contra los delitos informáticos. Los entrevistados destacaron que "obligar a las empresas privadas a responder a la información solicitada es fundamental, ya que muchas no responden adecuadamente". Esto refleja una falta de compromiso por parte del sector privado, que prioriza sus intereses comerciales sobre su responsabilidad en la seguridad digital.

Se mencionó que "las empresas internacionales no responden ni toman en cuenta el convenio, lo que dificulta las investigaciones". Esta resistencia para colaborar con las autoridades locales o internacionales dificulta la obtención de pruebas y ralentiza los procesos judiciales, afectando la efectividad de la persecución penal.

Además, los entrevistados indicaron que “porque no se recibe respuesta inmediata al pedido de información a las instituciones comprometidas, las investigaciones se ven retrasadas”. Esto resalta la importancia de establecer mecanismos obligatorios que exijan la cooperación del sector privado, especialmente en casos donde la rapidez en la respuesta es esencial para el éxito de las investigaciones.

La falta de colaboración también se traduce en una percepción de impunidad, ya que, como se expresó, “más información y colaboración entre empresas privadas y estatales es crucial”. Esto subraya la necesidad de un esfuerzo coordinado entre todos los actores relevantes para garantizar que las investigaciones puedan llevarse a cabo de manera eficiente y eficaz.

La cooperación limitada entre instituciones locales e internacionales es otro desafío significativo en el combate a los delitos informáticos. Según los entrevistados, “la regulación y la superioridad con el código penal deben estar más integradas a la normatividad nacional”. Esto indica la necesidad de un mayor alineamiento entre las leyes locales y las disposiciones internacionales para garantizar una respuesta más efectiva. Asimismo, se destacó que “las instituciones no responden adecuadamente a las solicitudes de información, lo que dificulta la persecución de los delitos”. Esta falta de coordinación entre entidades clave afecta directamente la capacidad de actuar de manera rápida y eficiente frente a las amenazas cibernéticas, especialmente en casos de delitos transnacionales.

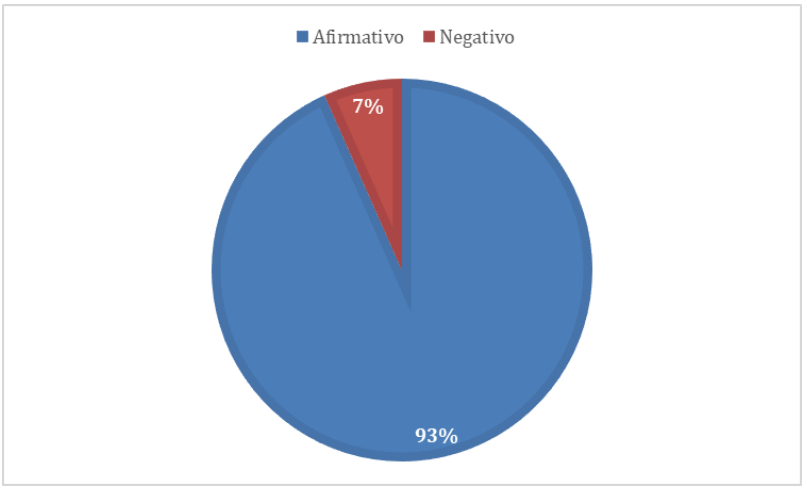
Otro punto mencionado es que “obligar a las empresas a colaborar de manera efectiva es fundamental para combatir los delitos informáticos”. Esto pone en relieve el papel crucial del sector privado en la recopilación de información y pruebas, y

cómo su reticencia a participar puede obstaculizar significativamente las investigaciones.

Por último, se señaló que “la colaboración debe incluir tanto a las empresas privadas como a las estatales, garantizando una respuesta coordinada”. Este enfoque integral permitiría enfrentar de manera más eficaz los desafíos asociados a los delitos informáticos, asegurando que todos los actores relevantes trabajen en conjunto para alcanzar este objetivo común.

Figura 1.

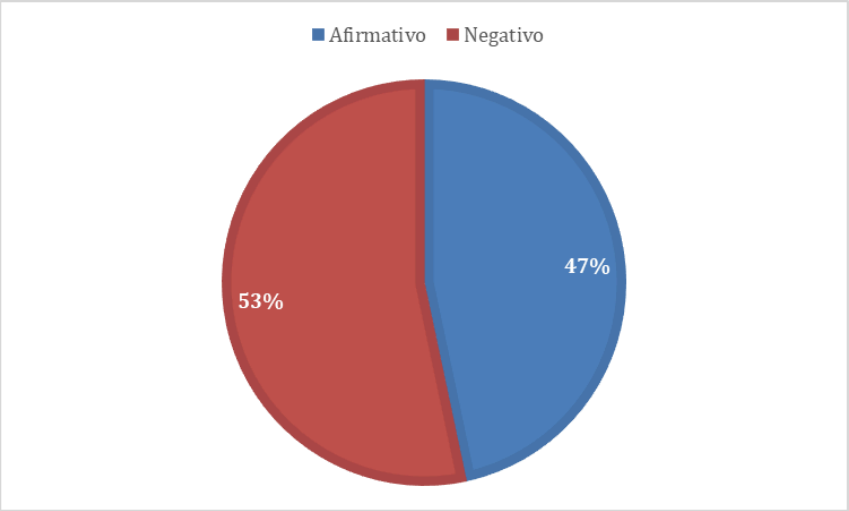
¿Considera usted que existen vacíos en la ley de delitos informáticos del Perú respecto al fraude informático?



El gráfico presentado evidencia que el 93% de los encuestados considera que existen vacíos en la legislación peruana sobre delitos informáticos relacionados con el fraude, mientras que solo el 7% opina lo contrario. Este amplio consenso subraya una percepción generalizada de insuficiencia en las normas actuales para enfrentar de manera efectiva los desafíos del fraude informático. La prevalencia del fraude digital, impulsada por el crecimiento de la tecnología y las transacciones en línea, parece superar la capacidad de la legislación vigente para abordar sus múltiples facetas. Este resultado señala una necesidad urgente de revisión y actualización normativa para cubrir lagunas legales y fortalecer la protección de los ciudadanos y las empresas frente a estos delitos. Asimismo, la percepción del 7% que no observa vacíos podría deberse a una interpretación más optimista o restrictiva de la normativa existente. Sin embargo, la abrumadora mayoría refleja una preocupación crítica sobre la efectividad y alcance de la ley. Esto implica un llamado a las autoridades legislativas para implementar reformas específicas que refuercen la seguridad digital, incluyan sanciones proporcionales y mecanismos preventivos que se adapten a la dinámica cambiante del fraude informático.

Figura 2.

¿Considera usted que existen vacíos en el convenio de Budapest respecto al fraude informático?

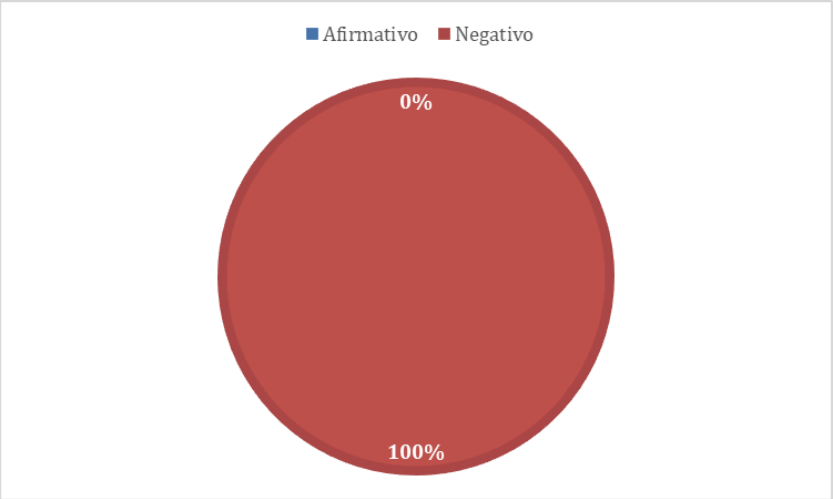


El gráfico muestra las respuestas a la pregunta sobre si existen vacíos en el Convenio de Budapest respecto al fraude informático. Los resultados revelan que el 53% de los encuestados considera que sí existen vacíos en el convenio, mientras que el 47% cree que no. A diferencia del gráfico anterior, donde existía un consenso mayoritario sobre la insuficiencia de la legislación peruana, en este caso, las opiniones están más divididas, aunque prevalece una ligera mayoría que identifica vacíos en el Convenio de Budapest. Este resultado sugiere una percepción crítica sobre la capacidad de dicho convenio para abordar de manera específica y efectiva las particularidades del fraude informático en el contexto global. Aunque el Convenio de Budapest es uno de los principales instrumentos internacionales contra los delitos cibernéticos, la naturaleza evolutiva del fraude digital y las diferencias en la implementación a nivel nacional podrían explicar las percepciones de insuficiencia. Por otro lado, el 47% que no percibe vacíos puede estar asociado a una valoración positiva de la estructura y alcance del convenio, al considerar que cubre de manera adecuada los aspectos esenciales de los delitos cibernéticos. Este contraste subraya la

necesidad de revisar y actualizar el Convenio de Budapest, adaptándolo a los nuevos desafíos tecnológicos y garantizando su efectividad frente al fraude informático.

Figura 3.

¿Considera usted que los policías y fiscales están totalmente preparados para combatir el fraude informático?

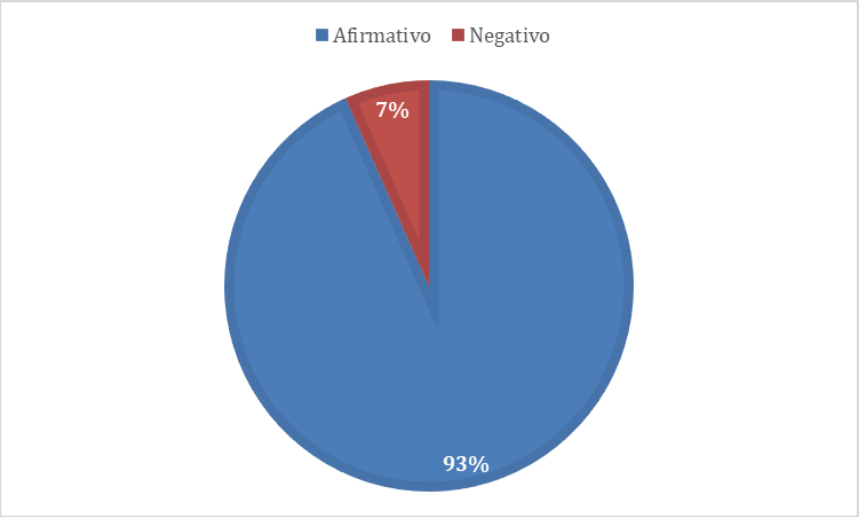


El gráfico refleja las respuestas a la pregunta sobre si policías y fiscales están totalmente preparados para combatir el fraude informático, mostrando que el 100% de los encuestados considera que no están preparados. Este resultado evidencia una preocupación unánime sobre la capacidad de las autoridades encargadas de hacer cumplir la ley para abordar los desafíos del fraude informático. La unanimidad en las respuestas puede deberse a múltiples factores, como la falta de formación especializada, la ausencia de recursos tecnológicos avanzados o la escasa actualización en técnicas modernas de investigación digital. Esto pone en evidencia un vacío crítico en el sistema de justicia penal respecto al tratamiento de delitos informáticos, especialmente en un contexto donde estos delitos crecen exponencialmente. Además, refleja la percepción de que el marco normativo, sin una adecuada capacitación de los operadores de justicia, resulta insuficiente. Este panorama subraya la necesidad urgente de implementar programas de formación

continua y dotar a policías y fiscales de herramientas tecnológicas y conocimientos actualizados. Sin una intervención estratégica, esta brecha de preparación continuará socavando los esfuerzos para combatir eficazmente el fraude informático, lo que podría comprometer la seguridad digital de los ciudadanos y las empresas en un entorno cada vez más interconectado.

Figura 4.

¿Considera usted que es necesario capacitar en forma permanente a los policías y fiscales para combatir con mayor eficacia el fraude informático?



El gráfico evidencia que el 93% de los encuestados considera necesario capacitar de manera permanente a policías y fiscales para combatir con mayor eficacia el fraude informático, mientras que solo el 7% opina lo contrario. Este resultado subraya la importancia que la mayoría de los encuestados otorga a la formación continua como un mecanismo indispensable para enfrentar la creciente complejidad de los delitos cibernéticos. La naturaleza dinámica y en constante evolución del fraude informático requiere que los operadores de justicia cuenten con conocimientos actualizados, habilidades específicas y acceso a herramientas tecnológicas avanzadas que les permitan investigar y procesar estos delitos de manera efectiva.

V.1.3. Objetivo específico 2

La normativa actual presenta una serie de ambigüedades y vacíos legales que complican su aplicación frente a los delitos informáticos. Según los participantes, “no existe forma de identificar de forma inmediata el alcance de la jurisdicción”, lo que evidencia una carencia fundamental en la capacidad de las leyes para responder ante situaciones de carácter transnacional. Este retraso jurisdiccional dificulta la persecución y sanción efectiva de los ciberdelitos, generando un entorno de impunidad que beneficia a los infractores.

Además, los entrevistados señalaron que “existen ambigüedades y vacíos legales, no existe legislación ni regulación clara, como por ejemplo la Ley 30096”. Este comentario refuerza la percepción de que las normativas existentes son insuficientes para abarcar las diversas modalidades delictivas en el ámbito digital. La falta de precisión en las leyes dificulta tanto la investigación como la aplicación de sanciones, dejando a las víctimas desprotegidas ante delitos como la suplantación de identidad.

Otro punto destacado es que “dicho delito conforme a su tipificación sanciona solo si existe algún perjuicio y solo suplantar no es sancionado”. Esto resalta un problema estructural en la normativa, que no considera como delito el acto mismo de suplantar identidad, a menos que exista un daño concreto. Esta limitación permite que los delincuentes actúen con mayor libertad y aprovechen las lagunas legales para evitar consecuencias penales.

Asimismo, se mencionó que “existe un fraude sistemático y las normas extrapenales en delitos informáticos son ineficaces frente a la impunidad delictiva”. Este análisis subraya la urgencia de reformar la legislación actual, incorporando disposiciones claras y específicas que aborden tanto la prevención como la sanción de

estos delitos, asegurando así una mayor protección para los ciudadanos y un marco jurídico sólido.

La regulación de la suplantación de identidad es señalada como uno de los mayores retos en el ámbito de los delitos informáticos. Según los comentarios, “resulta sencillo a través de la IA modificar una foto para suplantar la identidad”. Esto refleja cómo la tecnología, particularmente la inteligencia artificial, se ha convertido en una herramienta poderosa para facilitar este tipo de delitos, poniendo en evidencia la necesidad de una normativa que contemple estas innovaciones.

Otro aspecto señalado es que “la ley no regula sobre las transacciones comerciales de compra y venta por internet, constituyendo una fuente para que se utilice el phishing y el lishing”. Este vacío normativo permite que los delincuentes utilicen estrategias de ingeniería social para engañar a las personas y cometer suplantaciones de identidad con fines económicos, afectando tanto a individuos como a instituciones.

Se subraya también que “por cuanto dicho delito solo será sancionado si resulta algún perjuicio, no tomando como conducta ilícita el solo hecho de suplantar la identidad”. Esto revela que la normativa actual no penaliza preventivamente estas conductas, dejando una ventana abierta para que los delincuentes operen hasta que se produzca un daño material o moral demostrable.

Finalmente, se destaca que “la app de redes sociales no está respetando la privacidad de las personas y vulneran el sistema bancario para cometer delitos informáticos”. Este comentario enfatiza la falta de responsabilidad de las plataformas digitales en proteger la información de los usuarios, lo que facilita la comisión de suplantaciones de identidad y otros delitos relacionados.

El Convenio de Budapest es percibido por los entrevistados como una herramienta limitada en su capacidad para abordar los delitos informáticos. Señalaron que “ya que este convenio no se ajusta en la legislación peruana”, lo que evidencia una desconexión entre las disposiciones internacionales y las normativas locales, dificultando su implementación efectiva en contextos específicos como el peruano.

Además, indicaron que “los ciberdelincuentes utilizando la ingeniería social han traspasado las fronteras por lo que las empresas prestatarias de servicio no cumplen con el convenio”. Esto resalta cómo la falta de cooperación por parte de empresas internacionales afecta la capacidad de las autoridades para perseguir y sancionar delitos transnacionales, reduciendo la eficacia del convenio.

Otro punto relevante es que “para los vacíos de esta ley se tiene que tomar medidas como leyes acordes al tiempo y a forma como los ciberdelincuentes actúan”. Este comentario subraya la necesidad de actualizar el convenio y las normativas relacionadas para adaptarse a las dinámicas actuales del delito digital, incorporando medidas preventivas y sancionatorias más robustas.

Se menciona también que “aún falta mucho más, ya que la información por internet es volátil, eliminable y en muchos de los casos es falsa”. Este desafío técnico pone en evidencia la urgencia de desarrollar protocolos que permitan rastrear y preservar evidencia digital, asegurando que pueda ser utilizada en procesos judiciales de manera efectiva.

La falta de coordinación internacional es un problema señalado como clave para enfrentar los delitos informáticos. Según los entrevistados, “no existe coordinación con otros países”, lo que complica la persecución de delitos transnacionales que involucran múltiples jurisdicciones. Esta ausencia de colaboración limita la capacidad de respuesta de las autoridades y refuerza la impunidad.

Además, destacaron que “las empresas prestatarias de servicio no cumplen con el convenio”, lo que señala una desconexión entre las disposiciones internacionales y la práctica empresarial. La falta de obligatoriedad para que las empresas cooperen con las investigaciones limita la efectividad de las normativas, especialmente en casos de fraude y suplantación de identidad.

Otro aspecto crítico es que “el alcance de la jurisdicción queda rezagada”, lo que pone en evidencia que las normativas no han sido diseñadas para abordar delitos que trascienden fronteras. Esto subraya la necesidad de mecanismos internacionales más eficaces que permitan una acción coordinada entre diferentes países y actores.

Por último, los entrevistados señalaron que “los ciberdelincuentes utilizando la ingeniería social han traspasado las fronteras”, lo que enfatiza cómo las redes digitales han facilitado la expansión de estos delitos, desafiando las capacidades actuales de las autoridades para controlarlos. Esto refuerza la importancia de adoptar enfoques globales en la lucha contra los delitos informáticos.

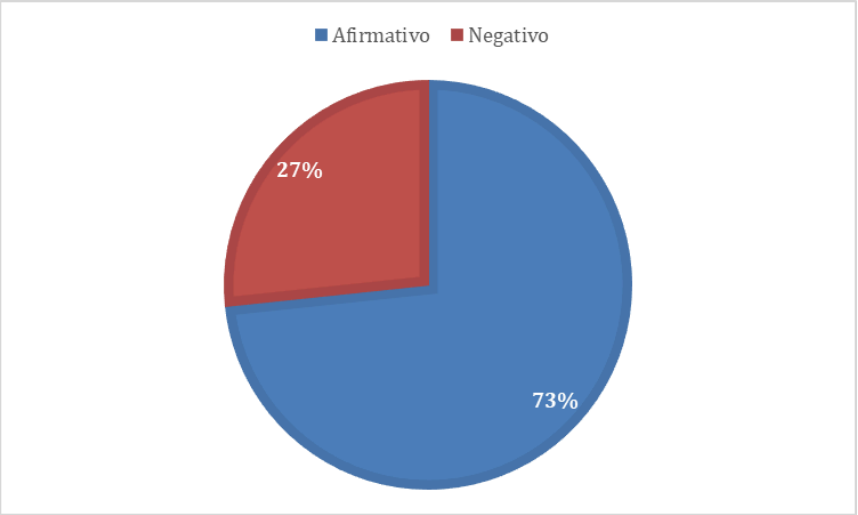
Los participantes destacaron varias propuestas para mejorar la normativa vigente y abordar los vacíos existentes. Indicaron que “se tienen que tomar medidas como leyes acordes al tiempo y a forma como los ciberdelincuentes actúan”. Esto sugiere que las normativas deben evolucionar al mismo ritmo que las estrategias utilizadas por los delincuentes, priorizando la agilidad y adaptabilidad.

Se mencionó también que “la ley penal en blanco no es efectiva en términos del tratamiento jurídico penal”. Esto indica que las leyes actuales, al carecer de especificidad, no logran responder adecuadamente a la complejidad de los delitos digitales. Una reforma que establezca disposiciones más claras y detalladas podría mejorar significativamente su eficacia. Otro comentario relevante es que “existe una dejadez y lentitud en la adaptación de la ley a la realidad cibernética”. Esto refleja la

necesidad de priorizar la actualización normativa como una estrategia para enfrentar las amenazas emergentes, asegurando que las leyes estén alineadas con las necesidades actuales. Finalmente, se señaló que “resulta sencillo a través de la IA modificar una foto para suplantar la identidad”. Esto pone en evidencia cómo las tecnologías emergentes están siendo utilizadas para cometer delitos, lo que resalta la urgencia de regular su uso y prevenir que sean herramientas al servicio de la criminalidad.

Figura 5.

¿Considera usted que existen vacíos en la ley de delitos informáticos del Perú, respecto a la suplantación de identidad?

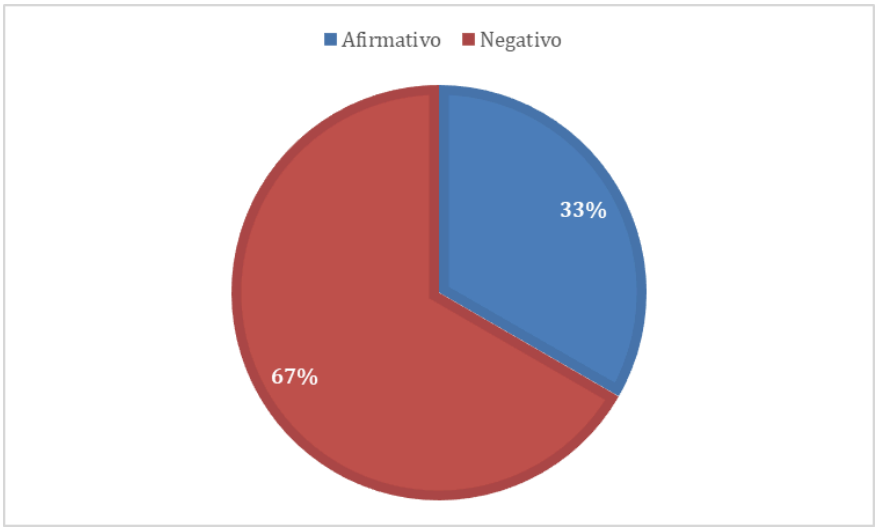


El gráfico muestra que el 73% de los encuestados considera que existen vacíos en la ley de delitos informáticos del Perú en relación con la suplantación de identidad, mientras que el 27% opina que no. Este resultado pone en evidencia que una amplia mayoría percibe insuficiencias legales para abordar de manera adecuada este tipo de delito, que ha ganado relevancia en el contexto digital actual. La suplantación de identidad es una práctica cada vez más frecuente que afecta tanto a individuos como a instituciones, generando consecuencias legales, financieras y reputacionales significativas. La percepción del 27% que no identifica vacíos podría derivar de una falta de conocimiento sobre los desafíos técnicos y legales que implica abordar este delito o de una confianza en las disposiciones actuales. Sin embargo, la mayoría refleja una preocupación legítima que sugiere la necesidad de una revisión de la normativa vigente, incluyendo medidas específicas para prevenir, investigar y sancionar este tipo de conductas. Este análisis subraya la importancia de actualizar el marco legal, incorporando aspectos como la definición clara de suplantación de

identidad, sanciones proporcionales y estrategias de cooperación internacional para combatir este delito.

Figura 6.

¿Considera usted que existen vacíos en el convenio de Budapest respecto a la suplantación de identidad?

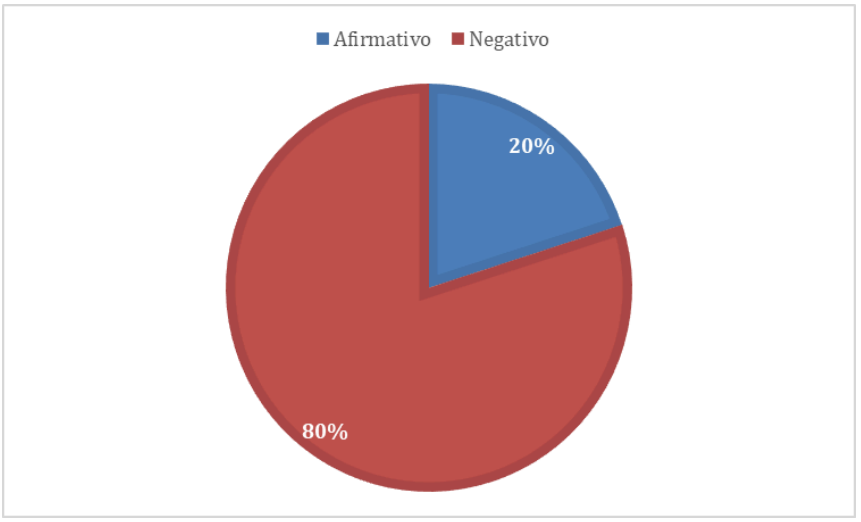


El gráfico muestra que el 67% de los encuestados considera que existen vacíos en el Convenio de Budapest respecto a la suplantación de identidad, mientras que el 33% opina que no. Este resultado indica que una mayoría significativa percibe que el Convenio de Budapest, aunque diseñado como un marco global contra los delitos cibernéticos, no aborda de manera suficiente o específica los desafíos asociados a la suplantación de identidad en un entorno digital. Este delito, caracterizado por el uso indebido de información personal para obtener beneficios ilegítimos, representa una amenaza creciente en la era digital. La percepción del 33% que no identifica vacíos podría interpretarse como una valoración positiva del alcance general del convenio, el cual establece principios básicos aplicables a diversos delitos informáticos. Sin embargo, la mayoría destaca una brecha en la capacidad del convenio para adaptarse a los delitos emergentes como la suplantación de identidad, lo que subraya la necesidad de una revisión y actualización. Esto podría incluir definiciones claras, protocolos de

cooperación internacional más específicos y herramientas legales mejoradas para su persecución.

Figura 7.

¿Considera usted que los policías y fiscales están totalmente preparados para combatir la suplantación de identidad?

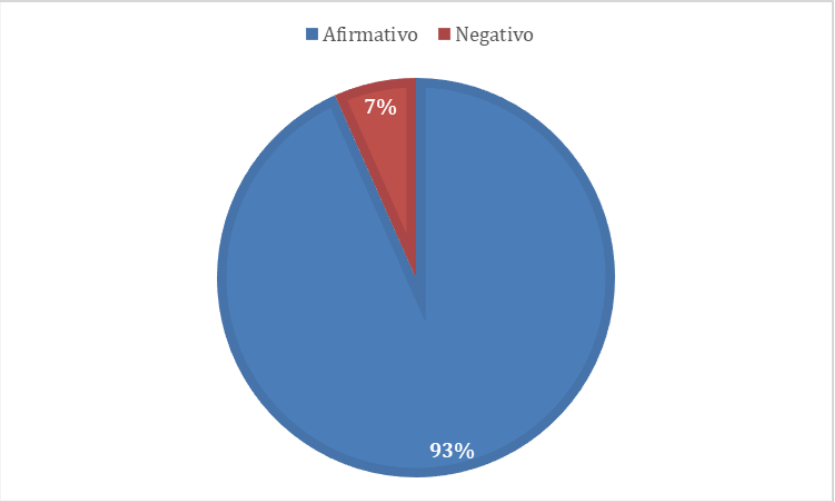


El gráfico revela que el 80% de los encuestados considera que policías y fiscales no están totalmente preparados para combatir la suplantación de identidad, mientras que solo el 20% cree que sí lo están. Este resultado evidencia una percepción mayoritaria de insuficiencia en las capacidades institucionales para enfrentar este delito, el cual ha ganado relevancia en la era digital debido a su impacto directo en la privacidad y la seguridad de los ciudadanos. La falta de preparación puede atribuirse a una capacitación inadecuada en aspectos tecnológicos, a recursos insuficientes para la investigación digital y a la ausencia de protocolos específicos para manejar casos de suplantación de identidad. Por otro lado, el 20% que opina afirmativamente podría reflejar confianza en esfuerzos recientes o iniciativas aisladas, aunque esta percepción positiva representa una clara minoría. Este panorama subraya la necesidad de implementar estrategias que fortalezcan las competencias de policías y fiscales

mediante programas de formación especializada, acceso a herramientas tecnológicas avanzadas y cooperación internacional en la persecución de estos delitos.

Figura 8.

¿Considera usted que es necesario capacitar en forma permanente a los policías y fiscales para combatir con mayor eficacia la suplantación de identidad?



El gráfico refleja que el 93% de los encuestados considera necesaria la capacitación permanente de policías y fiscales para combatir con mayor eficacia la suplantación de identidad, mientras que solo el 7% no lo considera necesario. Este resultado destaca un consenso mayoritario respecto a la importancia de fortalecer continuamente las competencias de los operadores de justicia en un entorno donde los delitos digitales, como la suplantación de identidad, evolucionan constantemente. La capacitación permanente es percibida como un mecanismo clave para dotar a policías y fiscales de conocimientos actualizados, herramientas tecnológicas avanzadas y estrategias legales efectivas que les permitan enfrentar estos delitos de manera proactiva y eficiente. El reducido 7% que no considera esta capacitación esencial podría reflejar una percepción optimista o una falta de conciencia sobre la complejidad de la suplantación de identidad y su impacto en la seguridad digital. Sin

embargo, la amplia mayoría indica la necesidad de priorizar la inversión en programas formativos especializados que aborden las dinámicas cambiantes de este delito.

V.1.4. Objetivo específico 3

La suplantación de identidad utilizando herramientas como la inteligencia artificial (IA) ha emergido como una de las principales preocupaciones en el ámbito de los delitos informáticos. Según los participantes, "el actual proponente utilice una IA para generarse un avatar con el cual se haga pasar por otro niño". Este escenario ilustra cómo la tecnología puede ser manipulada para facilitar delitos graves, especialmente aquellos dirigidos a menores de edad, sin que la normativa contemple mecanismos específicos para abordar estas situaciones.

Otro aspecto clave señalado es que "la ley no regula de manera clara el supuesto en el cual puede comprobarse dicho delito, se utilizan términos genéricos de 'connotación sexual'". La falta de claridad en la tipificación de estos delitos deja espacio para interpretaciones ambiguas, dificultando la labor de las autoridades judiciales y permitiendo que los ciberdelincuentes actúen con mayor libertad. Esto pone en evidencia la necesidad de una legislación que precise los elementos configurativos del delito para garantizar su efectiva aplicación. Asimismo, se mencionó que "debido a la interpretación judicial existen problemas y no se evalúa pertinentemente el grado de vinculación de las decisiones judiciales". Este comentario destaca cómo la falta de estandarización en la interpretación de las normas puede llevar a decisiones contradictorias, limitando la efectividad de las resoluciones judiciales en casos de suplantación de identidad.

Los entrevistados señalaron que "la ley no precisa claramente su configuración de qué manera la actividad sexual se da directa o física". Este vacío legislativo representa un desafío adicional en la persecución de delitos relacionados con la

suplantación de identidad, especialmente aquellos con fines de explotación sexual, evidenciando la necesidad de ajustar la normativa para abarcar estas conductas emergentes. El tratamiento legal de los delitos cibernéticos contra menores presenta múltiples deficiencias que dificultan su efectiva persecución. Según los participantes, "en este caso no hay más información de los IPs de conexión", lo que resalta cómo la volatilidad de la evidencia digital complica la identificación y localización de los responsables. Esto subraya la necesidad de protocolos que obliguen a las empresas tecnológicas a proporcionar datos de conexión de manera rápida y efectiva. Además, se indicó que "las empresas de páginas web, juegos en red, redes sociales no tienen regulación acorde al Convenio de Budapest". Este vacío normativo refuerza la percepción de que las plataformas digitales no están obligadas a colaborar con las autoridades en la protección de menores, lo que favorece la proliferación de delitos como el grooming y la explotación sexual.

Otro problema señalado es que "la ley no regula de manera clara el supuesto en el cual puede comprobarse dicho delito, se utilizan términos genéricos de 'connotación sexual'". Esto genera dificultades tanto en la investigación como en el enjuiciamiento, ya que las definiciones vagas permiten que las conductas delictivas pasen inadvertidas o no sean sancionadas adecuadamente. Los entrevistados subrayaron que "se debía formar otro convenio de esa magnitud al fin de salvaguardar el interés superior de los niños y adolescentes por medios tecnológicos". Esto evidencia la urgencia de actualizar tanto las normativas nacionales como los tratados internacionales para abordar las nuevas formas de victimización en línea. Los adolescentes mayores de 14 años enfrentan vacíos legales que los dejan desprotegidos frente a ciertos delitos cibernéticos. Los entrevistados afirmaron que "solo se considera a menores de 14 años, mas no en menores de 18 años". Este enfoque

limitado excluye a un grupo vulnerable, ignorando la realidad de que los adolescentes también son frecuentemente víctimas de delitos en entornos digitales.

Se destacó que “la ley no regula claramente su configuración de qué manera la actividad sexual se da directa o física”. Este comentario resalta la falta de especificidad en la legislación, que no contempla las diversas formas en que puede manifestarse el abuso sexual, ya sea en contextos físicos o virtuales. Esta ambigüedad limita la capacidad de las autoridades para sancionar estas conductas de manera efectiva. Otro punto relevante es que “regular las redes sociales para proteger a las niñas y niños de los pedófilos cibernéticos” es una necesidad urgente. La falta de control sobre estas plataformas permite que los delincuentes utilicen redes sociales, juegos en línea y otras herramientas digitales para explotar a menores, sin que existan mecanismos efectivos para prevenir o sancionar estas acciones. Se señaló que “las empresas de páginas web, juegos en red y redes sociales no tienen regulación acorde al Convenio de Budapest”. Esto evidencia que, aunque existen acuerdos internacionales, su implementación es limitada, dejando vacíos en la protección de adolescentes frente a delitos cibernéticos.

La falta de coordinación entre países y empresas tecnológicas es otro desafío importante en la lucha contra los delitos cibernéticos. Según los entrevistados, “no existe coordinación con otros países”, lo que dificulta la persecución de delitos transnacionales, especialmente aquellos que involucran la explotación de menores. Este comentario pone en evidencia la necesidad de fortalecer la cooperación internacional para abordar estas problemáticas. Asimismo, se mencionó que “las empresas de redes sociales no respetan la privacidad de las personas y vulneran el sistema bancario para cometer delitos informáticos”. Este escenario refleja cómo la ausencia de regulaciones específicas para las plataformas digitales permite que estas

sean utilizadas como herramientas para cometer delitos, afectando tanto a menores como a adultos.

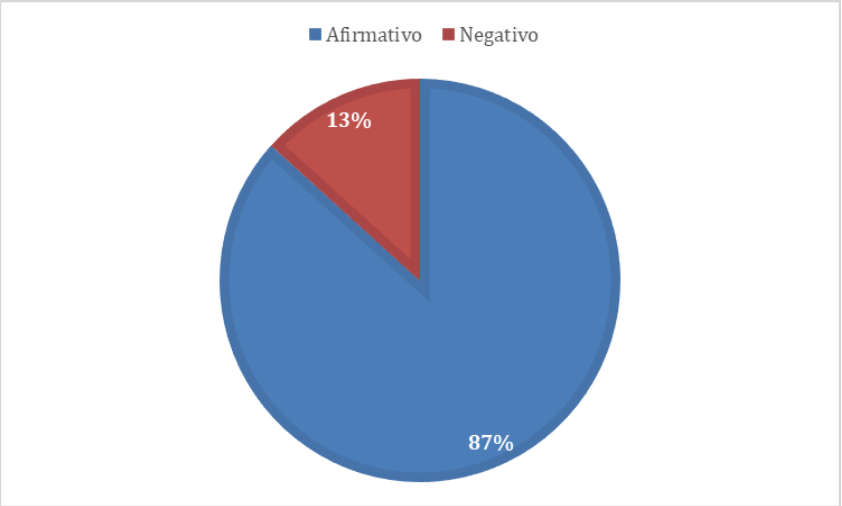
Se destacó también que “en este caso no hay más información de los IPs de conexión”, lo que subraya la importancia de obligar a las empresas a proporcionar datos clave para las investigaciones. La falta de acceso rápido y confiable a esta información limita la capacidad de las autoridades para actuar de manera efectiva. Se indicó que “se debía formar otro convenio de esa magnitud al fin de salvaguardar el interés superior de los niños y adolescentes por medios tecnológicos”. Este llamado resalta la necesidad de acuerdos internacionales más específicos y adaptados a las dinámicas actuales, que obliguen a las empresas a colaborar activamente en la protección de menores.

Los participantes propusieron varias medidas para mejorar la normativa actual y abordar los vacíos legales existentes. Indicaron que “considero que para poder investigar esta legislación debería ser más drástica ya que conforme abarca la ciberdelincuencia”. Esto pone en relieve la necesidad de normativas más estrictas y específicas para enfrentar la complejidad de los delitos digitales. También señalaron que “regular las redes sociales para proteger a las niñas y niños de los pedófilos cibernéticos” es esencial. Esta propuesta destaca la urgencia de establecer controles más rigurosos sobre las plataformas digitales, obligándolas a implementar medidas de seguridad que protejan a los menores de conductas delictivas. Además, se indicó que “se debía formar otro convenio de esa magnitud al fin de salvaguardar el interés superior de los niños y adolescentes por medios tecnológicos”. Este comentario resalta la importancia de crear acuerdos internacionales que consideren las particularidades de cada país y aborden de manera integral los delitos contra menores en entornos digitales.

Finalmente, los entrevistados afirmaron que “en este caso no hay más información de los IPs de conexión”, lo que pone de manifiesto la necesidad de implementar protocolos claros que obliguen a las empresas tecnológicas a proporcionar datos relevantes para las investigaciones, garantizando una respuesta efectiva frente a los delitos cibernéticos.

Figura 9.

¿Considera usted que existen vacíos en la ley de delitos informáticos del Perú, respecto a las proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos?

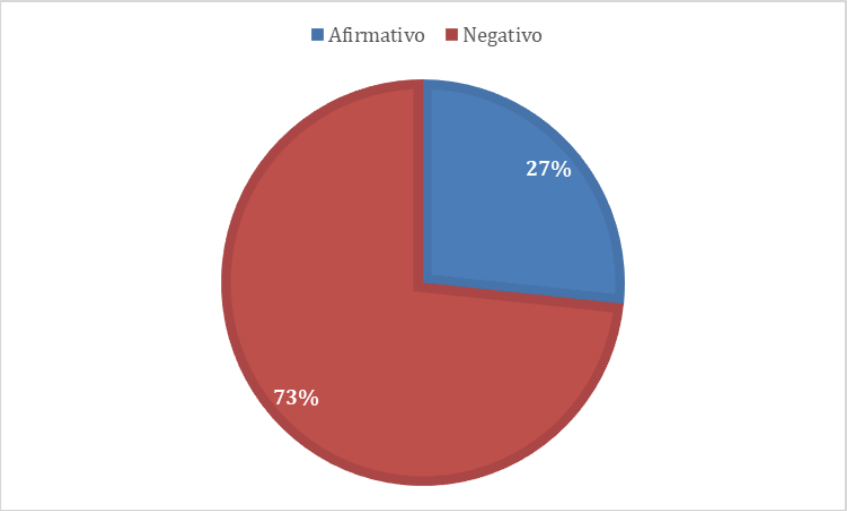


El gráfico evidencia que el 87% de los encuestados considera que existen vacíos en la ley de delitos informáticos del Perú respecto a las proposiciones con fines sexuales dirigidas a niños, niñas y adolescentes a través de medios tecnológicos, mientras que solo el 13% opina lo contrario. Este resultado destaca una percepción mayoritaria de insuficiencia en el marco legal actual para abordar este tipo de delitos, comúnmente asociados al grooming y otras formas de explotación sexual facilitadas por la tecnología. La preocupación expresada por los encuestados refleja la creciente incidencia de estas conductas y la necesidad de una legislación más robusta y específica que no solo contemple sanciones adecuadas, sino también medidas preventivas y de protección para las víctimas potenciales. El 13% que no percibe

vacíos en la normativa podría estar relacionado con un desconocimiento de las particularidades legales necesarias para abordar este problema o con una confianza en la capacidad actual del sistema legal. Sin embargo, la abrumadora mayoría subraya la urgencia de revisar y actualizar las leyes para adaptarse a los riesgos asociados a las nuevas tecnologías.

Figura 10.

¿Considera usted que existen vacíos en el convenio de Budapest respecto a las proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos?

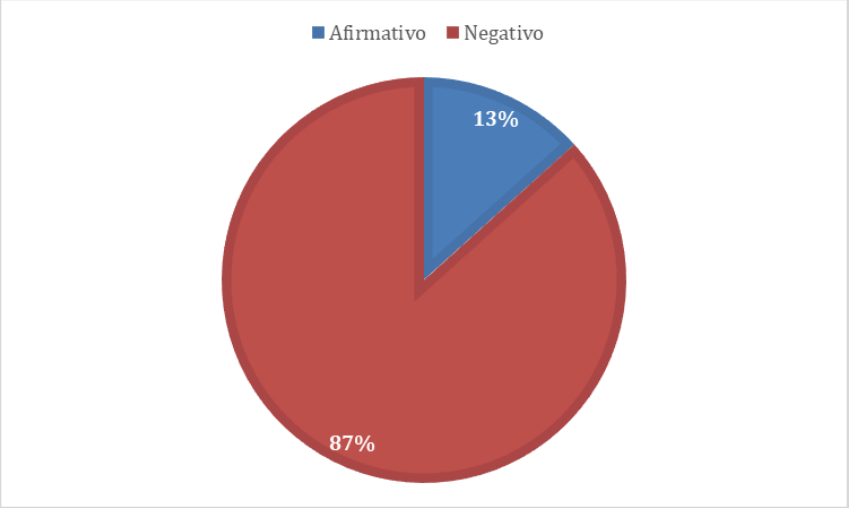


El gráfico refleja que el 73% de los encuestados considera que existen vacíos en el Convenio de Budapest respecto a las proposiciones con fines sexuales dirigidas a niños, niñas y adolescentes a través de medios tecnológicos, mientras que el 27% opina que no. Este resultado evidencia una percepción mayoritaria de insuficiencia en el marco normativo internacional para abordar delitos como el grooming, que se ha intensificado con el avance de la tecnología. Aunque el Convenio de Budapest es una herramienta clave para la cooperación internacional en delitos cibernéticos, esta percepción sugiere que no se ha adaptado completamente a los desafíos específicos que plantea la protección de menores en el entorno digital. El 27% que no identifica vacíos podría argumentar que las disposiciones generales del convenio son suficientes

para abordar estos casos o confiar en las implementaciones nacionales derivadas del convenio. Sin embargo, el 73% resalta la necesidad de incluir cláusulas más explícitas que contemplen este tipo de delitos, así como protocolos claros de prevención, persecución y cooperación entre países.

Figura 11.

¿Considera usted que los policías y fiscales están totalmente preparados para combatir las proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos?

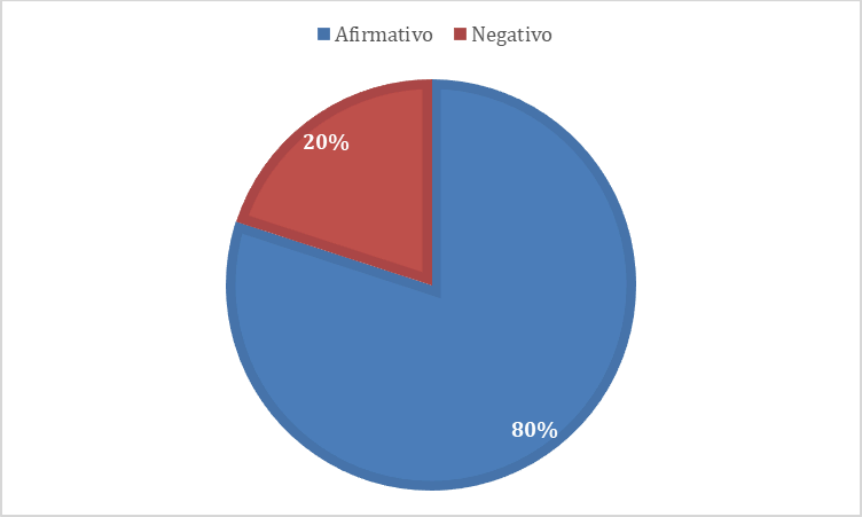


El gráfico muestra que el 87% de los encuestados considera que los policías y fiscales no están totalmente preparados para combatir las proposiciones con fines sexuales dirigidas a niños, niñas y adolescentes a través de medios tecnológicos, mientras que solo el 13% opina lo contrario. Este resultado refleja una percepción generalizada de que las capacidades actuales de las fuerzas del orden y del sistema judicial son insuficientes para enfrentar eficazmente este tipo de delito, que se ha incrementado con el auge de las plataformas digitales. La falta de preparación puede atribuirse a la limitada formación en herramientas tecnológicas avanzadas, la ausencia de protocolos especializados y una capacitación inadecuada para abordar estos delitos de manera integral. El reducido porcentaje de respuestas afirmativas podría indicar que existen sectores donde se perciben esfuerzos aislados o recientes para mejorar

estas capacidades. Sin embargo, la gran mayoría destaca una necesidad crítica de fortalecer las competencias de policías y fiscales mediante programas de formación continua, equipamiento tecnológico adecuado y estrategias de cooperación internacional para la investigación y sanción de estos crímenes.

Figura 12.

¿Considera usted que es necesario capacitar en forma permanente a los policías y fiscales para combatir con mayor eficacia las proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos?



El gráfico muestra que el 80% de los encuestados considera necesaria la capacitación permanente de policías y fiscales para combatir con mayor eficacia las proposiciones con fines sexuales dirigidas a niños, niñas y adolescentes a través de medios tecnológicos, mientras que el 20% opina que no es necesario. Este resultado refleja una percepción mayoritaria sobre la importancia de fortalecer continuamente las competencias de los operadores de justicia frente a los desafíos tecnológicos que presentan este tipo de delitos, conocidos como *grooming* u otras formas de explotación sexual en línea. La proporción significativa que aboga por la capacitación subraya la necesidad de dotar a las autoridades de herramientas actualizadas, conocimientos especializados y estrategias efectivas para la prevención, detección e

investigación de estas actividades ilícitas. Por otro lado, el 20% que no considera esencial esta capacitación podría reflejar un desconocimiento de la magnitud y complejidad del problema o una sobrevaloración de los recursos ya existentes. Sin embargo, la clara mayoría evidencia que la capacitación permanente no solo es necesaria, sino urgente, especialmente en un entorno digital que evoluciona rápidamente.

CAPÍTULO VI
DISCUSIÓN DE RESULTADOS

Objetivo específico 1: Analizar los vacíos en la legislación peruana y en el Convenio de Budapest respecto al fraude informático

El 93% de los encuestados identificó vacíos en la legislación peruana sobre fraude informático, señalando una percepción mayoritaria de insuficiencia normativa. Esta situación encuentra respaldo en Huaman (2020), quien destacó que, aunque la Ley 30096 representa un avance, no logra abordar completamente los delitos emergentes debido a su limitada capacidad de adaptación frente a la evolución tecnológica. Asimismo, Ayma (2020) argumenta que las fiscalías no están debidamente capacitadas para aplicar las disposiciones existentes, lo que exacerba la problemática al dificultar la persecución penal de los delitos. Por otro lado, el 7% que no percibe vacíos podría estar asociado a los avances señalados por Vitteri (2022), quien sostiene que la normativa peruana es un punto de partida sólido para futuras mejoras. Sin embargo, estas percepciones optimistas contrastan con el consenso general que exige reformas integrales y mecanismos más efectivos de sanción. La complejidad de los fraudes digitales, caracterizados por su alcance transnacional y el uso de tecnologías avanzadas, pone en evidencia que la legislación actual es insuficiente para abarcar todas las facetas de este tipo de delitos. Esto subraya la necesidad de integrar perspectivas globales y locales, garantizando un marco normativo flexible y actualizado que permita prevenir y sancionar estas conductas ilícitas de manera eficaz.

Respecto al Convenio de Budapest, el 53% de los encuestados considera que presenta vacíos en relación con el fraude informático, una opinión que refleja críticas similares a las mencionadas por Campina y Rodrigues (2022). Según estos autores,

aunque el convenio es un marco relevante, sus disposiciones requieren actualizaciones para incluir modalidades delictivas más recientes, como el phishing avanzado y el fraude financiero digital. Este análisis resalta la falta de especificidad en ciertos artículos del convenio, lo que dificulta su implementación efectiva en países como Perú. En contraste, el 47% que no identifica vacíos podría asociarse con las observaciones de Spiezia (2022), quien destaca el impacto positivo del Protocolo II, adoptado en 2021, al fortalecer la cooperación internacional y los mecanismos de protección de víctimas. Sin embargo, la división de opiniones evidencia que, aunque el convenio es considerado un avance importante, no logra adaptarse completamente a los desafíos tecnológicos actuales. Esto se agrava por la diversidad de realidades nacionales, donde las brechas tecnológicas y la falta de armonización legislativa limitan su aplicabilidad. Los resultados sugieren que, para maximizar su eficacia, el convenio debe incorporar enfoques más inclusivos y dinámicos que respondan a las necesidades específicas de cada región, priorizando el combate al fraude informático en un entorno globalizado.

La falta de preparación de policías y fiscales para combatir el fraude informático es una preocupación unánime entre los encuestados, reflejada en el 100% de respuestas negativas. Esto coincide con los hallazgos de Ayma (2020), quien identificó una brecha significativa en la formación de los operadores del sistema judicial, especialmente en el manejo de pruebas digitales y técnicas investigativas avanzadas. Este déficit de capacitación también es señalado por Fuentes (2021), quien enfatiza la necesidad de formar a las autoridades en el uso de herramientas tecnológicas específicas para abordar delitos como el phishing y el pharming. La carencia de recursos especializados y la falta de protocolos efectivos para manejar estos casos limitan la capacidad de respuesta del sistema de justicia. Además, la

evolución constante de las estrategias delictivas digitales requiere que las autoridades estén en constante actualización, algo que, según Vitteri (2022), solo puede lograrse mediante la creación de fiscalías especializadas. Estas fiscalías no solo deberían centrarse en la persecución de delitos, sino también en la prevención y en el fortalecimiento de las capacidades operativas mediante programas de formación continua. La ausencia de estas medidas genera un entorno donde los delincuentes tienen mayor margen de maniobra, lo que compromete tanto la seguridad digital como la confianza en las instituciones encargadas de protegerla.

El 93% que aboga por la capacitación continua de las autoridades destaca la relevancia de invertir en programas de formación especializada para enfrentar los desafíos dinámicos de la ciberdelincuencia. Esta necesidad es respaldada por Nguyen et al. (2022), quienes proponen enfoques adaptativos y flexibles para mejorar la gestión del ciberespacio y la efectividad en la lucha contra delitos digitales. Además, Huaman (2020) subraya que la cooperación internacional debe complementarse con esfuerzos locales que fortalezcan las competencias técnicas y legales de los operadores del sistema de justicia. Las herramientas tecnológicas avanzadas, combinadas con un conocimiento profundo de las dinámicas del fraude digital, son esenciales para garantizar investigaciones efectivas y sanciones proporcionales. Asimismo, la implementación de programas de capacitación debería estar acompañada de una revisión normativa que incorpore nuevas modalidades delictivas y adapte las sanciones a la gravedad de los delitos. Este enfoque integral no solo mejoraría la capacidad de las autoridades para actuar, sino que también aumentaría la confianza ciudadana en la capacidad del sistema legal para proteger sus derechos en el entorno digital.

En conjunto, estos resultados subrayan una desconexión crítica entre el avance de la ciberdelincuencia y la capacidad del marco normativo y operativo para contrarrestarla. Investigaciones como las de Ortiz (2019) y Sanmartin (2021) destacan que, aunque existen avances legislativos, las brechas en la implementación y la falta de armonización con estándares internacionales limitan la efectividad de las leyes. La integración de perspectivas internacionales, como las promovidas por el Convenio de Budapest, es crucial para cerrar estas brechas. Sin embargo, también es fundamental que las disposiciones globales se adapten a los contextos nacionales, garantizando que las normativas sean relevantes y aplicables. Esto requiere un enfoque colaborativo entre gobiernos, sector privado y organismos internacionales, priorizando tanto la prevención como la persecución efectiva del fraude informático. La implementación de estrategias de capacitación continua, junto con reformas legislativas específicas, representa un camino viable para fortalecer la respuesta frente a esta problemática, promoviendo un entorno digital más seguro y equitativo.

Objetivo específico 2: Identificar vacíos en la legislación peruana y el Convenio de Budapest respecto a la suplantación de identidad

El 73% de los encuestados percibe vacíos en la normativa peruana en relación con la suplantación de identidad, lo que subraya una preocupación generalizada sobre la insuficiencia legal para abordar esta problemática. Este resultado se alinea con Fuentes (2021), quien resalta que delitos como el phishing y el carding no están suficientemente tipificados en la Ley 30096, dificultando su adecuada persecución. A pesar de algunos avances legislativos destacados por Villareal (2020), quien menciona una coincidencia significativa entre la normativa peruana y el Convenio de Budapest, los encuestados parecen considerar que estos no son suficientes para abarcar la complejidad de las modalidades actuales de suplantación de identidad. Este delito,

facilitado por tecnologías emergentes como la inteligencia artificial, plantea desafíos que no están debidamente contemplados en las leyes vigentes. La falta de sanciones claras y la limitada capacidad para rastrear e identificar a los perpetradores refuerzan la percepción de que las disposiciones legales actuales son inadecuadas. Esto resalta la necesidad urgente de reformas legislativas que incluyan definiciones precisas del delito, así como mecanismos tecnológicos y legales para su prevención y sanción efectiva.

En relación con el Convenio de Budapest, el 67% de los encuestados considera que no aborda suficientemente la suplantación de identidad, lo que pone en evidencia una percepción crítica sobre su capacidad para adaptarse a los delitos emergentes. Esta opinión coincide con Campina y Rodrigues (2022), quienes argumentan que el convenio necesita actualizaciones para abarcar modalidades delictivas específicas, como la suplantación de identidad en entornos digitales. Aunque el convenio establece principios generales aplicables a varios delitos cibernéticos, su falta de detalle en ciertos aspectos limita su efectividad en contextos como el peruano. Sin embargo, el 33% que no identifica vacíos podría reflejar una valoración positiva de avances como el Protocolo II, señalado por Spiezia (2022) como un paso importante hacia una mayor cooperación internacional y la mejora de los marcos normativos nacionales. La división de opiniones sugiere que, aunque el convenio proporciona una base útil, su implementación y alcance podrían beneficiarse de una mayor especificidad y adaptabilidad a las necesidades locales.

El 80% que considera que las autoridades no están preparadas para combatir la suplantación de identidad refleja una realidad que también fue observada por Ayma (2020), quien destacó deficiencias en la capacitación de fiscales y policías en la gestión de pruebas digitales y técnicas de investigación. Esta falta de preparación se

traduce en una capacidad limitada para manejar casos complejos, lo que afecta negativamente la eficacia del sistema judicial. De manera similar, Vitteri (2022) resalta la necesidad de crear fiscalías especializadas para enfrentar delitos como la suplantación de identidad, asegurando un enfoque integral que incluya no solo la persecución del delito, sino también su prevención. La ausencia de formación específica no solo limita la capacidad de respuesta de las autoridades, sino que también refuerza la percepción de impunidad, debilitando la confianza de la ciudadanía en el sistema legal. Esto subraya la importancia de invertir en programas de capacitación que permitan a las autoridades desarrollar habilidades técnicas y legales para abordar los desafíos asociados a este tipo de delitos.

El consenso del 93% sobre la necesidad de capacitación permanente resalta la importancia de fortalecer las competencias de los operadores de justicia para enfrentar de manera efectiva los delitos relacionados con la suplantación de identidad. Nguyen et al. (2022) argumentan que los enfoques flexibles y adaptativos son esenciales para mejorar la gestión del ciberespacio, permitiendo a las autoridades mantenerse al día con la evolución de las amenazas digitales. Esta necesidad también es destacada por Huaman (2020), quien enfatiza que la cooperación internacional debe complementarse con esfuerzos nacionales para garantizar la formación continua de las autoridades. Además, las recomendaciones de Campina y Rodrigues (2022) sobre la importancia de la cooperación transnacional y la implementación de protocolos específicos encuentran eco en estos resultados, que subrayan la necesidad de un enfoque integral. Esto incluye no solo la capacitación en el manejo de pruebas digitales, sino también la creación de marcos normativos claros y adaptados que permitan abordar la suplantación de identidad desde una perspectiva preventiva y sancionatoria.

En resumen, los resultados reflejan una brecha significativa entre las capacidades actuales y los desafíos que plantea la suplantación de identidad en entornos digitales. Si bien investigaciones como las de Villareal (2020) y Fuentes (2021) destacan avances legislativos, la percepción generalizada de insuficiencia normativa y operativa subraya la necesidad de implementar reformas integrales. Estas deben incluir la actualización de la Ley 30096 para abordar modalidades delictivas emergentes y la revisión del Convenio de Budapest para adaptarlo a contextos nacionales específicos. Además, la creación de fiscalías especializadas y programas de capacitación continua se presentan como estrategias clave para fortalecer la capacidad del sistema de justicia. Este enfoque debe combinarse con iniciativas de cooperación internacional que permitan un intercambio efectivo de información y recursos, asegurando una respuesta coordinada frente a los desafíos que plantea la suplantación de identidad en un entorno digital en constante cambio.

Objetivo específico 3: Evaluar la efectividad de la legislación peruana y el Convenio de Budapest frente a proposiciones sexuales a menores por medios tecnológicos

El 87% de los encuestados considera que la legislación peruana presenta vacíos significativos respecto a las proposiciones sexuales a menores por medios tecnológicos, un resultado que coincide con los hallazgos de Alatrista y Magariño (2021). Estos autores destacan que el marco normativo actual no ha evolucionado al ritmo de los delitos cibernéticos que vulneran los derechos fundamentales de los menores. De manera similar, Fuentes (2021) señala que la Ley 30096, aunque progresiva, no contempla adecuadamente delitos específicos como el grooming. Por otro lado, el 13% que no identifica vacíos podría estar relacionado con una percepción optimista de los avances legislativos resaltados por Huaman (2020), quien argumenta

que la normativa peruana ha mostrado un desarrollo significativo en los últimos años. Sin embargo, la mayoría de los encuestados refleja una preocupación legítima sobre la falta de especificidad en la legislación para abordar delitos que afectan directamente a los menores. Esto subraya la necesidad de reforzar la normativa con disposiciones que incluyan definiciones claras, sanciones proporcionales y estrategias preventivas que protejan a las víctimas potenciales.

En cuanto al Convenio de Budapest, el 73% de los encuestados percibe vacíos significativos en su capacidad para abordar las proposiciones sexuales a menores por medios tecnológicos. Este resultado se alinea con las observaciones de Sanmartin (2021), quien destacó que la normativa ecuatoriana aún no cumple plenamente con los estándares del convenio, lo que limita su eficacia frente a delitos como el grooming. De manera similar, Campina y Rodrigues (2022) señalan que el convenio necesita ser actualizado para abordar con mayor especificidad las amenazas emergentes en el entorno digital. Sin embargo, el 27% que no percibe vacíos podría relacionarse con la apreciación de Spiezia (2022), quien subraya que el Protocolo II del Convenio de Budapest ha mejorado las capacidades de cooperación internacional y podría servir como una herramienta eficaz para fortalecer los marcos legales nacionales. Este contraste en las percepciones destaca la importancia de ajustar el convenio a las dinámicas locales y garantizar que contemple delitos específicos que afectan a los menores, incluyendo la implementación de protocolos claros de prevención y persecución.

El 87% de los encuestados que considera que policías y fiscales no están totalmente preparados para manejar estos casos refleja una problemática recurrente identificada por Ayma (2020), quien enfatiza la falta de formación en el manejo de evidencias digitales y técnicas investigativas específicas. Esta percepción se refuerza

con los hallazgos de Vitteri (2022), quien propone la creación de fiscalías especializadas como una estrategia esencial para enfrentar delitos cibernéticos complejos. La falta de preparación de las autoridades no solo limita su capacidad para investigar y sancionar estos delitos, sino que también reduce la confianza de la ciudadanía en la capacidad del sistema judicial para proteger a los menores. Este resultado subraya la urgencia de implementar programas de capacitación especializada que doten a las autoridades de herramientas y conocimientos actualizados. Además, Nguyen et al. (2022) destacan que los enfoques adaptativos y flexibles en la gestión del ciberespacio son esenciales para mejorar la efectividad de las respuestas legales frente a delitos emergentes.

El 80% que aboga por la capacitación permanente de policías y fiscales resalta la importancia de fortalecer las competencias tecnológicas y legales de los operadores de justicia. Esta necesidad encuentra respaldo en las conclusiones de Huaman (2020), quien señala que la cooperación internacional y la formación continua son esenciales para enfrentar delitos transnacionales. Asimismo, Spiezia (2022) enfatiza que el Protocolo II del Convenio de Budapest puede servir como un marco útil para mejorar la capacitación y colaboración entre países. Las herramientas tecnológicas avanzadas y el conocimiento especializado son esenciales para manejar las dinámicas cambiantes de los delitos cibernéticos que afectan a los menores. La capacitación continua, combinada con estrategias de cooperación internacional, permitiría a las autoridades abordar estos casos de manera más efectiva, garantizando tanto la protección de las víctimas como la persecución de los responsables. Esto se alinea con las recomendaciones de Campina y Rodrigues (2022), quienes destacan la importancia de reforzar los marcos normativos y operativos mediante la formación y la colaboración a nivel global.

Estos hallazgos subrayan la necesidad de un enfoque integral para abordar los delitos relacionados con las proposiciones sexuales a menores por medios tecnológicos. Si bien investigaciones como las de Alatrista y Magariño (2021) y Sanmartin (2021) destacan avances legislativos, los resultados reflejan una percepción generalizada de insuficiencia en la preparación institucional y la normativa vigente. Esto sugiere la necesidad de reformas legislativas específicas que contemplen la complejidad de estos delitos, así como la implementación de programas de capacitación continua para fortalecer las competencias de las autoridades. Además, la cooperación internacional, promovida por el Convenio de Budapest, debe complementarse con enfoques locales que adapten las disposiciones globales a las realidades nacionales. Este enfoque debe priorizar tanto la prevención como la persecución de estos delitos, asegurando la protección de los menores en un entorno digital que evoluciona rápidamente. La integración de estas estrategias permitiría cerrar las brechas existentes y garantizar una respuesta más efectiva frente a esta problemática, fortaleciendo la confianza en el sistema de justicia y mejorando la seguridad digital de los menores.

CONCLUSIONES

La investigación realizada detalla las siguientes conclusiones:

1. El análisis realizado evidencia una insuficiencia notable en la legislación peruana y en la implementación del Convenio de Budapest para abordar los desafíos que plantean los delitos informáticos. Desde una perspectiva, los resultados reflejan una percepción generalizada de vacíos normativos y operativos en aspectos como el fraude informático, la suplantación de identidad y las proposiciones sexuales a menores a través de medios digitales. Esta insuficiencia se traduce en una incapacidad institucional para combatir eficazmente estos delitos, como lo refleja el 100% de los encuestados que señala la falta de preparación de policías y fiscales. Se profundiza en la necesidad de adaptar las leyes y marcos internacionales al ritmo acelerado de las tecnologías, incorporando definiciones más claras, protocolos específicos y cooperación internacional efectiva. Asimismo, se resalta que la colaboración limitada entre empresas privadas e instituciones públicas agrava la sensación de impunidad, dejando vacíos que los ciberdelincuentes explotan. En conjunto, los hallazgos subrayan la urgencia de una reforma integral que abarque tanto la actualización normativa como el fortalecimiento institucional, priorizando la capacitación continua y el uso de herramientas tecnológicas avanzadas para garantizar la seguridad digital en un entorno globalizado y en constante cambio.
2. En el ámbito del fraude informático, los resultados muestran que el 93% de los encuestados identifica vacíos significativos en la legislación peruana, mientras que el 53% señala insuficiencias en el Convenio de Budapest. Esto sugiere una percepción de que tanto el marco normativo nacional como el internacional no están preparados para enfrentar las nuevas modalidades delictivas asociadas al

fraude digital. Se destaca que las leyes actuales carecen de flexibilidad para adaptarse a los avances tecnológicos, dejando conductas ilícitas sin regulación. Además, se señala la falta de mecanismos formales para la investigación y sanción de estos delitos, lo que limita la capacidad del sistema legal para responder eficazmente. La percepción unánime de que las autoridades encargadas de la justicia no están preparadas refuerza la necesidad de programas de capacitación continua y recursos tecnológicos avanzados. En suma, el tratamiento del fraude informático requiere una actualización normativa que contemple medidas preventivas, sanciones proporcionales y estrategias de cooperación internacional, así como un fortalecimiento institucional que permita enfrentar este delito de manera proactiva y eficiente.

3. Respecto a la suplantación de identidad, los datos reflejan que el 73% de los encuestados considera que la legislación peruana presenta vacíos, y el 67% percibe insuficiencias en el Convenio de Budapest. Estas cifras revelan una percepción extendida de que este delito, cada vez más frecuente en el entorno digital, no está adecuadamente regulado ni a nivel nacional ni internacional. Se identifica que las leyes actuales penalizan únicamente las conductas que generan perjuicio comprobable, dejando sin sanción el acto mismo de suplantar identidad. Además, se menciona cómo las innovaciones tecnológicas, como la inteligencia artificial, facilitan este tipo de delitos, exponiendo la necesidad de una regulación que contemple estas nuevas herramientas. La falta de capacitación especializada entre los operadores de justicia y la ausencia de protocolos específicos agravan el problema. Por tanto, se concluye que es esencial reformar las normativas existentes, incorporando definiciones claras y específicas, sanciones adecuadas y

mecanismos de cooperación internacional, además de priorizar la capacitación y dotación tecnológica de las autoridades encargadas de combatir este delito.

4. En cuanto a los delitos relacionados con proposiciones sexuales a menores a través de medios tecnológicos, el 87% de los encuestados señala vacíos en la legislación peruana, mientras que el 73% identifica insuficiencias en el Convenio de Budapest. Estas cifras destacan una preocupación extendida sobre la falta de protección legal frente a conductas como el grooming, facilitadas por plataformas digitales. Se profundiza en cómo la ausencia de normativas específicas y la falta de regulación en redes sociales y aplicaciones agravan esta problemática. Además, se resalta que las empresas tecnológicas no responden adecuadamente a las solicitudes de información por parte de las autoridades, retrasando las investigaciones y permitiendo la impunidad. También se identifica una brecha en la preparación de las autoridades judiciales para manejar este tipo de delitos, lo que refuerza la necesidad de capacitación permanente. En este contexto, se concluye que se requieren reformas legislativas que incluyan definiciones claras, sanciones proporcionales y protocolos de protección para menores, además de un fortalecimiento institucional que garantice la cooperación efectiva entre actores nacionales e internacionales en la lucha contra estos crímenes.

5.

RECOMENDACIONES

1. Acerca de la legislación y capacidades institucionales frente a los delitos informáticos, se recomienda al Congreso de la República y al Ministerio de Justicia promover una reforma integral del marco normativo peruano. Esta reforma debe incluir la creación de leyes adaptativas que integren definiciones claras y específicas sobre delitos emergentes, como el fraude informático, la suplantación de identidad y el grooming. Asimismo, se sugiere fortalecer las capacidades institucionales mediante la implementación de programas de capacitación continua para policías y fiscales, la dotación de herramientas tecnológicas avanzadas y la elaboración de protocolos especializados. Además, se recomienda fomentar la colaboración efectiva entre el sector privado, el Estado y la comunidad internacional, mediante la creación de mecanismos obligatorios que aseguren una cooperación eficaz. Este enfoque integral garantiza una respuesta adecuada a los desafíos de la seguridad digital en un contexto globalizado y en constante evolución.
2. Acerca del fraude informático, se recomienda al Poder Legislativo actualizar la Ley 30096 para incluir modalidades emergentes de este delito y definir medidas preventivas, sanciones proporcionales y estrategias de investigación más efectivas. Al Poder Judicial, se sugiere diseñar programas de formación continua dirigidos a fiscales y jueces especializados en ciberdelincuencia, con el apoyo de entidades académicas, para garantizar una aplicación precisa de las normativas. Además, se recomienda la creación de unidades especializadas en fraude informático dentro de las fiscalías, equipadas con tecnologías avanzadas de ciberseguridad. En paralelo, se sugiere fomentar investigaciones académicas sobre las herramientas tecnológicas utilizadas por los ciberdelincuentes y estudiar

modelos legislativos internacionales exitosos que puedan servir de base para futuras reformas.

3. Acerca de la suplantación de identidad, se recomienda al Congreso de la República trabajar en una reforma legal que tipifique este delito de manera específica, sancionando no solo los daños resultantes, sino también el acto mismo de suplantación. A las academias jurídicas, se sugiere incentivar investigaciones sobre el impacto de tecnologías emergentes, como la inteligencia artificial, en la facilitación de este delito, generando propuestas regulatorias. Asimismo, al Ministerio de Relaciones Exteriores, se le recomienda liderar iniciativas internacionales para adaptar el Convenio de Budapest a las particularidades nacionales, promoviendo protocolos de cooperación más específicos que permitan abordar eficazmente este delito en contextos transnacionales.
4. Acerca de las proposiciones sexuales a menores mediante medios digitales (grooming), se recomienda al Congreso de la República y al Ministerio de la Mujer y Poblaciones Vulnerables diseñar una normativa específica que contemple sanciones proporcionadas, medidas preventivas y protocolos claros de protección para menores. A las empresas tecnológicas, se sugiere colaborar activamente en las investigaciones judiciales, implementando medidas de seguridad en sus plataformas, como sistemas de detección de contenido sospechoso y mecanismos de reporte inmediato. Además, a las organizaciones académicas y de protección infantil, se recomienda realizar estudios sobre el impacto psicológico y social del grooming, a fin de desarrollar estrategias de intervención más efectivas. Finalmente, al Ministerio de Relaciones Exteriores, se le propone impulsar revisiones al Convenio de Budapest que incluyan cláusulas más específicas sobre la protección infantil en el entorno digital.

REFERENCIAS BIBLIOGRAFICAS

Akers, R. L. (1998). *Social learning and social structure*: A general theory of crime and deviance. Northeastern University Press.

Alatrista, D. E., & Magariño, M. N. (2021). *Los principios de independencia y autonomía y su relación con la garantía del pedido de acceso a la información pública que dan las autoridades nacionales de transparencia*. In [Tesis de licenciatura, Universidad Privada del Norte]. Repositorio de la Universidad Privada del Norte. https://hdl.handle.net/11537/28903

Ali, W. N. H. W., Mohd, M., & Fauzi, F. (2018). *Cyberbullying detection*: an overview. 2018 Cyber Resilience Conference (CRC, 1–3.

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). *Comprehensive review of cybercrime detection techniques*. *IEEE Access*, *8*, 137293–137311.

Amankwah-Amoah, J., Khan, Z., Wood, G., & Knight, G. (2021). *COVID-19 and digitalization*: The great acceleration. Journal of Business Research. https://doi.org/10.1016/j.jbusres.2021.08.011

Amick, M., Bentivegna, K., Hunter, A. A., Leventhal, J. M., Livingston, N., Bechtel, K., & Holland, M. L. (2022). *Child maltreatment-related children's emergency department visits before and during the COVID-19 pandemic in Connecticut. Child Abuse & Neglect*, 128, 105619. https://doi.org/10.1016/j.chiabu.2022.105619

ANDINA. (2020). *Estos son los delitos informáticos más frecuentes en el Perú, según la Policía*. ANDINA. https://andina.pe/agencia/noticia-estos-son-los-delitos-informaticos-mas-frecuentes-el-peru-segun-policia-81320.aspx

Arifin, R., Atikasari, H., & Waspiah, W. (2020). *The Intersection of Criminal Law, Technology and Business Commercial Law on Carding as Cyber Fraud*. Journal Hukum Novelty. https://doi.org/10.26555/novelty.v11i2.a15700

Ayma Huallpa, H. (2020). *Delitos informáticos y su relación con el proceso de investigación preliminar en el Distrito Fiscal de Lima Norte año 2019*. Universidad Alas Peruanas.

Bada, M., & Nurse, J. R. (2020). *The social and psychological impact of cyberattacks*. In Emerging cyber threats and cognitive vulnerabilities (pp. 73–92). Academic Press.

Bandura, A. (1977). *Social learning theory*. Prentice-Hall.

Becker, G. S. (1968). *Crime and punishment*: An economic approach. Journal of Political Economy, 76(2), 169–217.

Booth, K. (2007). *Theory of World Security*. In Theory of World Security. https://doi.org/10.1017/cbo9780511840210

Buchholtz, G., & Stentzel, R. (2018). Comment On Art. 5 Gdpr. In S. Gierschmann, K. Schlender, R. Stentzel, & W. Veil (Eds.), Kommentar Datenschutz- Grundverordnung (Vol. 23). *Bundesanzeiger Verlag*.

Burnes, D., DeLiema, M., & Langton, L. (2020). *Risk and protective factors of identity theft victimization in the United States*. Preventive Medicine Reports, 17. https://doi.org/10.1016/j.pmedr.2020.101058

Campina, A., & Rodrigues, C. (2022). Cybercrime and the Council of Europe Budapest Convention: Prevention, Criminalization, and International Cooperation. 1, 112.

Clough, J. (2014). *A world of difference: the Budapest convention on cybercrime and the challenges of harmonization*. Monash Univ Law Rev, 40(3).

CONAPOC. (2020). *Diagnóstico Situacional Multisectorial Sobre La Ciberdelincuencia En El Perú*. In Ministerio de Justicia y Derechos Humanos.

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

Coral Chalco, M. (2017). *La intervención mínima del derecho penal frente al cyberacoso a menores de edad, y los delitos de difamación y extorsión en el Perú, año* 2017. Universidad Nacional Santiago Antúnez de Mayolo, 1.

Cornish, D. B., & Clarke, R. V. (1986). *The reasoning criminal: Rational choice perspectives on offendin*g. Springer.

Council Europe. (2001a). *Explanatory report to the Budapest Convention.* https://rm.coe.int/16800cce5b.

Council Europe. (2001b). *The Budapest Convention on Cybercrime, Preamble Section 9*. https://rm.coe.int/1680081561

Davis, R. (2012). *Organized crime in a network society*. Journal of International Affairs, 66(1).

Dine, A. (2020). *When is cyber defense a crime? Evaluating active cyber defense measures under the Budapest Convention*. Chic J Int Law, 20(2).

Dragan, A. T. (2018). *Child pornography and child abuse in cyberspace*. Journal of Legal Studies "Vasile Goldiş," 21(35), 52–60.

Elizalde Castañeda, R. R., Flores Ramírez, H. H., & Castro Lorzo, E. M. (2021). *Los delitos cibernéticos en Chile, México y Colombia*. Un estudio

de Derecho Comparado. Ius Comitial is, 4(8), 252. https://doi.org/10.36677/iuscomitialis.v4i8.17320

Federal Supreme Court of Switzerland. (2014). *Federal Supreme Court of Switzerland decision 141 IV 108*. 141 IV 108, 122.

Fuentes Garrido, K. V. (2021). *Modificación de la ley 30096 para incorporar los delitos de phishing, pharming y carding como delitos penalizables con prisión, para reducir la ciberdelincuencia, Lima 2019*. Universidad Señor de Sipán.

Gallardo Granda, A. S. (2020). *Innovaciones en la tipificación de delitos con la ratificación del convenio contra el cibercrimen, en el Perú el año 2019*. Loreto. Universidad Científica del Perú.

Hernández Sampieri, R., & Mendoza Torres, C. (2018). *Metodología de la investigación - Las rutas cuantitativa, cualitativa y mixta* (Mc Graw Hill (ed.)). https://www.ebooks7-24.com:443/?il=6443.,

Hidalgo Coronel, C. N., & Solano Vidal, G. S. (2021). *El phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano. Propuesta de incorporación del artículo 7-a en la Ley de Delitos Informáticos 30096*. Universidad Nacional del Santa.

Huamán Cruz, M. Y. (2020). *Los delitos informáticos en Perú y la suscripción del Convenio de Budapest*. Universidad Andina del Cuzco.

Ibrahim, S. (2016). Causes of socioeconomic cybercrime in Nigeria. 2016 IEEE International Conference on Cybercrime and Computer Forensic, ICCCF 2016. https://doi.org/10.1109/ICCCF.2016.7740439

Isenring, B., Maybud, R. D., & Quiblier, L. (2019). *Phänomen Cybercrime – Herausforderungen und Grenzen des Straf- und Strafprozessrechts im*

Überblick. SJZ, 115(444).

J. (2020). *Americans' COVID-19 Stress, Coping, and Adherence to CDC Guidelines*. Journal of General Internal Medicine, 35(8), 2296–2303. https://doi.org/10.1007/s11606-020-05898-9

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). *Cybercrime classification and characteristics*. Cyber Crime and Cyber Terrorism Investigator's Handbook, 149–164.

Kansagra, D., Kumhar, M., & Jha, D. (2015*). Ransomware: a threat to cyber security*. IJCSCS, 7(226).

López, L. A. L. (2012). *Conductas de acoso en Facebook en estudiantes de preparatoria y facultad.* Revista Electrónica Diálogos Sobre Educación, 3, 1–17.

Marcum, C. D., & Higgins, G. E. (2019). *Cybercrime*. Handbook on Crime and Deviance, 459–475.

Marsili, M. (2019). *The war on cyberterrorism*. Democracy and Security, 15(2), 172– 199.

Miller, D., Costa, E., Haynes, N., McDonald, T., Nicolescu, R., Sinanan, J., Spyer, J., Venkatraman, S., & Wang, X. (2018). *How the World Changed Social Media*. In How the World Changed Social Media. https://doi.org/10.2307/j.ctt1g69z35

Ortiz Campos, N. J. (2019*). Normativa Legal sobre Delitos Informáticos en Ecuador*. Revista Científica Hallazgos21, 4(1), 100–111. https://revistas.pucese.edu.ec/hallazgos21/article/view/336

Park, C. L., Russell, B. S., Fendrich, M., Finkelstein-Fox, L., Hutchison, M., & Becker, Perera, A., & Fernando, P. (2021). *Accurate Cyberbullying*

Detection and Prevention on Social Media. Procedia Computer Science, 181, 605–611.

Pereyra Maita, L. A., & Turpo Hinostroza, J. A. (2020). *Instrumentos normativos que se deben adecuar en nuestra legislación según el marco del Convenio de Budapest como mecanismo legal de protección a la intimidad personal frente a las TICS*. Universidad Tecnológica del Perú.

Quispe, M. del C. A., & Alecchi, B. A. (2021). *Business School Student Satisfaction with Emergency Remote Teaching.* Journal of Education and E-Learning Research, 8(4), 375–384. https://doi.org/10.20448/journal.509.2021.84.375.384

Rios Cataño, C. (2020). *Aspectos éticos para la publicación científica en revistas de alto impacto*. Universidad Continental, 1–4.

Rodríguez, B. O., & Sánchez, T. L. (2020). *The Psychosocial Impact of COVID-19 on health care workers*. International Brazilian Journal of Urology, 46(suppl 1), 195–200. https://doi.org/10.1590/s1677-5538.ibju.2020.s124

Sae-Bae, N., Sun, X., Sencar, H. T., & Memon, N. D. (2014). *Towards automatic detection of child pornography*. 2014 IEEE International Conference on Image Processing (ICIP, 5332–5336).

Sanmartín Mora, W. C. (2021). *Los delitos informáticos en el Código Orgánico Integral Penal y el Convenio Internacional de Budapest*. In Trabajo de Titulación modalidad Proyecto de Investigación previo a la obtención del Título de Abogado de los Tribunales y Juzgados de la República. UCE.

Sharma, S., & Gaherwal, R. (2017). *Comparative Study and Analysis of Unique Identification Number and Social Security Number*. Int. Journal of

Scientific Research in Computer Science and Engineering, 27.

Singer, J., & Brodzinsky, D. (2020). *Virtual parent-child visitation in support of family reunification in the time of COVID-19*. Developmental Child Welfare, 2(3), 153–171. https://doi.org/10.1177/2516103220960154

Sosa Umbo, O. A. (2022). *Phishing como modalidad de delitos informáticos: a propósito de la suplantación y robo a los beneficiarios del Bono Universal en el Perú*. Universidad Nacional de Piura.

Spiezia, F. (2022). *International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime*. ERA Forum, 23(1), 101–108. https://doi.org/10.1007/s12027-022-00707-8

Statista. (2022). *Internet usage in the United States - statistics & facts | Statista*. https://www.statista.com/topics/2237/internet-usage-in-the-united-states/

Swiss Federal Council. (2020). *Swiss Federal Council official comment on the approval and implementation of the Budapest Convention into Swiss Law* (p. 4731). https://www.admin.ch/opc/de/federal-gazette/2010/4697.pdf.

Tsakalidis, G., & Vergidis, K. (2019). *A Systematic Approach Toward Description and Classification of Cybercrime Incidents*. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(4). https://doi.org/10.1109/TSMC.2017.2700495

USA department of justice. (2014). *United States Court of Appeals, Eighth Circuit Choice escrow & land title, LLC v*. Bancorpsouth Bank, 754 F.3d 6.

Van Nguyen, T., Truong, T. V., & Lai, C. K. (2022). *Legal challenges to combating cybercrime: An approach from Vietnam*. Crime, Law and

Social Change, 77(3), 231–252. https://doi.org/10.1007/s10611-021-09986-7

Vargas Miñan, W. (2022). *Necesidad de tipificar la estafa básica en la ley de delitos informáticos para reducir la impunidad en el Perú*. Universidad César Vallejo.

Villareal (2020). *Innovaciones en la tipificación de delitos con la ratificación del convenio contra el cibercrimen, en el Perú el año 2019*: http://repositorio.ucp.edu.pe/handle/UCP/984.

Vitteri Melgar, G. D. (2022). *Mecanismos jurídicos para implementar la Ley 30096 en los Delitos Informáticos contra el patrimonio frente a las nuevas Tecnologías Informáticas*. Universidad Inca Garcilazo de la Vega.

Vyawahare, M., & Chatterjee, M. (2020). *Taxonomy of cyberbullying detection and prediction techniques in online social networks*. In Data communication and networks (pp. 21–37). Springer.

Weissbrodt, D. (2013). *Cyber-conflict, cyber-crime, and cyber-espionage*. Minn J Int Law, 22(2).

Wittes, B., Poplin, C., Jurecic, Q., & Spera, C. (2016). *Sextortion: Cybersecurity, teenagers, and remote sexual assault 1*. Center for Tecnology Innovation at BROOKINGS, May.

Yar, M. (2019). *Transnational governance and cybercrime control: dilemmas, developments and emerging research agendas*. In A Research Agenda for Global Crime. https://doi.org/10.4337/9781786438676.00012

Zhang, L. (2008). *Effective techniques for detecting and attributing cyber criminals*. Iowa State University.

ANEXOS

Anexo A. Matriz de Consistencia

Título preliminar:

APLICACIÓN DEL CONVENIO DE BUDAPEST EN LA LEY DE DELITOS INFORMÁTICOS DEL PERÚ, CUSCO 2024.

Problemas	Objetivos de la investigación
Problema general	**Objetivo General**
¿Cómo se ha aplicado el convenio de Budapest con respecto a la ley de delitos informáticos del Perú, Cusco 2024?	Comparar la aplicación del convenio de Budapest con respecto a la ley de delitos informáticos del Perú para afrontar la ciberdelincuencia, Cusco 2024.
Problemas específicos	**Objetivos Específicos**
¿Cómo se ha aplicado el convenio de Budapest con respecto a la ley de delitos informáticos del Perú, sobre el bien jurídico del patrimonio en el delito de fraude informático, Cusco 2024?	Identificar cómo se ha aplicado el convenio de Budapest con respecto a la ley de delitos informáticos del Perú, sobre el bien jurídico del patrimonio en el delito de fraude informático, Cusco 2024.
¿Cómo se ha aplicado el convenio de Budapest con respecto a la ley de delitos informáticos del Perú, sobre el bien jurídico de la fe pública en el delito de suplantación de identidad, Cusco 2024?	Identificar cómo se ha aplicado el convenio de Budapest con respecto a la ley de delitos informáticos del Perú, sobre el bien jurídico de la fe pública en el delito de suplantación de identidad, Cusco 2024.

¿Cómo se ha aplicado el convenio de Budapest con respecto a la ley de delitos informáticos del Perú, sobre el bien jurídico de la indemnidad e intangibilidad sexual en el delito de proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, Cusco 2024?	Identificar cómo se ha aplicado el convenio de Budapest con respecto a la ley de delitos informáticos del Perú, sobre el bien jurídico de la indemnidad e intangibilidad sexual en el delito de proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, Cusco 2024.

Diseño metodológico			
Tipos de documentos	**Criterios de Selección de documentos**	**Técnicas de recojo de información**	**Instrumentos para recoger información**
Cualitativo	Fuente primaria	Encuesta	Cuestionario

Objetivos	**Hipótesis**
Objetivo General	**Hipótesis General**
Comparar la aplicación del convenio de Budapest con respecto a la ley de delitos informáticos del Perú para afrontar la ciberdelincuencia, Cusco 2024.	Existe una diferencia significativa entre la ley de delitos informáticos del Perú y el convenio de Budapest acerca de la ciberdelincuencia, Cusco 2024.
Objetivos Específicos	**Hipótesis Específicas**
Identificar cómo se ha aplicado el convenio de Budapest con respecto a la ley de delitos informáticos del Perú, sobre el bien jurídico del patrimonio en el delito de fraude informático, Cusco 2024.	Existe una diferencia significativa entre la ley de delitos informáticos del Perú y el convenio de Budapest acerca del bien jurídico del patrimonio en la modalidad de fraude informático, Cusco 2024.

Identificar cómo se ha aplicado el convenio de Budapest con respecto a la ley de delitos informáticos del Perú, sobre el bien jurídico de la fe pública en el delito de suplantación de identidad, Cusco 2024.	Existe una diferencia significativa entre la ley de delitos informáticos del Perú y el convenio de Budapest acerca del bien jurídico de la fe pública en la modalidad de la suplantación de identidad Cusco 2024.
Identificar cómo se ha aplicado el convenio de Budapest con respecto a la ley de delitos informáticos del Perú, sobre el bien jurídico de la indemnidad e intangibilidad sexual en el delito de proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, Cusco 2024.	Existe una diferencia significativa entre la ley de delitos informáticos del Perú y el convenio de Budapest acerca del bien jurídico de la libertad e intangibilidad sexual en la modalidad de proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, Cusco 2024.
Bibliografía de sustento para la justificación y delimitación del problema	Bibliografía de sustento usada para el diseño metodológico
(Vargas Miñan, 2022; Yar, 2019)	(Hernández Sampieri & Mendoza Torres, 2018)

Anexo B. Matriz de Operacionalización de Variables

	Categoría 1: Convenio de Budapest
Definición Conceptual	**Instrumento internacional que busca armonizar las leyes nacionales para combatir el ciberdelito mediante la cooperación internacional y la tipificación específica de delitos cibernéticos.**
Definición Operacional	Evaluación de la implementación del Convenio de Budapest en el marco legal peruano sobre ciberdelitos.
Dimensiones	Tipificación de delitos cibernéticos
Indicadores	Inclusión de delitos específicos como fraude informático y suplantación de identidad; Obligación de preservar datos; Aplicación práctica en procesos penales.
Instrumentos	Encuestas y entrevistas a juristas y especialistas en ciberdelitos; análisis documental del marco legal.
	Categoría 2: Ley de Delitos Informáticos del Perú (Ley N° 30096)
Definición Conceptual	**Normativa nacional que regula los delitos cibernéticos en Perú, enfocada en la protección de bienes jurídicos como el patrimonio, la fe pública y la indemnidad sexual.**
Definición Operacional	Análisis de la eficacia y limitaciones de la Ley N° 30096 frente a los delitos cibernéticos más comunes.
Dimensiones	Protección del patrimonio
Indicadores	Regulación de fraude informático; sanciones por suplantación de identidad; medidas contra proposiciones sexuales en línea.
Instrumentos	Encuestas a operadores del sistema de justicia; entrevistas a legisladores; revisión de casos judiciales.

Anexo C. Instrumentos

CIBERDELITOS SEGÚN LA LEY DE DELITOS INFORMÁTICOS DEL PERÚ RESPECTO AL CONVENIO DE BUDAPEST.

Institución donde pertenece:

.....

Cargo:

.....

Nombre:

.....

Instrucciones: A continuación, verá algunas afirmaciones respecto de algunos delitos cibernéticos, asociados a la normativa planteada en la ley de delitos informáticos peruana. Lea con atención y cuidado cada una de ellas. En cada frase, señale con una equis (X) la columna que mejor indique su respuesta en cada frase:

Cuestionario:

	DESCRIPCIÓN	SI	NO
DELITOS INFORMÁTICOS, RESPECTO AL BIEN JURÍDICO DEL PATRIMONIO EN EL DELITO DE FRAUDE INFORMÁTICO			
1	¿Considera usted que existen vacíos en la ley de delitos informáticos del Perú respecto al fraude informático?		
2	¿Considera usted que existen vacíos en el convenio de Budapest respecto al fraude informático?		
3	¿Considera usted que los policías y fiscales están totalmente preparados para combatir el fraude informático?		
4	¿Considera usted que es necesario capacitar en forma permanente a los policías y fiscales para combatir con mayor eficacia el fraude informático?		

En caso de marcar si a la pregunta uno (01) cuál considera que sea :

.....

En caso de marcar si a la pregunta uno (02) cuál considera que sea :

.....

DELITOS INFORMÁTICOS, RESPECTO AL BIEN JURÍDICO DE LA FE PÚBLICA EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD			
1	¿Considera usted que existen vacíos en la ley de delitos informáticos del Perú, respecto a la suplantación de identidad?		
2	¿Considera usted que existen vacíos en la ley de delitos informáticos del Perú respecto a la suplantación de identidad?		
3	¿Considera usted que los policías y fiscales están totalmente preparados para combatir la suplantación de identidad?		
4	¿Considera usted que es necesario capacitar en forma permanente a los policías y fiscales para combatir con mayor eficacia la suplantación de identidad?		

En caso de marcar si a la pregunta uno (01) cuál considera que sea :

.....

En caso de marcar si a la pregunta uno (02) cuál considera que sea :

.....

DELITOS INFORMÁTICOS, RESPECTO AL BIEN JURÍDICO DE LA INDEMNIDAD E INTANGIBILIDAD SEXUAL EN EL DELITO DE PROPOSICIONES A NIÑOS, NIÑAS Y ADOLESCENTES CON FINES SEXUALES POR MEDIOS TECNOLÓGICOS			
1	¿Considera usted que existen vacíos en la ley de delitos informáticos del Perú, respecto a las proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos?		
2	¿Considera usted que existen vacíos en la ley de delitos informáticos del Perú respecto a las proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos?		

3	¿Considera usted que los policías y fiscales están totalmente preparados para combatir las proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos?		
4	¿Considera usted que es necesario capacitar en forma permanente a los policías y fiscales para combatir con mayor eficacia las proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos?		

En caso de marcar si a la pregunta uno (01) cuál considera que sea:

.....

En caso de marcar si a la pregunta uno (02) cuál considera que sea:

.....

Lugar y fecha:

.....

Firma

DNI. N° .....

Anexo D. Declaración de Consentimiento Informado

Título del estudio: Aplicación del Convenio de Budapest en la Ley de Delitos Informáticos del Perú, Cusco 2024

Investigadores responsables:

Bach. Ruth Stefany Quincho Laura

Bach. Jose Fernando Aylas Dionicio

Bach. Joel Arcos Huayhua

Introducción:

Usted está invitado a participar en un estudio que tiene como objetivo analizar la aplicación del Convenio de Budapest en la legislación peruana sobre delitos informáticos. Este estudio es parte de una investigación académica conducida por los investigadores arriba mencionados, quienes están optando por el título de abogado en la Universidad de Cusco. Su participación en este estudio es voluntaria y su decisión de participar o no, no afectará su relación profesional o personal con los investigadores o la institución.

Propósito del estudio:

El propósito de este estudio es comparar la ley peruana de delitos informáticos con el Convenio de Budapest, identificando las diferencias y posibles mejoras en el tratamiento de la ciberdelincuencia en el país.

Procedimientos:

Si usted decide participar, se le pedirá que responda a un cuestionario que se ha diseñado para recoger información sobre su experiencia profesional en casos relacionados con ciberdelitos. Este cuestionario contiene preguntas que buscan conocer su opinión sobre la legislación actual y la implementación del Convenio de Budapest en Perú.

Riesgos y beneficios:

No se prevén riesgos mayores asociados con su participación en este estudio. Los beneficios incluyen la posibilidad de contribuir con su experiencia a la mejora del marco legislativo en el Perú en relación a los ciberdelitos, lo que puede tener un impacto positivo en la sociedad.

Confidencialidad:

Toda la información proporcionada será tratada de manera confidencial y se utilizará únicamente para fines académicos. Los datos recogidos serán anonimizados para

proteger su identidad y no se divulgarán sin su consentimiento. Los resultados del estudio pueden ser publicados, pero no contendrán información que lo identifique de manera individual.

Derechos del participante:

Su participación es completamente voluntaria. Usted tiene el derecho de retirarse del estudio en cualquier momento sin necesidad de dar explicaciones y sin que esto genere ningún tipo de consecuencia negativa. También puede negarse a responder cualquier pregunta que no desee contestar.

Contacto:

Si tiene preguntas sobre este estudio o sus derechos como participante, puede contactar a los investigadores al siguiente correo electrónico: [correo electrónico de los investigadores].

Consentimiento:

He leído y comprendido la información proporcionada en este documento y estoy de acuerdo en participar en este estudio bajo los términos mencionados. Entiendo que mi participación es voluntaria y que puedo retirarme en cualquier momento.

Firma del participante: _____

Fecha: _____

Firma del investigador: _____

Fecha: _____