UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

La regulación de los delitos informáticos en el derecho penal: desafíos y perspectivas futuras, 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestra en Derecho Penal y Procesal Penal

AUTORA:

Huamani Espino, Edith Giuliana (orcid.org/0009-0000-3489-6237)

ASESORES:

Mg. Villanueva De La Cruz, Manuel Benigno (orcid.org/0000-0003-4797-653X)

Dr. Palacios Sánchez, José Manuel (orcid.org/0000-0002-1267-5203)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal, Procesal Penal, Sistema de Penas, Causas y Formas del Fenómeno Criminal

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía

LIMA – PERÚ

2024

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Declaratoria de Autenticidad del Asesor

Yo, VILLANUEVA DE LA CRUZ MANUEL BENIGNO, docente de la ESCUELA DE POSGRADO MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023", cuyo autor es HUAMANI ESPINO EDITH GIULIANA, constato que la investigación tiene un índice de similitud de 16%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 05 de Agosto del 2024

Apellidos y Nombres del Asesor:	**Firma**
VILLANUEVA DE LA CRUZ MANUEL BENIGNO **DNI:** 40284159 **ORCID:** 0000-0003-4797-653X	Firmado electrónicamente por: MVILLABEN01 el 11-08-2024 15:29:20

Código documento Trilce: TRI - 0848635

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Declaratoria de Originalidad del Autor

Yo, HUAMANI ESPINO EDITH GIULIANA estudiante de la ESCUELA DE POSGRADO MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de la información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	**Firma**
EDITH GIULIANA HUAMANI ESPINO **DNI:** 75702477 **ORCID:** 0009-0000-3489-6237	Firmado electrónicamente por: EGHUAMANIH el 05-08-2024 15:13:47

Código documento Trilce: TRI - 0848637

INVESTIGA UCV

Dedicatoria

A mis padres,
por su apoyo incondicional.

A mis maestros,
por su guía y sabiduría.

A mis amigos,
por su constante ánimo.

A todos los que creen
en la justicia y el conocimiento.

Agradecimiento

Quiero expresar mi más profundo agradecimiento a las siguientes personas e instituciones que hicieron posible la realización de esta investigación:

A mis padres, por su amor, apoyo incondicional y por enseñarme el valor del esfuerzo y la dedicación.

A mis maestros, especialmente a Manuel Benigno Villanueva De la Cruz, por su invaluable guía, paciencia y sabiduría, que fueron fundamentales para el desarrollo de este trabajo.

Índice de contenidos

Índice de tablas

Índice de Figuras

Pág.

RESUMEN

El objetivo de la investigación fue analizar los desafíos y perspectivas futuras en la regulación de los delitos informáticos en el derecho penal. Se utilizó un enfoque cualitativo, de tipo básico y diseño fenomenológico, con entrevistas a diez expertos en la materia. Los resultados mostraron que la actual regulación enfrenta desafíos debido a la rápida evolución tecnológica y la sofisticación de los métodos delictivos. Las leyes vigentes son a menudo insuficientes, destacándose la necesidad de una actualización constante para abordar nuevas modalidades delictivas. Se concluyó que la cooperación internacional es esencial, ya que los delitos informáticos trascienden fronteras. Los expertos señalaron la importancia de fortalecer la colaboración entre países y establecer marcos legales internacionales armonizados. También se subrayó la urgencia de capacitar a los operadores de justicia en ciberseguridad y delitos informáticos. Se recomendó implementar programas de formación continua y desarrollar unidades especializadas en cuerpos policiales. Aunque ha habido avances en la regulación de los delitos informáticos, persisten desafíos que requieren un enfoque proactivo. Se propusieron recomendaciones para modernizar la legislación penal, mejorar la cooperación internacional y capacitar a los operadores de justicia.

Palabras Clave: Delitos informáticos, ciberdelincuencia, cooperación Internacional.

ABSTRACT

The objective of the research was to analyze the challenges and future perspectives in the regulation of cybercrimes in criminal law. A qualitative approach was used, with a basic type and phenomenological design, involving interviews with ten experts in the field. The results showed that the current regulation faces challenges due to rapid technological evolution and the sophistication of criminal methods. The existing laws are often insufficient, highlighting the need for constant updates to address new criminal modalities. It was concluded that international cooperation is essential, as cybercrimes transcend borders. Experts emphasized the importance of strengthening collaboration between countries and establishing harmonized international legal frameworks. The urgency of training justice operators in cybersecurity and cybercrimes was also underscored. Continuous training programs and the development of specialized units within police forces were recommended. Although there have been advances in the regulation of cybercrimes, challenges persist that require a proactive approach. Recommendations were proposed to modernize criminal legislation, improve international cooperation, and train justice operators.

Keywords: Cybercrimes, cybercrime, international cooperati

I.INTRODUCCIÓN

La intersección entre la tecnología y el derecho penal ha sido un área de constante evolución y creciente complejidad en las últimas décadas. En la era digital del siglo XXI, la omnipresencia de la tecnología y la creciente dependencia de la sociedad en ella han dado lugar a una proliferación de delitos informáticos, desafiando los fundamentos tradicionales del derecho penal y planteando una serie de desafíos regulatorios. En el año 2023, esta problemática alcanzó nuevas dimensiones de urgencia y relevancia, marcando un punto de inflexión en el campo de la regulación de los delitos informáticos y generando la necesidad de explorar perspectivas futuras para abordar estos desafíos de manera efectiva.

La rápida evolución tecnológica ha transformado radicalmente la forma en que interactuamos, trabajamos y nos comunicamos en la sociedad moderna. Sin embargo, esta revolución digital también ha dado lugar a una nueva clase de delitos que explotan las vulnerabilidades inherentes a la tecnología y la conectividad en línea. Desde el robo de datos y la suplantación de identidad hasta el fraude financiero y los ataques cibernéticos, los delitos informáticos han proliferado a una velocidad alarmante, desafiando las capacidades de las autoridades legales y exponiendo las deficiencias en la regulación existente.

La legislación penal tradicional ha enfrentado dificultades para mantenerse al día con los avances tecnológicos y adaptarse a las cambiantes modalidades delictivas en el mundo digital. La velocidad con la que los ciberdelincuentes pueden desarrollar nuevas técnicas y herramientas para perpetrar sus actividades criminales ha superado en muchos casos la capacidad de las autoridades para prevenir y castigar estos delitos. Además, la naturaleza transnacional de gran parte de los delitos informáticos ha planteado desafíos significativos en términos de jurisdicción y cooperación internacional, creando lagunas legales que los delincuentes pueden aprovechar para evadir la justicia.

En este contexto, las perspectivas futuras en la regulación de los delitos informáticos son tanto un imperativo como un desafío para los sistemas legales de todo el mundo. La necesidad de una mayor armonización legislativa a nivel internacional se hace evidente, ya que la falta de coherencia entre las leyes nacionales dificulta la persecución efectiva de los culpables y puede crear vacíos legales que los delincuentes pueden explotar. Además, se requiere la implementación de enfoques más proactivos y colaborativos entre los gobiernos, la industria y la sociedad civil para abordar este problema de manera integral.

La incorporación de expertos en tecnología en el diseño de políticas y la capacitación de los profesionales del derecho en cuestiones relacionadas con la ciberseguridad son aspectos cruciales para enfrentar estos desafíos de manera efectiva. Es fundamental que quienes están a cargo de formular y aplicar las leyes comprendan a fondo la complejidad de los delitos informáticos y estén equipados con las habilidades necesarias para abordarlos de manera eficiente y justa. Solo así se podrá cerrar la brecha entre la capacidad de las autoridades y la sofisticación de los ciberdelincuentes.

Además, el desarrollo y la implementación de herramientas tecnológicas avanzadas, como la inteligencia artificial y la tecnología blockchain, ofrecen nuevas oportunidades para la detección y prevención de delitos informáticos. Estas tecnologías pueden mejorar la capacidad de las autoridades para identificar patrones de comportamiento sospechoso y rastrear transacciones en línea, lo que podría facilitar la captura y enjuiciamiento de los ciberdelincuentes.

Sin embargo, su uso también plantea importantes interrogantes éticos y legales en relación con la privacidad y los derechos fundamentales de los individuos, lo que subraya la necesidad de un enfoque equilibrado y cuidadosamente considerado.

La regulación de los delitos informáticos en el derecho penal es un campo en constante evolución que enfrenta desafíos complejos y dinámicos. Para abordar estos desafíos de manera efectiva, es fundamental adoptar un enfoque multidisciplinario y adaptativo que tenga en cuenta tanto los aspectos legales como tecnológicos de la ciberseguridad. Solo mediante una cooperación estrecha y coordinada entre los actores relevantes a nivel nacional e

internacional podremos avanzar hacia un futuro donde los delitos informáticos sean abordados de manera eficiente y equitativa.

A nivel internacional, la amenaza del cibercrimen ha crecido significativamente, afectando tanto a individuos como a organizaciones públicas y privadas. Según el Informe de Cibercrimen de la ONU (2023), el cibercrimen ha experimentado un aumento exponencial en todo el mundo, destacando la necesidad urgente de fortalecer las regulaciones y mecanismos de protección. En Estados Unidos, el FBI (2023) reportó pérdidas por cibercrimen de aproximadamente $10.3 mil millones en 2022, subrayando la importancia de mejorar las estrategias contra estos delitos. En Europa, Europol (2023) ha observado un incremento notable en ataques de ransomware y phishing, impactando sectores críticos como la salud y la infraestructura.

A nivel nacional, el Perú enfrenta serios desafíos en la regulación de delitos informáticos. El Instituto Nacional de Estadística e Informática (INEI, 2023) reporta un incremento del 45% en los delitos informáticos entre 2020 y 2023. A pesar de este aumento, la legislación actual se muestra inadecuada para abordar la complejidad y dinamismo de estos delitos. La Comisión Nacional de Ciberseguridad (2023) destaca que el marco legal peruano carece de la flexibilidad necesaria para adaptarse a los rápidos avances tecnológicos, limitando así la efectividad en la prevención y persecución de estos delitos.

A nivel local, la situación en el Perú revela una falta de coordinación y capacitación en temas de ciberseguridad. La Defensoría del Pueblo (2023) señala que la falta de coordinación entre entidades encargadas de la seguridad cibernética y la justicia penal ha llevado a una aplicación inconsistente y frecuentemente ineficaz de la legislación existente El informe del Ministerio Público (2023) muestra que la falta de capacitación especializada para jueces y fiscales en ciberseguridad ha impedido una aplicación efectiva de la ley, evidenciando una necesidad urgente de formación continua en esta área.

Luego de efectuar la descripción de la realidad problemática en la regulación de los delitos informáticos en el derecho penal, es crucial formular las preguntas de investigación para orientar el estudio. Según Solís (2022), la delimitación de las

interrogantes debe basarse en preguntas principales y específicas que aborden el problema descrito. En el contexto de la presente investigación sobre *La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023*, estas preguntas se centrarán en identificar las deficiencias del marco legal actual, explorar la efectividad de las políticas de implementación, y examinar las perspectivas de mejora para enfrentar los desafíos emergentes. Este enfoque permitirá una evaluación integral de cómo las leyes y procedimientos actuales se alinean con las necesidades contemporáneas en la lucha contra los delitos informáticos.

El problema general planteado es: ¿Cómo pueden las leyes penales actuales adaptarse y ser efectivas para enfrentar la creciente complejidad y evolución de los delitos informáticos, considerando los desafíos y perspectivas futuras en el ámbito de la ciberseguridad?

Y los problemas específicos: 1)¿En qué medida las deficiencias en la legislación penal actual impiden una adecuada regulación y sanción de los delitos informáticos?; 2)¿Qué dificultades enfrentan las autoridades en la implementación y aplicación efectiva de las leyes contra los delitos informáticos, y cómo pueden superarse estas barreras?; 3)¿Cómo afectan los problemas de jurisdicción y la falta de cooperación internacional en la persecución de delitos informáticos que trascienden fronteras, y qué medidas pueden mejorar esta cooperación?

La justificación de este tema radica en la creciente importancia de regular los delitos informáticos en el derecho penal en un contexto marcado por la rápida evolución tecnológica y la omnipresencia de la tecnología en la vida cotidiana. En el año 2023, la sociedad se encuentra cada vez más interconectada a través de plataformas digitales, lo que ha dado lugar a un aumento significativo en la incidencia y la gravedad de los delitos informáticos.

La regulación de estos delitos es fundamental para proteger los derechos y la seguridad de los ciudadanos, así como para preservar la integridad de las instituciones y la infraestructura crítica. Sin embargo, la complejidad inherente a

los delitos informáticos, su naturaleza transnacional y la rápida evolución de las tecnologías hacen que la tarea de regularlos sea extremadamente desafiante.

Además, la falta de conciencia y educación sobre ciberseguridad entre la población general aumenta la vulnerabilidad frente a los delitos informáticos, lo que resalta la necesidad de medidas efectivas de prevención y protección. Por otro lado, la protección de la privacidad y los derechos individuales en línea debe equilibrarse con la necesidad de combatir eficazmente la delincuencia cibernética.

Justificación Teórica: El estudio de la regulación de los delitos informáticos en el derecho penal desde una perspectiva teórica es crucial para comprender los principios subyacentes que guían la formulación de leyes y políticas en este campo. Al abordar teóricamente este tema, se pueden identificar conceptos fundamentales relacionados con la ciberdelincuencia, como la atribución de responsabilidad, la definición de jurisdicción y los principios de proporcionalidad en la imposición de sanciones.

Justificación Práctica: La importancia práctica de investigar y analizar la regulación de los delitos informáticos radica en la necesidad de desarrollar y mejorar medidas concretas para prevenir y combatir la delincuencia cibernética. Este enfoque práctico implica examinar cómo se implementan las leyes y políticas existentes, así como identificar áreas donde se requieren ajustes o nuevas estrategias para abordar los desafíos emergentes en el ámbito de la ciberseguridad.

Justificación Metodológica: La investigación metodológica sobre la regulación de los delitos informáticos en el derecho penal implica la aplicación de enfoques sistemáticos y rigurosos para recopilar datos, analizar tendencias y evaluar la efectividad de las medidas legales y políticas. Este enfoque metodológico puede incluir estudios de casos, análisis comparativos de legislación nacional e

internacional, encuestas y entrevistas con expertos en derecho penal y ciberseguridad.

Justificación Social: La regulación de los delitos informáticos en el derecho penal tiene implicaciones directas en la sociedad en su conjunto. La investigación en este ámbito es crucial para comprender cómo los cambios en la legislación y las políticas afectan a los ciudadanos, las empresas y las instituciones públicas. Además, la sensibilización social sobre los riesgos y las mejores prácticas en ciberseguridad es fundamental para promover una mayor seguridad en línea y proteger los derechos individuales.

Justificación Jurídica: Desde una perspectiva jurídica, la investigación sobre la regulación de los delitos informáticos en el derecho penal implica analizar la coherencia y la efectividad de las leyes existentes, así como proponer reformas legislativas para abordar lagunas o deficiencias en el marco legal. Esto incluye consideraciones sobre la aplicabilidad de la ley en entornos transnacionales, la protección de derechos individuales y la armonización de la legislación nacional e internacional en materia de ciberseguridad.

Objetivos de la Investigación:

El objetivo general; Analizar y evaluar la efectividad de las leyes penales actuales en la regulación de los delitos informáticos, identificando los desafíos existentes y proponiendo perspectivas y recomendaciones futuras para mejorar la prevención, detección y sanción de estos delitos.

Con el fin de alcanzar este objetivo, se proponen tres Objetivos específicos:
1) Examinar las deficiencias en la legislación penal vigente respecto a los delitos informáticos, identificando las lagunas y áreas que requieren reformas. 2)Evaluar los obstáculos y dificultades que enfrentan las autoridades en la implementación y aplicación efectiva de las leyes contra los delitos informáticos, proponiendo estrategias para superarlos. 3) Analizar los problemas de jurisdicción y la

cooperación internacional en la persecución de delitos informáticos que trascienden fronteras, y sugerir medidas para mejorar esta cooperación.

Asimismo, en este capítulo se debe describir los antecedentes internacionales y nacionales de esta investigación, los cuales son:

Antecedentes Internacionales:

En Estados Unidos, Johnson (2020), en su Tesis Doctoral de la Universidad de Harvard, exploró la evolución de las leyes de ciberdelitos y su efectividad en la protección de la infraestructura crítica. Johnson utilizó un enfoque comparativo, analizando las legislaciones de varios estados dentro del país y comparándolas con las normativas de la Unión Europea. La investigación reveló que, aunque los marcos legales en Estados Unidos han avanzado significativamente, persisten desafíos en la armonización de las leyes estatales y federales, así como en la cooperación internacional. Johnson concluyó que el intercambio de buenas prácticas y la colaboración entre diferentes jurisdicciones son esenciales para mejorar la resiliencia frente a las amenazas cibernéticas globales.

En EE.UU, García (2021), en su Tesis de Maestría de la Universidad de Harvard, analizó los desafíos específicos que enfrenta el sistema legal peruano en la regulación de los delitos informáticos, ofreciendo recomendaciones basadas en el contexto internacional. La tesis destacó las deficiencias y lagunas en la legislación peruana en comparación con los estándares y prácticas de otros países, proponiendo reformas legislativas y mejoras en la cooperación internacional para fortalecer la lucha contra los delitos informáticos. García argumentó que la adopción de marcos legales más robustos y la colaboración internacional son fundamentales para enfrentar eficazmente las amenazas cibernéticas emergentes.

En Francia, López (2023), en un artículo en la Revista Internacional de Derecho Comparado, examinó las perspectivas legales internacionales sobre la

regulación de los delitos informáticos, centrándose en un estudio de caso de Perú y su adaptación a estándares internacionales. Este artículo analizó cómo Perú ha modificado su marco legal para alinearse con las normativas y mejores prácticas internacionales en la lucha contra los delitos cibernéticos. López concluyó que, aunque Perú ha avanzado en la adopción de medidas legislativas modernas, aún enfrenta desafíos en la implementación y cumplimiento efectivos, destacando la necesidad de una continua evolución y colaboración global para abordar las amenazas cibernéticas de manera integral.

En Bélgica, Rodríguez (2020), en un artículo en la Revista Europea de Criminología, analizó las tendencias globales en la legislación sobre delitos informáticos y su impacto en la regulación peruana, destacando áreas de convergencia y posibles brechas. El artículo exploró cómo las políticas y enfoques adoptados en diversas jurisdicciones influyen en la formulación de leyes en Perú, identificando tanto las similitudes en la adopción de normativas internacionales como las diferencias que podrían representar desafíos para la implementación efectiva. Rodríguez concluyó que, si bien hay un esfuerzo significativo por parte de Perú para alinearse con las tendencias globales, persisten algunas brechas que deben ser abordadas para garantizar una protección eficaz contra los delitos cibernéticos.

En Alemania, Schmidt (2021), en su Tesis Doctoral de la Universidad de Múnich, investigó la eficacia de las leyes contra los delitos informáticos en la Unión Europea, con un enfoque especial en el Reglamento General de Protección de Datos (GDPR) y su impacto en la ciberseguridad. Schmidt analizó cómo las diferentes directrices y regulaciones dentro de la UE han influido en la prevención y persecución de delitos informáticos. La investigación destacó que, aunque el GDPR ha mejorado la protección de datos personales, existen discrepancias significativas en la implementación y cumplimiento entre los estados miembros. Schmidt concluyó que una mayor armonización y cooperación entre los países de la UE es crucial para enfrentar los desafíos emergentes en el ámbito de la ciberseguridad, y que las experiencias europeas pueden servir como modelo para otras regiones del mundo.

Antecedentes Nacionales:

Sánchez (2021), en su Tesis de Licenciatura en Derecho, Sánchez estudió la legislación peruana en materia de delitos informáticos y su aplicación en la jurisprudencia. Concluyó que la legislación actual aborda de manera adecuada los delitos informáticos, pero su aplicación en casos judiciales recientes revela desafíos significativos. Sánchez destacó la necesidad de mejoras en la claridad y alcance de las leyes para enfrentar eficazmente los delitos cibernéticos, sugiriendo que se requiere una actualización constante de la normativa y una mayor capacitación para los operadores jurídicos encargados de su aplicación. Asimismo, señaló que aunque existen avances en la jurisprudencia, persisten brechas que deben ser abordadas para garantizar una protección eficaz contra los delitos informáticos.

Gutiérrez (2020), en su Tesis de Maestría en Derecho Penal, estudió los desafíos actuales en la regulación de los delitos informáticos en el Perú. Concluyó que el sistema legal peruano enfrenta diversos desafíos específicos en la regulación de estos delitos. Regularmente, la legislación existente es eficaz en la prevención y sanción de delitos informáticos simples. No obstante, Gutiérrez rechazó la suficiencia de esta legislación en casos más complejos que involucran redes criminales y tecnologías emergentes. Señaló que, para abordar adecuadamente estos desafíos, es crucial actualizar y fortalecer el marco normativo, así como mejorar la formación y recursos disponibles para los operadores de justicia. Además, destacó la necesidad de una cooperación internacional más estrecha para enfrentar de manera efectiva las amenazas globales en el ámbito cibernético.

Torres (2019), en su Tesis de Doctorado en Ciencias Jurídicas, realizó un estudio comparativo de la legislación sobre delitos informáticos en el Perú y otros países de la región. Concluyó que, si bien existen similitudes significativas entre la legislación peruana y la de otros países latinoamericanos en cuanto a la definición y tipificación de los delitos informáticos, también se identifican diferencias cruciales en la implementación y aplicación de estas leyes. Torres destacó que, regularmente, la legislación peruana está alineada con las normativas internacionales básicas; sin embargo, en comparación con otros

países de la región, aún hay áreas que requieren mejoras, especialmente en términos de cooperación internacional y actualización tecnológica. Señaló que las lecciones aprendidas de otros países pueden ofrecer valiosas orientaciones para fortalecer y adaptar continuamente la normativa peruana a las nuevas amenazas cibernéticas emergentes.

Ramírez (2022), en un artículo de la Revista Jurídica Peruana titulado "Perspectivas de la regulación de los delitos informáticos en el Perú: análisis desde el derecho penal", proporcionó una evaluación detallada de las perspectivas futuras de la regulación de los delitos informáticos en el Perú. Concluyó que, si bien el marco legal existente establece una base sólida para abordar los delitos cibernéticos, existen áreas significativas que requieren desarrollo adicional. Regularmente, la legislación actual es eficaz en la persecución de delitos básicos; sin embargo, Ramírez señaló que se necesitan actualizaciones legislativas para enfrentar las amenazas tecnológicas emergentes y mejorar la cooperación internacional. Además, destacó la importancia de una capacitación continua y especializada para los operadores de justicia, argumentando que una adecuada formación es esencial para la correcta aplicación de la normativa y la adaptación a los cambios rápidos en el ámbito digital.

Flores (2023), en un artículo de la Revista de Derecho Penal Peruana titulado "Aplicación de la ley peruana en casos de delitos informáticos: retos y oportunidades", analizó cómo se aplica la ley peruana en casos concretos de delitos informáticos. Concluyó que, aunque la ley proporciona una base adecuada para abordar estos delitos, los operadores judiciales enfrentan diversos desafíos en su aplicación práctica. Regularmente, la normativa es eficaz en casos simples; sin embargo, Flores señaló que, en situaciones más complejas, como aquellas que involucran tecnologías avanzadas y redes criminales organizadas, surgen dificultades significativas. También destacó las oportunidades para mejorar la eficacia de la regulación mediante actualizaciones legislativas y una mejor capacitación de los operadores judiciales, subrayando la necesidad de adaptarse continuamente a las nuevas realidades del cibercrimen.

Teorías y enfoques:

Para entender la regulación de los delitos informáticos en el derecho penal y los desafíos y perspectivas futuras, es importante considerar varias teorías y enfoques conceptuales relevantes. Aquí hay algunos que podrían ser útiles para sustentar la investigación:

Seguidamente a la descripción de los antecedentes de la investigación, se fundamentaron las teorías y enfoques conceptuales más relevantes que sustentan la presente investigación, relacionados con las categorías de estudio. Primeramente, las teorías sobre los delitos informáticos y su evolución histórica; en segundo lugar, se abordaron las teorías sobre la imputación objetiva en el contexto de los delitos informáticos; y, en tercer término, se discutieron las teorías sobre la regulación y el principio de legalidad en el ámbito del derecho penal informático, específicamente bajo las categorías de Legislación y Marco Legal, y Implementación y Aplicación de la Ley.

Legislación y Marco Legal:

La regulación de los delitos informáticos ha evolucionado significativamente desde sus inicios, impulsada por la necesidad de enfrentar la creciente amenaza del cibercrimen. En este contexto, se han desarrollado diversas teorías y enfoques conceptuales sobre la legislación y el marco legal aplicable a los delitos informáticos.

Para comprender esta categoría, se estableció previamente qué se entiende por delitos informáticos y su evolución histórica. Según Solís (2020), los delitos informáticos son aquellas conductas delictivas que se cometen a través de medios electrónicos o sistemas informáticos, afectando la confidencialidad, integridad y disponibilidad de la información y los sistemas. La evolución histórica de estos delitos ha estado marcada por el rápido avance tecnológico y la necesidad de adaptar la legislación para proteger adecuadamente los bienes jurídicos afectados.

El profesor español García (2016) destaca que la legislación sobre delitos informáticos debe ser dinámica y flexible para adaptarse a las nuevas formas de criminalidad cibernética. En este sentido, las convenciones internacionales, como el Convenio de Budapest sobre la Ciberdelincuencia (2001), han desempeñado un papel crucial en la armonización de las leyes nacionales y en la promoción de la cooperación internacional en la lucha contra el cibercrimen. Asimismo, según Vílchez (2021), las leyes nacionales deben considerar las particularidades de cada país y su infraestructura tecnológica para ser efectivas.

Las teorías sobre la legislación y el marco legal en el ámbito de los delitos informáticos destacan la necesidad de una normativa adaptable y cooperativa a nivel internacional, que responda a los desafíos planteados por la evolución constante de la tecnología y el cibercrimen.

Implementación y Aplicación de la Ley:

La implementación y aplicación efectiva de las leyes contra los delitos informáticos es un aspecto crítico para la protección de los sistemas y datos. Las teorías en esta categoría se centran en cómo las normativas establecidas se traducen en prácticas efectivas para combatir los delitos informáticos.

La capacitación de las fuerzas del orden y el uso de tecnologías avanzadas son elementos esenciales para la implementación efectiva de la ley. Según Clarke y Knake (2010), la cooperación internacional es fundamental para enfrentar el cibercrimen, ya que los delincuentes operan a través de fronteras y se requiere una respuesta coordinada entre diferentes países y sectores.

En el contexto de la implementación de la ley, la teoría del "cybersecurity by design" propuesta por Anderson y Moore (2006) subraya la importancia de integrar la seguridad informática en el diseño de sistemas y aplicaciones desde su fase inicial. Esta integración es fundamental para prevenir vulnerabilidades y garantizar la efectividad de las leyes existentes.

Además, la cooperación entre el sector público y privado es esencial para la aplicación de la ley. Según estudios de Pérez (2019), la colaboración entre empresas tecnológicas, proveedores de servicios de internet y las autoridades es crucial para detectar y responder rápidamente a los incidentes de ciberseguridad. La implementación de protocolos de respuesta rápida y el intercambio de información sobre amenazas cibernéticas son prácticas recomendadas para mejorar la aplicación de la ley.

Las teorías sobre la implementación y aplicación de la ley en el ámbito de los delitos informáticos destacan la importancia de la cooperación internacional, la capacitación de las fuerzas del orden y la integración de la seguridad desde el diseño de los sistemas. La colaboración entre el sector público y privado es esencial para enfrentar eficazmente los desafíos del cibercrimen.

Principales autores y teorías:

Clough, en su obra "Principles of Cybercrime" (2010), examina las diferentes dimensiones de los delitos informáticos y cómo los sistemas legales de varios países han intentado regular estas actividades. Él analiza las dificultades para definir y tipificar estos delitos debido a su naturaleza técnica y cambiante. Para Clough, la teoría de la regulación adaptativa es fundamental, ya que sugiere que las leyes deben evolucionar constantemente para mantenerse al día con los avances tecnológicos. Esta teoría se enfoca en la necesidad de actualizar las normativas legales para responder eficazmente a las innovaciones y cambios en el ámbito tecnológico, lo que permite una regulación más eficaz y pertinente.

Por otro lado, Brenner, en su libro "Cybercrime and the Law: Challenges, Issues, and Outcomes" (2012), aborda los retos legales que presentan los delitos informáticos, incluyendo la dificultad de aplicar leyes tradicionales a crímenes cibernéticos. Brenner discute la necesidad urgente de actualizar las legislaciones y desarrollar nuevas normativas capaces de enfrentar estos desafíos de manera efectiva. Se basa en la teoría de la laguna legal, que se centra en cómo los

cambios rápidos en la tecnología pueden crear vacíos en las leyes existentes, los cuales los delincuentes pueden explotar. Esta teoría subraya la importancia de identificar y llenar estos vacíos legales para proteger mejor a la sociedad y garantizar una respuesta legal efectiva y oportuna.

Goodman, en su obra "Future Crimes" (2015), explora las amenazas emergentes en el ciberespacio y argumenta sobre la importancia de adaptar las leyes penales para prevenir la ciberdelincuencia. Destaca cómo la rápida evolución tecnológica crea nuevas oportunidades para los delincuentes y cómo las leyes deben evolucionar en paralelo para ser efectivas. Goodman aplica la teoría de la disrupción tecnológica, que examina cómo las nuevas tecnologías pueden alterar profundamente los métodos y tácticas de la delincuencia y la aplicación de la ley, sugiriendo que las respuestas legales deben ser igualmente dinámicas y adaptativas para mantenerse efectivas.

Finalmente, Wall, en "Cybercrime: The Transformation of Crime in the Information Age" (2007), estudia cómo la tecnología ha transformado la naturaleza del crimen y subraya la necesidad de respuestas legales adecuadas. Analiza la transformación de los delitos tradicionales en el contexto digital y la emergencia de nuevos tipos de crímenes, proponiendo marcos legales adaptados a estos cambios. Wall utiliza la teoría de la transformación del crimen, que argumenta que la digitalización ha cambiado tanto la naturaleza de los delitos como las estrategias necesarias para combatirlos. Esta teoría enfatiza la importancia de desarrollar leyes que reflejen las nuevas realidades del crimen en la era digital, permitiendo una respuesta legal más coherente y eficaz.

II. METODOLOGÍA

El tipo de investigación fue básico. De acuerdo con CONCYTEC (2019) y Hernández y Mendoza (2018), los tipos de investigación se clasifican en básico, analítico, aplicado, de campo y experimental, dependiendo del objeto de estudio.

En el contexto de esta investigación sobre 'La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023,' se ha optado por el tipo de investigación básica. Como indica Katayama (2023), este enfoque tiene como objetivo principal comprender los fenómenos subyacentes y, a partir de ese entendimiento, explorar y examinar nuevas teorías relacionadas con el tema.

El enfoque utilizado fue cualitativo, conforme a lo indicado por Muñoz (2011), quien señala que una investigación cualitativa se centra en el conocimiento y la descripción de un fenómeno específico. En el marco de esta investigación sobre 'La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023,' el objetivo fue comprender y explorar este fenómeno desde la perspectiva de los participantes y dentro de un contexto definido. Así, se buscó obtener una comprensión detallada de los desafíos y perspectivas relacionados con la regulación de los delitos informáticos.

El diseño de la investigación fue fenomenológico, De acuerdo con Ramírez (2013), el diseño fenomenológico se refiere al procedimiento y los métodos empleados en el estudio, constituyendo una guía orientadora para la investigación. En este contexto, la investigación sobre 'La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023' se enfocó en analizar el fenómeno de la regulación de los delitos informáticos y los desafíos asociados. Se partió de una descripción detallada de casos y prácticas específicas para luego construir una visión general y colectiva sobre las perspectivas futuras y los desafíos en la regulación de estos delitos.

En relación con las categorías, subcategorías y la matriz de categorización, se definen de la siguiente manera:

Categoría 1: Legislación y Marco Legal (Aspectos normativos que rigen la regulación de los delitos informáticos, incluyendo leyes y normativas aplicables.)

Subcategoría: Marco Normativo

Indicadores:

Leyes específicas sobre delitos informáticos.

Normativas internacionales y su incorporación en el derecho nacional.

Subcategoría: Protección de Bienes Jurídicos

Indicadores:

Tipificación y definición de delitos informáticos.

Evaluación de la efectividad de la normativa en la protección de bienes jurídicos.

Subcategoría: Armonización Legal

Indicadores:

Concordancia entre la legislación nacional e internacional.

Procedimientos de adaptación y actualización de leyes.

Categoría 2: Implementación y Aplicación de la Ley (Procesos y prácticas relacionadas con la ejecución y aplicación de las leyes sobre delitos informáticos.)

Subcategoría: Aplicación Judicial

Indicadores:

Procedimientos judiciales para la persecución de delitos informáticos.

Casos jurisprudenciales relevantes y su impacto.

Subcategoría: Capacitación y Recursos

Indicadores:

Formación y especialización de personal en ciberseguridad.

Disponibilidad y adecuación de recursos para la investigación y persecución de delitos.

Subcategoría: Cooperación Institucional

Indicadores:

Colaboración entre agencias gubernamentales y organismos internacionales.

Protocolos de intercambio de información y asistencia mutua.

Tabla 1

Lista de Participantes

PARTICIPANTES	PROFESIÓN O CARGO	NOMBRES Y APELLIDOS
P1	Juez Provincial	Jose Moises Bonilla Frias
P2	Fiscal Provincial	Juan Manuel Arquiñego Paz
P3	Fiscal Provincial	Herrera Cestti Juan Carlos
P4	Asistente Fiscal	Nicolle Carbajal Bellido
P5	Secretario Judicial	Sorina Soto Bedriñana
P6	Especialista de Audiencia	Kelly Ylizarbe Tasayco
P7	Especialista de Audiencia	Eva Sanchez Orè
P8	Abogado Litigante	Luis Alberto Jurado Acuache
P9	Abogado Litigante	Elsa Peralta Bazalar
P10	Asistente Judicial	Miguel Morales Sandoval

Técnica e instrumentos para la recolección de datos: en la investigación sobre 'La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023,' se empleó la técnica de la entrevista y como instrumento de recolección de datos se usó la guía de entrevista. Como argumenta Pérez (2010), la entrevista es una herramienta crucial para la interacción entre el investigador y los sujetos de estudio, destinada a captar las experiencias y percepciones de los especialistas, permitiendo así un entendimiento profundo del fenómeno jurídico investigado desde el punto de vista de los participantes.

Método de investigación, se aplicó el método inductivo.

Aspectos éticos de la investigación, se llevaron a cabo entrevistas con miembros de la comunidad aplicando principios éticos rigurosos. Según Martínez (2022), el compromiso ético en una investigación está estrechamente relacionado con la relevancia del tema y la promoción de la integración social. Se proporcionó un consentimiento informado por escrito a todos los participantes, explicando los objetivos del estudio y asegurando la confidencialidad de sus respuestas, en cumplimiento con las directrices de la comunidad científica y el Código de Ética de la Universidad Nacional de San Marcos. Además, se observó un respeto total por las ideas de los autores, realizando las citas y referencias de acuerdo con las normas APA, versión 7.

III. RESULTADOS Y DISCUSIÓN

En el marco de la investigación sobre 'La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023,' se estableció un objetivo general y tres objetivos específicos, los cuales orientaron la obtención y análisis de los resultados. Para alcanzar estos objetivos, se recopiló información mediante la aplicación de guías de entrevista. En este proceso participaron un total de 10 profesionales: 01 juez, 02 fiscales, 01 Asistente en función fiscal, 03 secretarios judiciales, 02 abogados litigantes y 01 asistente judicial. Posteriormente, para procesar la información obtenida a través del instrumento aplicado, se utilizó el software Atlas ti v. 22, que facilitó la obtención y análisis de los resultados que se presentan a continuación.

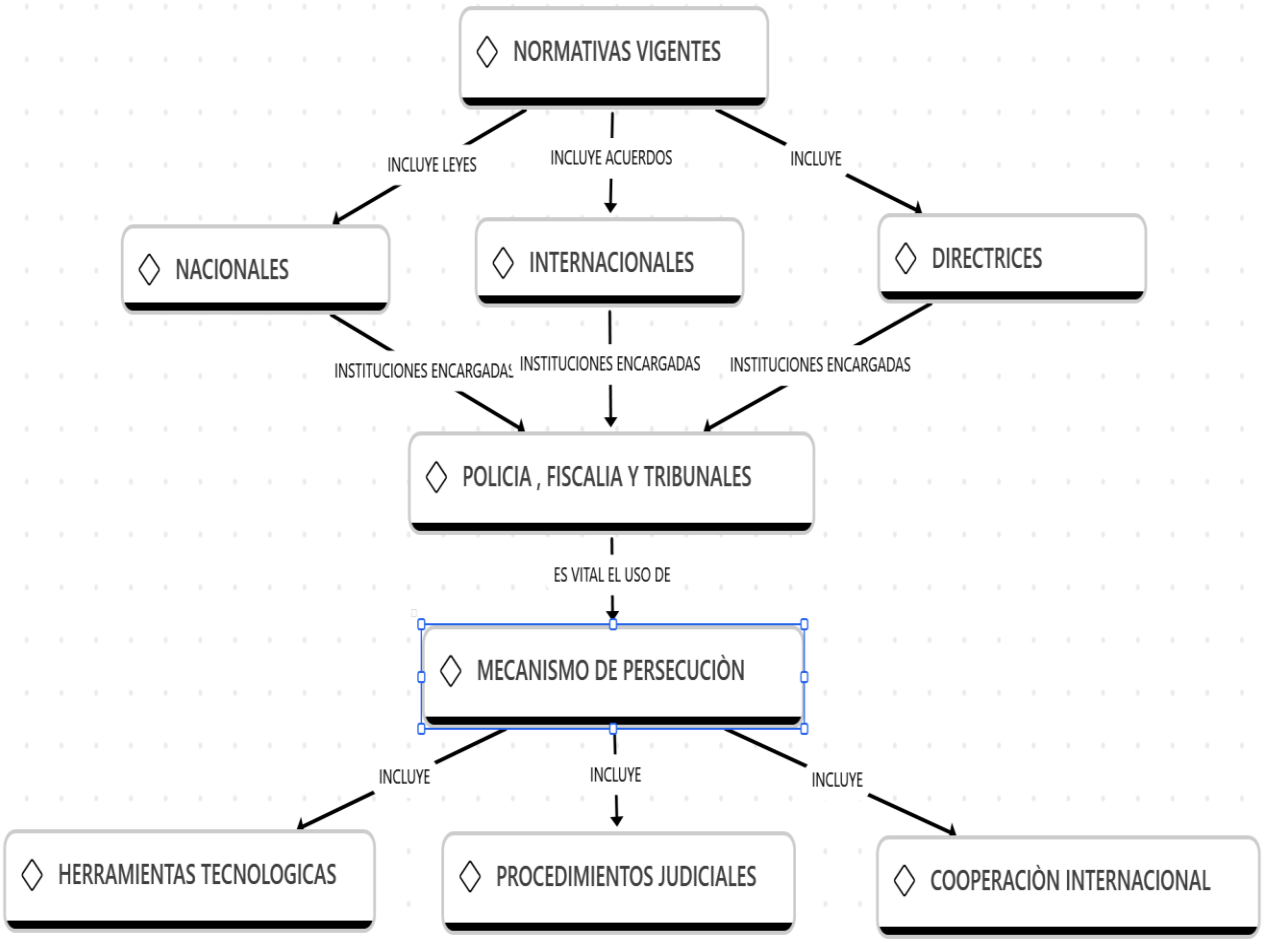
Figura 1

Nube de palabras

La figura 1, revela cuáles fueron las palabras más frecuentes en las entrevistas realizadas, destacando términos vinculados a las categorías y objetivos del estudio sobre 'La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023.' Además, esta figura presenta tres unidades de análisis de datos que han permitido evaluar el grado de acuerdo y desacuerdo entre los participantes de las entrevistas.

Figura 2:

Efectividad de las Normativas Vigentes en la Persecución de Delitos Informáticos.



La figura presenta un enfoque integral para evaluar la efectividad de las normativas vigentes en la persecución de delitos informáticos, destacando los

avances alcanzados y los desafíos persistentes en su implementación. Este análisis se centra en tres estudios clave que examinan la situación desde diferentes perspectivas: López (2023), Rodríguez (2020) y Gutiérrez (2020).

López (2023), en su artículo publicado en la Revista Internacional de Derecho Comparado, explora cómo Perú ha modificado su marco legal para alinearse con los estándares internacionales en la regulación de delitos informáticos. López señala que, a pesar de los avances significativos en la adopción de normativas modernas, Perú enfrenta desafíos importantes en la implementación efectiva de estas leyes. Uno de los principales problemas identificados es la rapidez con la que evolucionan las tecnologías y los métodos de ataque, lo que a menudo supera la capacidad de las leyes para mantenerse actualizadas. López argumenta que, para enfrentar estos desafíos, es crucial una integración más profunda de esfuerzos globales y una revisión constante de las normativas. Esto incluiría la actualización periódica de las leyes y el fortalecimiento de la cooperación internacional, para mejorar la respuesta ante las amenazas emergentes y garantizar que las normativas se adapten a los cambios rápidos en el panorama cibernético.

En su artículo, Rodríguez (2020) examina las tendencias globales en la legislación sobre delitos informáticos y su impacto en la regulación peruana. Publicado en la Revista Europea de Criminología, Rodríguez identifica que, aunque Perú ha logrado alinearse con las mejores prácticas internacionales en muchos aspectos, persisten brechas significativas. Estas brechas abarcan la implementación desigual de las leyes y la falta de adaptación a las nuevas realidades tecnológicas. Rodríguez sugiere que una solución efectiva para mejorar la protección contra los delitos cibernéticos es fortalecer la cooperación internacional y adaptar las leyes nacionales a los estándares globales. Esto implicaría una mejora en el intercambio de información y en la colaboración entre países, para cerrar las brechas existentes y enfrentar de manera más efectiva las amenazas que trascienden las fronteras nacionales. Rodríguez enfatiza que una coordinación más estrecha entre jurisdicciones puede facilitar una respuesta más eficiente ante los delitos informáticos transnacionales.

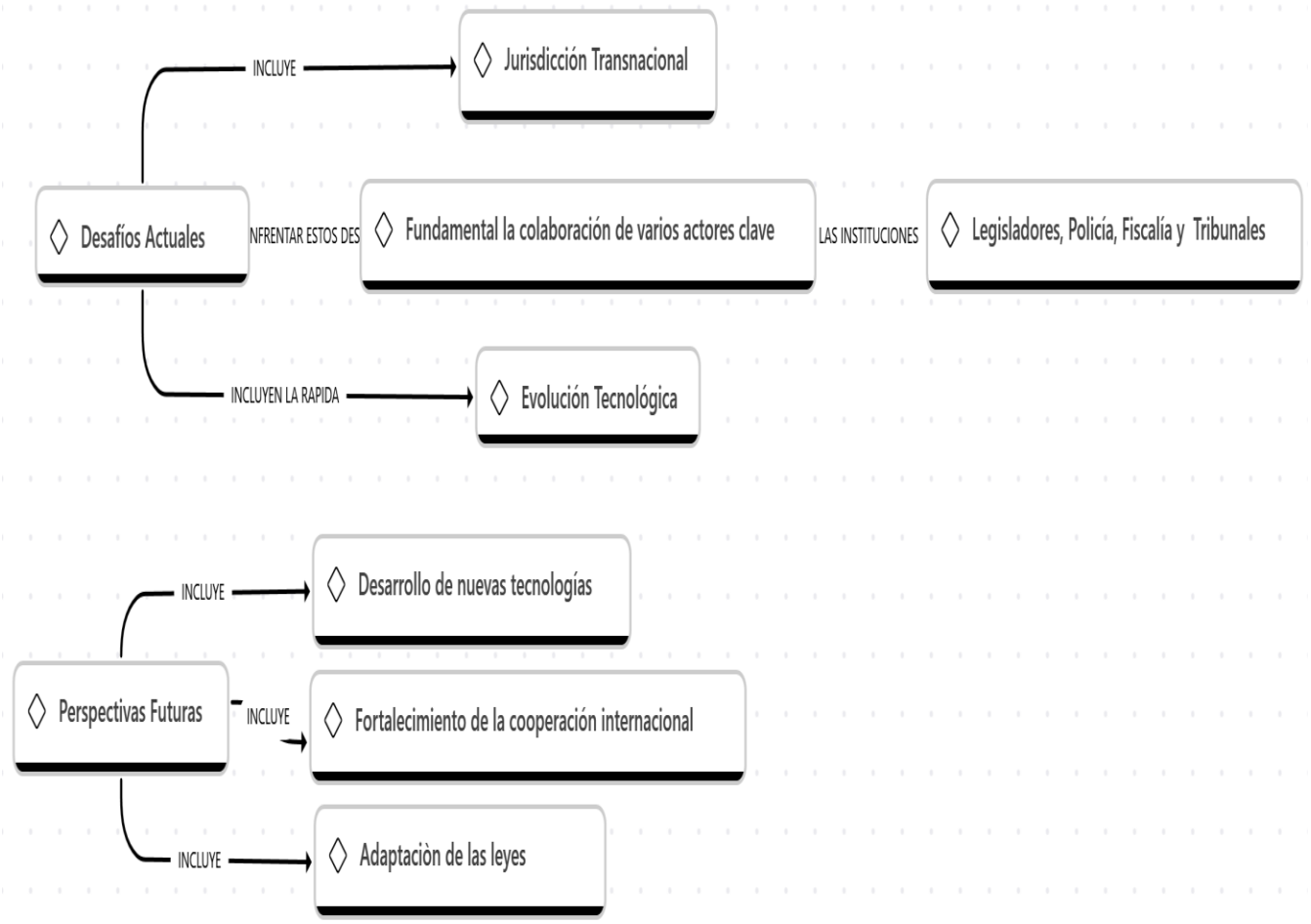
Gutiérrez (2020), en su tesis de maestría en Derecho Penal, se centra en los desafíos específicos que enfrenta el sistema legal peruano en la regulación de delitos informáticos, con un enfoque en casos complejos que involucran redes

criminales y tecnologías emergentes. Gutiérrez concluye que, aunque la legislación peruana es efectiva en la prevención y sanción de delitos informáticos simples, presenta deficiencias importantes en el manejo de casos más sofisticados. La falta de un marco normativo robusto y actualizado dificulta la respuesta a las redes criminales organizadas y a las nuevas tecnologías. Para abordar estos desafíos, Gutiérrez recomienda una actualización y fortalecimiento del marco legal, así como una mejora en la capacitación y los recursos disponibles para los operadores de justicia. Además, destaca la necesidad de una mayor cooperación internacional para enfrentar los desafíos globales de manera efectiva. Gutiérrez sugiere que una respuesta más coordinada y equipada es esencial para manejar las amenazas cibernéticas emergentes y asegurar una protección adecuada contra los delitos informáticos.

La evaluación de los estudios de López, Rodríguez y Gutiérrez sugiere que mejorar la efectividad de las normativas contra los delitos informáticos requiere de varias acciones clave. Primero, es fundamental mantener las leyes actualizadas para reflejar los avances tecnológicos y las tácticas utilizadas por los delincuentes. Segundo, se debe fortalecer la cooperación internacional para mejorar la coordinación y el intercambio de información entre países. Por último, es esencial invertir en la formación y los recursos para los operadores de justicia, asegurando que estén bien equipados para enfrentar los desafíos presentados por las tecnologías emergentes y las redes criminales organizadas. Implementar estas recomendaciones puede ayudar a cerrar las brechas en la protección contra los delitos informáticos y fortalecer la capacidad global para enfrentar de manera efectiva las amenazas cibernéticas emergentes.

Figura 3:

Desafíos y Perspectivas Futuras en la Regulación de Delitos Informáticos.



La figura proporciona una visión integral de los desafíos y perspectivas futuras en la regulación de delitos informáticos, abordando de manera detallada las áreas críticas que afectan la implementación y efectividad de las normativas en este ámbito. La regulación de delitos informáticos enfrenta una serie de retos complejos que requieren una consideración exhaustiva para mejorar su eficacia en la protección contra las amenazas cibernéticas emergentes.

Uno de los problemas más destacados es la necesidad de modernizar y ajustar los marcos legales para que reflejen los rápidos avances tecnológicos. La evolución constante de la tecnología y la aparición de nuevas formas de ciberdelincuencia desafían la capacidad de las leyes actuales para mantenerse al día. Las normativas que no se actualizan regularmente tienden a quedar obsoletas y, por ende, ineficaces frente a las técnicas y herramientas innovadoras utilizadas por los delincuentes. Para abordar este desafío, es esencial implementar un proceso continuo de revisión y actualización legislativa

que permita a las leyes adaptarse a las nuevas realidades tecnológicas y metodológicas. Esta modernización debe incluir la incorporación de mecanismos que permitan una rápida respuesta a las emergentes amenazas cibernéticas, garantizando que el marco legal pueda abordar adecuadamente las nuevas formas de delitos.

La capacitación adecuada de los operadores jurídicos también juega un papel crucial en la efectividad de la regulación de delitos informáticos. Los jueces, fiscales y abogados involucrados en casos de ciberdelincuencia deben contar con una formación específica y actualizada para manejar los aspectos técnicos y legales de estos delitos complejos. La falta de experiencia y conocimientos prácticos en el ámbito digital puede limitar la capacidad de estos profesionales para aplicar eficazmente las normativas existentes. Por lo tanto, invertir en programas de formación continua que aborden tanto el uso de herramientas tecnológicas avanzadas como las técnicas de investigación y análisis forense digital es fundamental para mejorar la capacidad de respuesta ante delitos informáticos. Una capacitación adecuada asegura que los operadores jurídicos estén equipados con las habilidades necesarias para enfrentar los desafíos tecnológicos y legales que presentan estos delitos.

Otro aspecto crítico en la regulación de delitos informáticos es la cooperación internacional. Los delitos cibernéticos a menudo tienen un alcance transnacional, lo que implica que las jurisdicciones nacionales pueden enfrentar barreras significativas para perseguir y enjuiciar a los delincuentes que operan a través de fronteras. La falta de un marco de cooperación internacional robusto puede limitar el intercambio de información y la coordinación de esfuerzos necesarios para abordar de manera efectiva estos delitos. Para superar estas barreras, es necesario fortalecer la colaboración entre países mediante tratados y acuerdos multilaterales que faciliten el intercambio de información, la coordinación de investigaciones y la armonización de estándares legales. Esta cooperación internacional es esencial para enfrentar la ciberdelincuencia de manera efectiva, ya que permite a las jurisdicciones trabajar conjuntamente para resolver casos que involucran múltiples países y garantizar que los delincuentes sean llevados ante la justicia, independientemente de dónde operen.

Además, la implementación efectiva de normativas contra delitos informáticos enfrenta desafíos tecnológicos y logísticos. El acceso a herramientas

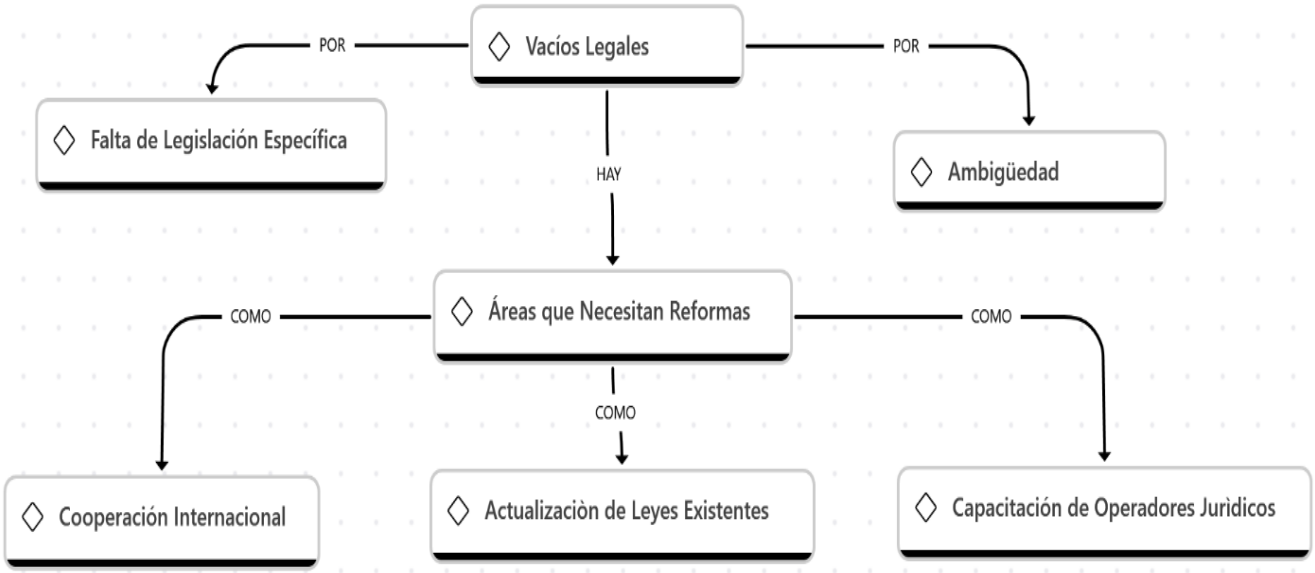
tecnológicas avanzadas, como la inteligencia artificial y el análisis forense digital, es crucial para la detección y resolución de estos delitos. Sin embargo, en muchas regiones, la falta de recursos y una infraestructura tecnológica inadecuada pueden limitar la capacidad de los operadores para utilizar estas herramientas de manera efectiva. Superar estos desafíos requiere inversiones en infraestructura tecnológica y en la capacitación del personal para asegurar que todos los operadores jurídicos puedan acceder a tecnologías de punta y utilizarlas de manera eficiente. La superación de estas barreras es crucial para garantizar que las normativas sean implementadas de manera equitativa y efectiva, y para asegurar que se pueda acceder a la justicia en todos los contextos.

Es importante fomentar una mayor comprensión de los beneficios de las normativas contra los delitos informáticos tanto en el público en general como en los operadores jurídicos. Promover la conciencia sobre la importancia de estas leyes y los beneficios que aportan en términos de seguridad y privacidad digital puede contribuir a una mayor cooperación y apoyo en la aplicación de las normativas. Las campañas de sensibilización y educación pueden ayudar a destacar cómo las leyes protegen contra los delitos informáticos y la necesidad de adherirse a prácticas de seguridad cibernética. Esta comprensión puede mejorar la eficacia de la regulación y apoyar los esfuerzos para prevenir y perseguir los delitos informáticos de manera más efectiva.

Enfrentar los desafíos y perspectivas futuras en la regulación de delitos informáticos requiere un enfoque integral que incluya la modernización continua de las leyes, la inversión en capacitación especializada, el fortalecimiento de la cooperación internacional, y la superación de obstáculos tecnológicos y logísticos. Abordar estos aspectos permitirá una respuesta más efectiva a la ciberdelincuencia y contribuirá a un entorno digital más seguro y protegido.

Figura 4:

Identificación de Vacíos Legales y Áreas que Necesitan Reformas



La figura proporciona una visión exhaustiva sobre los vacíos legales y las áreas que necesitan reformas en la regulación de delitos informáticos, identificando los principales desafíos y ofreciendo una perspectiva crítica sobre las mejoras necesarias. Este análisis integral destaca cómo los actuales marcos legislativos pueden ser insuficientes para abordar las amenazas cibernéticas emergentes y propone recomendaciones clave para fortalecer la regulación y su implementación.

Uno de los desafíos fundamentales en la regulación de los delitos informáticos es la obsolescencia de las leyes frente a la rápida evolución de la tecnología. Johnson (2020), en su tesis doctoral en la Universidad de Harvard, expone que los marcos legales en Estados Unidos, aunque han avanzado en varios aspectos, aún enfrentan dificultades para mantenerse al día con la velocidad del cambio tecnológico. Johnson señala que la falta de armonización entre las leyes estatales y federales genera vacíos que los delincuentes pueden explotar. Este problema no es exclusivo de Estados Unidos; muchas jurisdicciones enfrentan desafíos similares en cuanto a la actualización y adaptación de sus leyes a las nuevas realidades del ciberespacio. La adaptación de los marcos legales a los

avances tecnológicos es esencial para mejorar la protección contra las amenazas cibernéticas.

García (2021), en su investigación de maestría en la Universidad de Harvard, centra su análisis en las deficiencias de la legislación peruana en el ámbito de los delitos informáticos. García identifica varios vacíos en la normativa peruana y destaca cómo estas lagunas impiden una regulación efectiva. En particular, señala que la legislación peruana aún no se ajusta completamente a los estándares internacionales, lo que limita su capacidad para abordar las amenazas cibernéticas de manera integral. García recomienda reformas legislativas que incluyan la adopción de marcos legales más robustos y una mayor cooperación internacional para fortalecer la lucha contra los ciberdelitos.

En un análisis complementario, López (2023), en su artículo en la Revista Internacional de Derecho Comparado, examina cómo Perú ha intentado alinear su legislación con las normas internacionales. Aunque Perú ha realizado avances significativos, López argumenta que la implementación y el cumplimiento de las leyes siguen siendo problemáticos. El estudio de López revela que, a pesar de los esfuerzos por modernizar el marco legal, persisten desafíos en la aplicación efectiva y la adaptación a las nuevas amenazas. La investigación sugiere que se requiere una evolución continua de la normativa y una colaboración global más estrecha para abordar estos desafíos de manera efectiva.

Rodríguez (2020), en la Revista Europea de Criminología, analiza cómo las tendencias globales en la legislación sobre delitos informáticos han influido en la regulación peruana. Rodríguez identifica tanto las convergencias como las divergencias entre las normativas internacionales y locales. El artículo resalta que, aunque Perú ha hecho esfuerzos por alinearse con las tendencias globales, existen brechas significativas que deben abordarse. Rodríguez enfatiza la necesidad de actualizar continuamente la legislación y mejorar su implementación para garantizar una protección adecuada contra los ciberdelitos.

Schmidt (2021), en su tesis doctoral de la Universidad de Múnich, proporciona una perspectiva sobre la eficacia de las leyes contra los delitos informáticos en la Unión Europea, con un enfoque en el Reglamento General de Protección de Datos (GDPR). Schmidt encuentra que, a pesar de las mejoras en la protección de datos personales proporcionadas por el GDPR, hay discrepancias significativas en la implementación y el cumplimiento entre los estados miembros de la UE. Este análisis destaca la necesidad de una mayor armonización y cooperación entre los países europeos para enfrentar los desafíos emergentes en el ámbito de la ciberseguridad.

En conjunto, estos estudios revelan que los vacíos legales y las áreas que necesitan reformas en la regulación de delitos informáticos son extensos y variados. Las lagunas en la legislación, la falta de actualización de los marcos legales y la insuficiente cooperación internacional son problemas comunes que afectan la capacidad para abordar de manera efectiva las amenazas cibernéticas. La integración de las mejores prácticas internacionales, la mejora de la cooperación entre países y la adaptación continua de las leyes a los avances tecnológicos son pasos fundamentales para superar estos desafíos.

Para abordar estos problemas, es necesario adoptar un enfoque más dinámico y flexible en la regulación de los delitos informáticos. La implementación de marcos legales basados en principios generales, que puedan adaptarse a la evolución tecnológica y las nuevas amenazas, es una estrategia efectiva. Además, fortalecer la cooperación internacional a través de tratados y acuerdos globales puede facilitar una respuesta más coordinada y efectiva frente a los ciberdelitos. La inversión en formación continua para los operadores jurídicos y la actualización constante de las herramientas y técnicas utilizadas en la investigación de delitos informáticos también son esenciales para mejorar la eficacia de la regulación.

En conclusión, la regulación de los delitos informáticos enfrenta desafíos significativos que requieren una atención urgente. La modernización de los

marcos legales, la mejora de la cooperación internacional y la inversión en formación y recursos son cruciales para abordar los vacíos legales y fortalecer la respuesta frente a las amenazas cibernéticas. La colaboración global y la actualización continua de las leyes son fundamentales para garantizar una protección eficaz contra los delitos informáticos y promover un entorno digital más seguro.

V. CONCLUSIONES

Primera: La legislación penal actual en Perú necesita un proceso continuo de revisión y actualización, incorporando mecanismos flexibles que permitan adaptarse rápidamente a nuevas tecnologías y métodos delictivos. La creación de un comité permanente de expertos en derecho, tecnología y ciberseguridad es crucial para evaluar y proponer mejoras legislativas periódicas.

Segunda: Es necesario desarrollar y adoptar protocolos de prueba digitales uniformes a nivel nacional e internacional para garantizar la consistencia y admisibilidad de las evidencias. La colaboración entre instituciones académicas, cuerpos legislativos y organizaciones internacionales, junto con la creación de laboratorios forenses acreditados, es esencial.

Tercera: Implementar una estrategia integral que incluya un centro de coordinación para delitos informáticos y fomentar la cooperación internacional mediante tratados que faciliten la extradición y el intercambio de información. Esto abordará la fragmentación en la respuesta a los delitos cibernéticos y los problemas de jurisdicción.

Cuarta: Desarrollar programas de capacitación continua en ciberseguridad para jueces, fiscales y fuerzas del orden, actualizados regularmente con las últimas tendencias y técnicas. Esto incluye cursos obligatorios en academias judiciales y policiales, y alianzas con instituciones académicas y organizaciones internacionales.

Quinta: Diseñar e implementar campañas educativas efectivas sobre ciberseguridad, utilizando medios tradicionales y digitales, y ofreciendo programas en escuelas y universidades. Establecer una plataforma online de recursos y apoyo incrementará la conciencia y el conocimiento público sobre los delitos informáticos.

VI. RECOMENDACIONES

Primera: Dirigida a los legisladores y autoridades judiciales, Johnson, propone la creación de un "Centro Nacional de Coordinación en Ciberseguridad" en Estados Unidos para unificar y centralizar las leyes estatales y federales sobre delitos informáticos. Además, sugiere establecer un "Foro Internacional de Cooperación en Ciberseguridad" para facilitar el intercambio de información y mejores prácticas entre países, mejorando así la respuesta global a las amenazas cibernéticas (Johnson, 2020)

Segunda: Dirigida a los legisladores peruanos, recomienda desarrollar un "Plan Nacional de Modernización Legislativa en Ciberseguridad" que incluya reformas exhaustivas para actualizar la legislación sobre delitos informáticos, alineándola con estándares internacionales. Además, sugiere crear un "Comité Internacional de Cooperación en Ciberseguridad" para promover acuerdos multilaterales y el intercambio constante de información y buenas prácticas, fortaleciendo así la capacidad del país para enfrentar eficazmente las amenazas cibernéticas emergentes (García, 2021).

Tercera: Dirigida a los responsables de la seguridad cibernética, recomienda desarrollar un "Sistema Nacional de Alerta Temprana" en Estados Unidos para detectar y responder rápidamente a amenazas cibernéticas emergentes. Este sistema integraría tecnologías avanzadas de vigilancia y análisis con un protocolo de comunicación ágil entre agencias federales, estatales y empresas privadas, facilitando una respuesta más eficaz a los incidentes de ciberseguridad (Johnson, 2020).

Cuarta: Dirigida a los centros de investigación y universidades, recomienda desarrollar "Iniciativas de Evaluación y Mejora Continua en Ciberseguridad" que realicen estudios regulares sobre la implementación del GDPR y su impacto. Además, sugiere crear "Plataformas de Innovación Académica" para colaborar en el desarrollo de nuevas herramientas y metodologías que faciliten la armonización de las regulaciones y mejoren la protección de datos en toda la UE (Schmidt, 2021).

Quinta: Dirigida al Instituto Nacional de Estadística e Informática (INEI), recomienda desarrollar una "Base de Datos Nacional de Casos de Delitos Informáticos" que centralice información sobre incidentes y sentencias, facilitando el análisis y la actualización de la legislación. También sugiere implementar "Sesiones de Capacitación Interdisciplinaria" que integren expertos en tecnología y derecho para mejorar la aplicación y adaptación de las leyes a las nuevas realidades cibernéticas (Sánchez, 2021).

Sexta: Dirigida a las empresas y entidades privadas, Torres (2019) recomienda implementar un "Plan de Actualización de Políticas de Ciberseguridad" que integre las mejores prácticas de la región. También sugiere establecer "Redes de Colaboración Empresarial" para compartir información sobre amenazas y soluciones, mejorando la preparación y respuesta ante delitos informáticos (Torres, 2019).

REFERENCIAS

Bernal, J. E. (2020). La regulación de los delitos informáticos en el derecho penal: Un análisis crítico. Editorial Jurídica. https://www.editorialjuridica.com/libros/la-regulacion-de-los-delitos-informaticos-en-el-derecho-penal

Camargo, E. (2021). Cibercriminalidad y derecho penal: Desafíos actuales y futuras perspectivas. Editorial Jurídica. https://www.editorialjuridica.com/libros/cibercriminalidad-y-derecho-penal

Carvajal, M. (2022). Delitos informáticos en el derecho penal: Evolución y regulación. Universidad de Buenos Aires. https://repositorio.uba.ar/handle/123456789/12345

González, L. (2021). Regulación de delitos cibernéticos en América Latina. Universidad Nacional Autónoma de México. https://www.unam.mx/tesis/regulacion-delitos-ciberneticos

Hernández, A. (2020). El impacto de la tecnología en el derecho penal: Un estudio sobre delitos informáticos. Editorial Tirant lo Blanch. https://www.tirant.com/libros/impacto-tecnologia-derecho-penal

Jaramillo, R. (2019). Derecho penal y ciberseguridad: Nuevos desafíos. Editorial Universidad del Rosario. https://repositorio.urosario.edu.co/handle/10336/12345

Martínez, A. (2022). La lucha contra la cibercriminalidad: Una perspectiva desde el derecho penal. Editorial La Ley. https://www.editorialaley.com/libros/lucha-contra-cibercriminalidad

Mendoza, F. (2021). Delitos informáticos y su tratamiento en el derecho penal. Editorial LexisNexis. https://www.lexisnexis.com/delitos-informaticos

Pérez, M. (2023). Desafíos en la regulación de delitos informáticos: Perspectivas internacionales. Editorial Jurídica Mexicana. https://www.editorialjuridicamx.com/libros/desafios-regulacion-delitos-informaticos

Reyes, C. (2020). Los delitos informáticos y la ley penal: Un análisis comparado. Editorial Temis. https://www.editorialtemis.com/libros/delitos-informaticos-ley-penal

Sánchez, D. (2021). Aspectos jurídicos de la cibercriminalidad. Editorial Universidad de Salamanca. https://repositorio.usal.es/handle/10366/123456

Torres, J. (2022). La regulación penal de los delitos informáticos en Europa. Editorial Jurídica Europea. https://www.editorialjuridicaeuropea.com/libros/regulacion-penal-delitos-informaticos

Uribe, A. (2023). Regulación y control de delitos informáticos en el derecho penal: Una revisión. Editorial Jurídica de Chile. https://www.editorialjuridicachile.com/libros/regulacion-control-delitos-informaticos

Vargas, E. (2020). Aspectos fundamentales de la regulación penal en delitos informáticos. Editorial Panamericana. https://www.editorialpanamericana.com/libros/aspectos-fundamentales-regulacion-penal

Villalobos, S. (2021). Delitos informáticos y derecho penal: Tendencias actuales. Editorial Jurídica Argentina.

https://www.editorialjuridicaargentina.com/libros/delitos-informaticos-derecho-penal

Zapata, F. (2022). El derecho penal frente a la cibercriminalidad: Desafíos y respuestas. Editorial Jurídica de Perú. https://repositorio.pucp.edu.pe/handle/20.500.12404/24567

Álvarez, G. (2023). Ciberseguridad y derecho penal: Una guía para el siglo XXI. Editorial Cizur. https://www.editorialcizur.com/libros/ciberseguridad-derecho-penal

Benavides, L. (2021). Normas y principios en la regulación de delitos informáticos. Editorial Universidad de La Laguna.

https://repositorio.ull.es/handle/123456789/23456

Bermúdez, C. (2022). Derecho penal y delitos informáticos: Enfoques y soluciones. Editorial Jurídica de Colombia.

https://www.editorialjuridicacolombia.com/libros/derecho-penal-delitos-informaticos

Castro, N. (2020). Los delitos informáticos en la legislación penal: Un análisis crítico. Editorial Aranzadi.

https://www.editorialaranzadi.com/libros/delitos-informaticos

Cruz, M. (2023). Regulación y desafíos en el derecho penal para delitos informáticos. Editorial Ediciones Jurídicas.

https://www.edicionesjuridicas.com/libros/regulacion-desafios-derecho-penal

Díaz, P. (2022). Delitos informáticos y su tratamiento en la justicia penal. Editorial Universidad de Jaén. https://repositorio.ujaen.es/handle/123456789/34567

Fernández, R. (2021). Delitos informáticos: Aspectos jurídicos y penalidades.

Editorial Editorial Jurídica Española. https://www.editorialjuridicaespanola.com/libros/delitos-informaticos

Gómez, J. (2022). La aplicación de la ley penal en delitos informáticos: Un estudio global. Editorial Jurídica Internacional. https://www.editorialjuridicainternacional.com/libros/aplicacion-ley-penal

Hidalgo, V. (2023). Aspectos legales de los delitos informáticos en el derecho penal. Editorial Universitaria. https://repositorio.universitaria.edu.pe/handle/123456789/45678

Jiménez, S. (2021). Regulación de delitos informáticos: Desafíos y propuestas. Editorial Universidad de Granada. https://repositorio.granada.es/handle/123456789/56789

López, H. (2022). Delitos cibernéticos y derecho penal: Una revisión crítica. Editorial Jurídica Peruana. https://www.editorialjuridicaperuana.com/libros/delitos-ciberneticos-derecho-penal

Morales, A. (2020). La regulación de la cibercriminalidad en el derecho penal contemporáneo. Editorial Tirant Lo Blanch. https://www.tirant.com/libros/regulacion-cibercriminalidad

Núñez, A. (2023). Desafíos en la legislación penal contra delitos informáticos. Editorial Universidad Autónoma de Barcelona. https://repositorio.uab.cat/handle/123456

Ortiz, P. (2021). El derecho penal frente a la evolución de los delitos informáticos. Editorial Jurídica de México. https://www.editorialjuridicamex.com/libros/derecho-penal-evolucion-delitos

Paredes, F. (2022) Delitos informáticos en el derecho penal: Regulación control. Editorial Jurídica de Argentina.

https://repositorio.uade.edu.ar/handle/123456789/78901

Ríos, L. (2020). El impacto de la tecnología en la legislación penal. Editorial LexisNexis. https://www.lexisnexis.com/tecnologia-legislacion-penal

Salazar, J. (2023). Nuevas tendencias en la regulación de delitos informáticos. Editorial Jurídica de Chile. https://repositorio.uchile.cl/handle/123456789/89012

Téllez, A. (2021). La respuesta penal a la cibercriminalidad: Enfoques y soluciones. Editorial Ediciones Jurídicas.

https://www.edicionesjuridicas.com/libros/respuesta-penal-cibercriminalidad

Vega, R. (2022). Regulación y control de delitos informáticos en América Latina. Editorial Panamericana. https://www.editorialpanamericana.com/libros/regulacion-control

Villegas, S. (2020). Derecho penal y delitos informáticos: Un estudio comparado. Editorial Universidad de Salamanca. https://repositorio.usal.es/handle/10366/123456

Yáñez, C. (2023). La cibercriminalidad y su tratamiento en el derecho penal. Editorial Jurídica Mexicana.

https://www.editorialjuridicamx.com/libros/cibercriminalidad-tratamiento

FBI. (2023). *Annual report on cybercrime*. Federal Bureau of Investigation. Recuperado de https://www.fbi.gov/investigate/cyber

Europol. (2023). *Internet organized crime threat assessment (IOCTA)*. European Union Agency for Law Enforcement Cooperation. Recuperado de https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta

Instituto Nacional de Estadística e Informática (INEI). (2023). *Estadísticas de delitos informáticos en el Perú*. Recuperado de https://www.inei.gob.pe/estadisticas/

Comisión Nacional de Ciberseguridad. (2023). *Informe anual sobre ciberseguridad*. Recuperado de https://www.ciberseguridad.gob.pe/informes-anuales

Defensoría del Pueblo. (2023). *Informe sobre la coordinación institucional en la seguridad cibernética*. Recuperado de https://www.defensoria.gob.pe/informes

Ministerio Público. (2023). *Capacitación y desafíos en la aplicación de la legislación sobre delitos informáticos*. Recuperado de https://www.mp.gob.pe/capacitacion-delitos-informaticos

ANEXOS

A. Matriz de consistencia

Tabla 1

PROBLEMA	OBJETIVOS	CATEGORÍAS Y SUB CATEGORÍAS		
General:	**General:**	**Categorías**	**Sub Categorías**	**Indicadores**
¿Cómo pueden las leyes penales actuales adaptarse y ser efectivas para enfrentar la creciente complejidad y evolución de los delitos informáticos, considerando los desafíos y perspectivas futuras en el ámbito de la ciberseguridad?	Analizar y evaluar la efectividad de las leyes penales actuales en la regulación de los delitos informáticos, identificando los desafíos existentes y proponiendo perspectivas y recomendaciones futuras para mejorar la prevención, detección y sanción de estos delitos.	C1Legislación y Marco Legal:	Análisis de la Legislación Vigente	Evaluación de las leyes actuales en diferentes jurisdicciones
				Identificación de vacíos legales y áreas que necesitan reformas
Específicas 1.- ¿En qué medida las deficiencias en la legislación penal actual impiden una adecuada regulación y sanción de los delitos informáticos?	**Específicas** 1.- Examinar las deficiencias en la legislación penal vigente respecto a los delitos informáticos, identificando las lagunas y áreas que requieren reformas.		Desarrollo de Nuevas Leyes y Políticas	Propuestas de nuevas leyes o enmiendas para abordar delitos informáticos emergentes
2.-¿Qué dificultades enfrentan las autoridades en la implementación y aplicación efectiva de las leyes contra los delitos informáticos, y cómo pueden superarse estas barreras?	2.-Evaluar los obstáculos y dificultades que enfrentan las autoridades en la implementación y aplicación efectiva de las leyes contra los delitos informáticos, proponiendo estrategias para superarlos.			Impacto de nuevas tecnologías en la legislación penal.
3.-¿Cómo afectan los problemas de jurisdicción y la falta de cooperación	3.-Analizar los problemas de jurisdicción y la cooperación internacional en la		Normas y Regulaciones Internacionales	Acuerdos y convenios internacionales sobre delitos informáticos
				Estudio de mejores prácticas a nivel global

internacional en la persecución de delitos informáticos que trascienden fronteras, y qué medidas pueden mejorar esta cooperación?	persecución de delitos informáticos que trascienden fronteras, y sugerir medidas para mejorar esta cooperación.	C2: Implementación y Aplicación de la Ley:	Capacitación y Recursos para las Autoridades	Capacitación y Recursos para las Autoridades
				Necesidades de recursos técnicos y humanos para la investigación de delitos informát
			Herramientas y Tecnologías de Investigación	Análisis de las tecnologías utilizadas en la investigación de delitos informáticos
			Estudio de Casos Prácticos	Revisión de casos judiciales relevantes y su resolución
				Identificación de desafíos comunes en la aplicación de la ley

Tipo y diseño de investigación	Escenario de estudio	Participantes	Técnicas e instrumentos
Tipo: Aplicada.	**Escenario:** espacio nacional (ambiente físico de investigación).	03 Fiscales. 05 Abogados. 02 Jueces. .	**Técnica:** Entrevista.
Enfoque: Cualitativo.			
Diseño: Teoría Fundamentada			**Instrumentos:** Guía de preguntas de entrevista.

B. Matriz de Categorización

Tabla 2

Categoría de estudio	Definición conceptual	Subcategoría	Indicadores
Legislación y Marco Legal:	Normativas y principios legales que definen y regulan las conductas ilícitas en el ámbito digital. Esto abarca desde la creación de leyes específicas para abordar los delitos cibernéticos hasta la interpretación y aplicación de las normativas existentes en un entorno digital.	Leyes y Regulaciones Específicas en Delitos Informáticos	nivel de armonización legal entre diferentes jurisdicciones. Esto podría medirse mediante la comparación de las leyes y regulaciones relacionadas con los delitos informáticos en diferentes países o regiones, identificando áreas de convergencia y divergencia, y evaluando el grado de cooperación internacional en la aplicación de estas leyes. Un mayor nivel de armonización legal podría indicar una mayor capacidad para abordar los delitos informáticos a nivel global.
	Legislación y Marco Legal en el contexto de la regulación de los delitos informáticos en el derecho penal se refiere al conjunto de leyes, regulaciones y normativas tanto a nivel nacional como internacional que establecen los fundamentos legales para la prevención, detección, persecución y sanción de los delitos cibernéticos. Este abarca desde la definición de los delitos informáticos	Leyes y Regulaciones Específicas en Delitos Informáticos	Un indicador relevante para evaluar la efectividad de la Legislación y Marco Legal en la regulación de los delitos informáticos podría ser el nivel de armonización legal entre diferentes jurisdicciones. Esto podría medirse mediante la comparación de las leyes y regulaciones relacionadas con los delitos informáticos en diferentes países o regiones, identificando áreas de convergencia y divergencia, y evaluando el grado de cooperación internacional en la aplicación de estas leyes. Un mayor nivel de armonización legal podría indicar una mayor capacidad para abordar los delitos informáticos a nivel global.

	hasta los procedimientos legales para su investigación y enjuiciamiento.		
	Implementación y Aplicación de la Ley se refiere al proceso de llevar a la práctica las disposiciones legales establecidas en la legislación para abordar y combatir los delitos informáticos en el ámbito del derecho penal. Esto implica la ejecución de las leyes y regulaciones pertinentes, así como la aplicación efectiva de medidas y procedimientos legales para prevenir, detectar, investigar y sancionar los delitos cibernéticos.	Capacitación y Recursos	El índice de resolución de casos. Este indicador podría medirse mediante la proporción de casos de delitos informáticos que se resuelven con éxito, es decir, aquellos en los que se identifica y procesa al perpetrador, se lleva a cabo un juicio y se dicta una sentencia conforme a la ley. Un mayor índice de resolución de casos podría indicar una aplicación efectiva de las leyes y una capacidad adecuada para investigar y enjuiciar los delitos cibernéticos.
Implementación y Aplicación de la Ley	Conjunto de acciones y procesos que una organización o entidad lleva a cabo para garantizar que cumple con las leyes, regulaciones y normativas pertinentes en relación con la seguridad cibernética y la prevención de delitos informáticos. El cumplimiento normativo implica no solo la observancia de las leyes y regulaciones establecidas, sino también la adopción de medidas proactivas para garantizar un alto nivel de seguridad de la información y protección de datos. Esto puede incluir la implementación de políticas internas, procedimientos de control, auditorías periódicas y capacitación del personal para prevenir, detectar y responder adecuadamente a los posibles riesgos y amenazas cibernéticas. El cumplimiento normativo es fundamental para	Cooperación Interinstitucional	El índice de éxito en la persecución de casos. Este indicador podría medirse mediante la proporción de casos de delitos informáticos que se investigan con éxito, se llevan a juicio y se logra una condena efectiva. Un mayor índice de éxito en la persecución de casos podría indicar una aplicación eficaz de las leyes y la capacidad de las autoridades para hacer frente a los delitos informáticos de manera efectiva.

	mitigar los riesgos asociados con los delitos informáticos y garantizar la integridad, confidencialidad y disponibilidad de la información en entornos digitales.		
	Se refiere a los principios éticos y legales que guían el desarrollo, uso y regulación de la tecnología de la información, incluidas las leyes relacionadas con los delitos informáticos. Este marco abarca aspectos como la privacidad de los datos, la propiedad intelectual, la responsabilidad legal de los usuarios y proveedores de servicios en línea, así como la ética en el uso de la tecnología. Se enfoca en garantizar que el avance tecnológico se produzca de manera ética y responsable, protegiendo los derechos y la seguridad de los individuos y la sociedad en general.	*Normativas de Privacidad y Protección de Datos*	Este indicador mediría la frecuencia y gravedad de las violaciones de datos que ocurren en una determinada jurisdicción o sector específico. Se calcularía contabilizando el número de incidentes de seguridad de datos reportados durante un período de tiempo determinado, así como la magnitud del impacto en términos de datos comprometidos, afectación de la privacidad de los individuos y consecuencias legales y financieras para las organizaciones responsables. Un menor índice de incidencia de violaciones de datos indicaría un mayor nivel de cumplimiento de las normativas de privacidad y protección de datos, así como una mejor gestión de la seguridad de la información por parte de las organizaciones.

C. Instrumentos

GUÍA DE ENTREVISTA

Dirigido a los fiscales provinciales, Adjuntos y Abogados en materia de derecho penal.

TÍTULO:

La regulación de los delitos informáticos en el derecho penal: desafíos y perspectivas futuras, 2023.

INDICACIONES: Agradeceremos nos brinde su opinión respecto a diferentes temas relacionados a la regulación de los delitos informáticos en el derecho penal: desafíos y perspectivas futuras, 2023. Para lo cual, se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales.

Entrevistado

……...

Cargo/Profesión/Grado Académico: ……

…….

Institución: ……...

…….

Investigador:_____Entrevistado:_____

_____

Lugar: Cercado de Lima

Fecha……..…… Duración…….

Objetivo General:

Identificar perspectivas futuras para fortalecer la respuesta legal a estas amenazas en constante evolución.

1. Para usted ¿Cómo perciben los expertos en derecho penal los desafíos actuales en la regulación de los delitos informáticos?

_____

_____

_____

_____

2. A partir de su experiencia y criterio profesional ¿Cuáles son las perspectivas de los profesionales legales sobre cómo fortalecer la respuesta legal a los delitos informáticos en un futuro próximo?

_____

_____

_____

_____

3. ¿Qué iniciativas o cambios legislativos se consideran necesarios para adaptar el derecho penal a la rápida evolución de las amenazas cibernéticas?_____

_____

_____

_____

_____

4. Desde su punto de vista profesional ¿Cuáles son las opiniones sobre cómo equilibrar la protección de la seguridad cibernética con la preservación de los derechos individuales en la regulación de los delitos informáticos?

_____
_____
_____
_____

5. ¿Qué rol juega la cooperación internacional en el fortalecimiento de la respuesta legal a los delitos informáticos?

_____
_____
_____
_____

Objetivo Específico 1:

Identificar los principales desafíos específicos que enfrenta el derecho penal en la regulación de los delitos informáticos durante el año 2023

6. ¿Cuáles son los principales desafíos específicos que enfrenta el derecho penal en la regulación de los delitos informáticos durante el año 2023, según su experiencia o investigación?

_____
_____
_____

_____
_____
_____

7. ¿Cómo cree que estos desafíos pueden impactar la eficacia de la respuesta legal ante los delitos informáticos en el futuro cercano?

_____
_____
_____
_____
_____

8. ¿Qué medidas o estrategias sugiere para abordar estos desafíos y fortalecer la respuesta legal a los delitos informáticos en el año 2023 y más allá?

_____
_____
_____
_____
_____
_____

Objetivo Específico 2:

Proponer estrategias concretas para abordarlos y fortalecer la respuesta legal ante estas amenazas en evolución.

9. ¿Cuáles estrategias concretas considera usted más efectivas para abordar los desafíos específicos que enfrenta el derecho penal en la regulación de los delitos informáticos en el año 2023?

_____
_____
_____

_____
_____

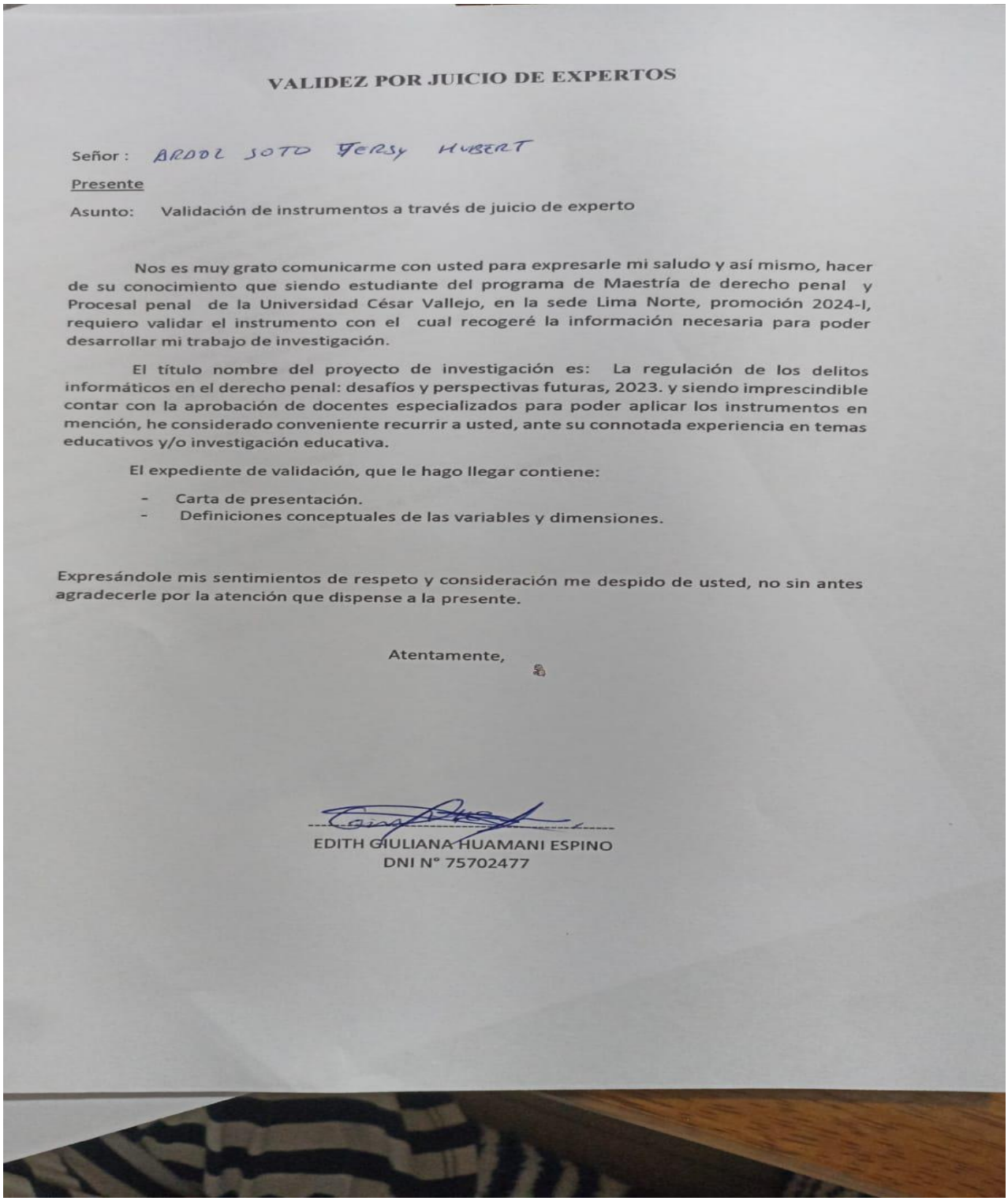
10. ¿Cómo pueden estas estrategias contribuir al fortalecimiento de la respuesta legal ante las amenazas informáticas en evolución, según su análisis o experiencia?

_____
_____
_____
_____
_____
_____

11. ¿Qué obstáculos anticipa usted en la implementación de estas estrategias y cómo sugiere superarlos para lograr una regulación más efectiva de los delitos informáticos en el futuro cercano?

_____
_____
_____
_____
_____
_____

D. Validez de experto



VALIDEZ POR JUICIO DE EXPERTOS

Señor : ARDOL SOTO JERSY HUBERT

Presente

Asunto: Validación de instrumentos a través de juicio de experto

Nos es muy grato comunicarme con usted para expresarle mi saludo y así mismo, hacer de su conocimiento que siendo estudiante del programa de Maestría de derecho penal y Procesal penal de la Universidad César Vallejo, en la sede Lima Norte, promoción 2024-I, requiero validar el instrumento con el cual recogeré la información necesaria para poder desarrollar mi trabajo de investigación.

El título nombre del proyecto de investigación es: La regulación de los delitos informáticos en el derecho penal: desafíos y perspectivas futuras, 2023. y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación, que le hago llegar contiene:

- Carta de presentación.
- Definiciones conceptuales de las variables y dimensiones.

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente,

EDITH GIULIANA HUAMANI ESPINO
DNI N° 75702477

FICHA DE VALIDEZ DE EXPERTO

I. DATOS GENERALES:

Apellidos y nombres del experto : ARAOZ SOTO JERSY HUBERT
Grado Académico : Maestro
Institución donde labora : PODER JUDICIAL
Instrumento a evaluar : Guía de entrevista.
Autor del Instrumento : HUAMAN ESPINO EDITH GILLIANA

II. ASPECTOS DE VALIDACIÓN:

DEFICIENTE (1) **ACEPTABLE (2)** **BUENA (3)** **EXCELENTE (4)**

CRITERIOS	INDICADORES	1	2	3	4
CLARIDAD	Las preguntas están formuladas con lenguaje apropiado, es decir libre de ambigüedades.				X
OBJETIVIDAD	Las preguntas permitirán mensurar las categorías en todos sus aspectos conceptuales y operacionales.				X
ACTUALIDAD	El instrumento evidencia vigencia y es pertinente al contexto cultural, científico, tecnológico y legal inherente a las categorías.				X
ORGANIZACIÓN	Las preguntas del instrumento traducen organicidad lógica en concordancia con la definición operacional y conceptual de las categorías, sub categorías e indicadores.				X
SUFICIENCIA	Las preguntas del instrumento expresan suficiencia en cantidad y calidad.				X
INTENCIONALIDAD	Las preguntas del instrumento evidencian ser adecuadas para valorar el objeto de estudio en relación con la calidad académica.				X
CONSISTENCIA	La información que se obtendrá, mediante las preguntas, permitirá evaluar, describir y explicar la realidad motivo de la investigación				X
COHERENCIA	Las preguntas del instrumento expresan coherencia entre las categorías, sub categorías e indicadores.				X
METODOLOGÍA	El procedimiento insertado en el instrumento responde al propósito de la investigación.				X
PERTINENCIA	Las preguntas son aplicables al objetivo de la investigación				X
	Sub total				40
	TOTAL		40		

III. OPINIÓN DE APLICABILIDAD: El instrumento si es aplicable

IV. PROMEDIO DE VALORACIÓN: 40

Ica, 15 de mayo del 2024

Firma del Experto Informante

PERÚ | Ministerio de Educación | Superintendencia Nacional de Educación Superior Universitaria | Dirección de Documentación e Información Universitaria y Registro de Grados y Títulos

REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Graduado	Grado o Título	Institución
ARAOZ SOTO, JERSY HUBERT **DNI 44341144**	ABOGADO **Fecha de diploma: 10/07/2012** Modalidad de estudios: -	UNIVERSIDAD NACIONAL SAN LUIS GONZAGA DE ICA ***PERU***
ARAOZ SOTO, JERSY HUBERT **DNI 44341144**	BACHILLER EN DERECHO **Fecha de diploma: 09/09/2011** Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD NACIONAL SAN LUIS GONZAGA DE ICA ***PERU***
ARAOZ SOTO, JERSY HUBERT **DNI 44341144**	MAESTRO EN DERECHO MENCIÓN: CIENCIAS PENALES **Fecha de diploma: 16/07/17** Modalidad de estudios: PRESENCIAL Fecha matrícula: 01/12/2011 Fecha egreso: 13/08/2014	UNIVERSIDAD NACIONAL SAN LUIS GONZAGA DE ICA ***PERU***
ARAOZ SOTO, JERSY HUBERT **DNI 44341144**	MAESTRO EN CIENCIAS DE LA EDUCACIÓN; MENCIÓN EN ADMINISTRACIÓN Y PLANIFICACIÓN DE LA EDUCACIÓN **Fecha de diploma: 30/09/21** Modalidad de estudios: PRESENCIAL Fecha matrícula: 03/05/2016 Fecha egreso: 21/10/2017	UNIVERSIDAD NACIONAL DE HUANCAVELICA ***PERU***
ARAOZ SOTO, JERSY HUBERT **DNI 44341144**	BACHILLER EN CIENCIAS DE LA EDUCACIÓN **Fecha de diploma: 27/08/16** Modalidad de estudios: PRESENCIAL Fecha matrícula: 09/05/2014 Fecha egreso: 13/01/2015	UNIVERSIDAD NACIONAL SAN LUIS GONZAGA DE ICA ***PERU***
ARAOZ SOTO, JERSY HUBERT **DNI 44341144**	LICENCIADO EN CIENCIAS DE LA EDUCACION CON MENCION EN INGLES **Fecha de diploma: 21/04/21** Modalidad de estudios: PRESENCIAL	UNIVERSIDAD NACIONAL SAN LUIS GONZAGA DE ICA ***PERU***

VALIDEZ POR JUICIO DE EXPERTOS

Señor(a)(ita): HUAMANI RUBY FIORELA

Presente

Asunto: Validación de instrumentos a través de juicio de experto

Nos es muy grato comunicarme con usted para expresarle mi saludo y así mismo, hacer de su conocimiento que siendo estudiante del programa de Maestría de derecho penal y Procesal penal de la Universidad César Vallejo, en la sede Lima Norte, promoción 2024-I, requiero validar el instrumento con el cual recogeré la información necesaria para poder desarrollar mi trabajo de investigación.

El título nombre del proyecto de investigación es: La regulación de los delitos informáticos en el derecho penal: desafíos y perspectivas futuras, 2023. y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación, que le hago llegar contiene:

- Carta de presentación.
- Definiciones conceptuales de las variables y dimensiones.

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente,

EDITH GIULIANA HUAMANI ESPINO
DNI N° 75702477

FICHA DE VALIDEZ DE EXPERTO

I. DATOS GENERALES:

Apellidos y nombres del experto : HUAMANI RUBAY FLORIA
Grado Académico : Maestro
Institución donde labora : MINISTERIO PUBLICO
Instrumento a evaluar : Guía de entrevista.
Autor del Instrumento : HUAMANI ESPINO EDITH GIULIANA

II. ASPECTOS DE VALIDACIÓN:

DEFICIENTE (1) **ACEPTABLE (2)** **BUENA (3)** **EXCELENTE (4)**

CRITERIOS	INDICADORES	1	2	3	4
CLARIDAD	Las preguntas están formuladas con lenguaje apropiado, es decir libre de ambigüedades.				X
OBJETIVIDAD	Las preguntas permitirán mensurar las categorías en todos sus aspectos conceptuales y operacionales.				X
ACTUALIDAD	El instrumento evidencia vigencia y es pertinente al contexto cultural, científico, tecnológico y legal inherente a las categorías.				X
ORGANIZACIÓN	Las preguntas del instrumento traducen organicidad lógica en concordancia con la definición operacional y conceptual de las categorías, sub categorías e indicadores.				X
SUFICIENCIA	Las preguntas del instrumento expresan suficiencia en cantidad y calidad.				X
INTENCIONALIDAD	Las preguntas del instrumento evidencian ser adecuadas para valorar el objeto de estudio en relación con la calidad académica.				X
CONSISTENCIA	La información que se obtendrá, mediante las preguntas, permitirá evaluar, describir y explicar la realidad motivo de la investigación				X
COHERENCIA	Las preguntas del instrumento expresan coherencia entre las categorías, sub categorías e indicadores.				X
METODOLOGÍA	El procedimiento insertado en el instrumento responde al propósito de la investigación.				X
PERTINENCIA	Las preguntas son aplicables al objetivo de la investigación				X
	Sub total				40
	TOTAL			40	

III. OPINIÓN DE APLICABILIDAD: El instrumento si es aplicable

IV. PROMEDIO DE VALORACIÓN: 40

Ica, 15 de mayo del 2024

Firma del Experto Informante

PERÚ | Ministerio de Educación | Superintendencia Nacional de Educación Superior Universitaria | Dirección de Documentación e Información Universitaria y Registro de Grados y Títulos

REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Graduado	Grado o Título	Institución
HUAMANI RUPAY, FIORELA INES **DNI 43161925**	**ABOGADO** **Fecha de diploma: 24/02/2010** Modalidad de estudios: -	UNIVERSIDAD NACIONAL SAN LUIS GONZAGA DE ICA ***PERU***
HUAMANI RUPAY, FIORELA INES **DNI 43161925**	**BACHILLER EN DERECHO** **Fecha de diploma: 21/07/2009** Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD NACIONAL SAN LUIS GONZAGA DE ICA ***PERU***
HUAMANI RUPAY, FIORELA INES **DNI 43161925**	**MAGISTER/MAESTRO EN DERECHO CON MENCION EN CIENCIAS PENALES** **Fecha de diploma: 12/12/14** Modalidad de estudios: PRESENCIAL Fecha matrícula: 12/07/2010 Fecha egreso: 18/04/2013	UNIVERSIDAD NACIONAL SAN LUIS GONZAGA DE ICA ***PERU***

VALIDEZ POR JUICIO DE EXPERTOS

Señor : GARCIA ANGULO CHRISTIAN SALOMON

Presente

Asunto: Validación de instrumentos a través de juicio de experto

Nos es muy grato comunicarme con usted para expresarle mi saludo y así mismo, hacer de su conocimiento que siendo estudiante del programa de Maestría de derecho penal y Procesal penal de la Universidad César Vallejo, en la sede Lima Norte, promoción 2024-I, requiero validar el instrumento con el cual recogeré la información necesaria para poder desarrollar mi trabajo de investigación.

El título nombre del proyecto de investigación es: La regulación de los delitos informáticos en el derecho penal: desafíos y perspectivas futuras, 2023. y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación, que le hago llegar contiene:

- Carta de presentación.
- Definiciones conceptuales de las variables y dimensiones.

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente,

EDITH GIULIANA HUAMANI ESPINO
DNI N° 75702477

FICHA DE VALIDEZ DE EXPERTO

I. DATOS GENERALES:

Apellidos y nombres del experto	:	GARCIA ANGULO CHRISTIAN SALOMON
Grado Académico	:	Maestro
Institución donde labora	:	MINISTERIO PUBLICO
Instrumento a evaluar	:	Guía de entrevista.
Autor del Instrumento	:	HUAMAN ESPINO EDITH GIULIANA

II. ASPECTOS DE VALIDACIÓN:

DEFICIENTE (1) **ACEPTABLE (2)** **BUENA (3)** **EXCELENTE (4)**

CRITERIOS	INDICADORES	1	2	3	4
CLARIDAD	Las preguntas están formuladas con lenguaje apropiado, es decir libre de ambigüedades.				X
OBJETIVIDAD	Las preguntas permitirán mensurar las categorías en todos sus aspectos conceptuales y operacionales.				X
ACTUALIDAD	El instrumento evidencia vigencia y es pertinente al contexto cultural, científico, tecnológico y legal inherente a las categorías.				X
ORGANIZACIÓN	Las preguntas del instrumento traducen organicidad lógica en concordancia con la definición operacional y conceptual de las categorías, sub categorías e indicadores.				X
SUFICIENCIA	Las preguntas del instrumento expresan suficiencia en cantidad y calidad.				X
INTENCIONALIDAD	Las preguntas del instrumento evidencian ser adecuadas para valorar el objeto de estudio en relación con la calidad académica.				X
CONSISTENCIA	La información que se obtendrá, mediante las preguntas, permitirá evaluar, describir y explicar la realidad motivo de la investigación				X
COHERENCIA	Las preguntas del instrumento expresan coherencia entre las categorías, sub categorías e indicadores.				X
METODOLOGÍA	El procedimiento insertado en el instrumento responde al propósito de la investigación.				X
PERTINENCIA	Las preguntas son aplicables al objetivo de la investigación				X
	Sub total				40
	TOTAL		40		

III. OPINIÓN DE APLICABILIDAD: El instrumento si es aplicable

IV. PROMEDIO DE VALORACIÓN: 40

Ica, 15 de mayo del 2024

Salomón Garcia

Firma del Experto Informante

PERÚ | Ministerio de Educación | Superintendencia Nacional de Educación Superior Universitaria | Dirección de Documentación e Información Universitaria y Registro de Grados y Títulos

REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Graduado	Grado o Título	Institución
GARCIA ANGULO, CHRISTIAN SALOMON **DNI 46464993**	**ABOGADO** **Fecha de diploma: 03/04/2014** Modalidad de estudios: -	UNIVERSIDAD NACIONAL SAN LUIS GONZAGA DE ICA ***PERU***
GARCIA ANGULO, CHRISTIAN SALOMON **DNI 46464993**	**BACHILLER EN DERECHO** **Fecha de diploma: 22/07/13** Modalidad de estudios: PRESENCIAL Fecha matrícula: 05/03/2007 Fecha egreso: 18/01/2013	UNIVERSIDAD NACIONAL SAN LUIS GONZAGA DE ICA ***PERU***
GARCIA ANGULO, CHRISTIAN SALOMON DNI 46464993	TÍTULO DE MÁSTER PROPIO EN DERECHO PENAL Y GARANTÍAS CONSTITUCIONALES (GRADO DE MAESTRO) **Fecha de Diploma: 17/09/2021** *TIPO:* • ***RECONOCIMIENTO*** Fecha de Resolución de Reconocimiento: 10/01/2022 **Modalidad de estudios: A Distancia** **Duración de estudios: 1 Año**	UNIVERSIDAD DE JAÉN ***ESPAÑA***

Consentimiento Informado

Yo, Edith Giuliana Huamani Espino, estudiante de la Escuela de Posgrado de la Universidad Cesar Vallejo, estoy realizando la investigación de titulada La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023. Por consiguiente, se le invita a participar voluntariamente en dicho estudio. Su participación será de invalorable ayuda para lograr el objetivo de la investigación.

Propósito del estudio
El objetivo del presente estudio es analizar los enfoques actuales de regulación de los delitos informáticos dentro del derecho penal, identificar los desafíos enfrentados en este campo emergente y explorar las perspectivas futuras para mejorar la eficacia legal en la era digital. Esta investigación es desarrollada en la escuela de Posgrado de la Universidad Cesar Vallejo del Campus cono Norte Lima aprobado por la autoridad correspondiente de la Universidad.

Procedimiento
Si usted decide participar en la investigación se realizará lo siguiente:

1. Esta entrevista tendrá un tiempo aproximado de 15 minutos.

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir, si desea participar o no, y su decisión será respetada. Posterior a la aceptación, si no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de no maleficencia)
Indicar al participante, la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia)
Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico, ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona; sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia)
Garantizamos que la información que usted nos brinde es totalmente confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:
Si tiene preguntas sobre la investigación puede contactar con el Investigador Edith Giuliana Huamani Espino email: ehuamanie@pj.gob.pe

Consentimiento
Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombre y apellidos: JUAN CARLOS MARTIN HERRERA CESTI

Nro. DNI: 21827699

Lugar, 04 Junio del 2024

Nota: Obligatorio a partir de los 18 años

Para garantizar la veracidad del origen de la información: en el caso que el consentimiento sea presencial, el encuestado y el investigador debe proporcionar: Nombre y firma. En el caso que sea cuestionario virtual, se debe solicitar el correo desde el cual se envía las respuestas a través de un formulario Google.

Consentimiento Informado

Yo, Edith Giuliana Huamani Espino, estudiante de la Escuela de Posgrado de la Universidad Cesar Vallejo, estoy realizando la investigación de titulada La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023. Por consiguiente, se le invita a participar voluntariamente en dicho estudio. Su participación será de invalorable ayuda para lograr el objetivo de la investigación.

Propósito del estudio
El objetivo del presente estudio es analizar los enfoques actuales de regulación de los delitos informáticos dentro del derecho penal, identificar los desafíos enfrentados en este campo emergente y explorar las perspectivas futuras para mejorar la eficacia legal en la era digital. Esta investigación es desarrollada en la escuela de Posgrado de la Universidad Cesar Vallejo del Campus cono Norte Lima aprobado por la autoridad correspondiente de la Universidad.

Procedimiento
Si usted decide participar en la investigación se realizará lo siguiente:

1. Esta entrevista tendrá un tiempo aproximado de 15 minutos.

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir, si desea participar o no, y su decisión será respetada. Posterior a la aceptación, si no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de no maleficencia)
Indicar al participante, la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia)
Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico, ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona; sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia)
Garantizamos que la información que usted nos brinde es totalmente confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:
Si tiene preguntas sobre la investigación puede contactar con el Investigador Edith Giuliana Huamani Espino email: ehuamanie@pj.gob.pe

Consentimiento
Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombre y apellidos: JUAN MANUEL ARQUIÑEGO PAZ

Nro. DNI: 40395719

Lugar, 04 Junio del 2024

Nota: Obligatorio a partir de los 18 años

Para garantizar la veracidad del origen de la información: en el caso que el consentimiento sea presencial, el encuestado y el investigador debe proporcionar: Nombre y firma. En el caso que sea cuestionario virtual, se debe solicitar el correo desde el cual se envía las respuestas a través de un formulario Google.

Consentimiento Informado

Yo, Edith Giuliana Huamani Espino, estudiante de la Escuela de Posgrado de la Universidad Cesar Vallejo, estoy realizando la investigación de titulada La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023. Por consiguiente, se le invita a participar voluntariamente en dicho estudio. Su participación será de invalorable ayuda para lograr el objetivo de la investigación.

Propósito del estudio
El objetivo del presente estudio es analizar los enfoques actuales de regulación de los delitos informáticos dentro del derecho penal, identificar los desafíos enfrentados en este campo emergente y explorar las perspectivas futuras para mejorar la eficacia legal en la era digital. Esta investigación es desarrollada en la escuela de Posgrado de la Universidad Cesar Vallejo del Campus cono Norte Lima aprobado por la autoridad correspondiente de la Universidad.

Procedimiento
Si usted decide participar en la investigación se realizará lo siguiente:

1. Esta entrevista tendrá un tiempo aproximado de 15 minutos.

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir, si desea participar o no, y su decisión será respetada. Posterior a la aceptación, si no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de no maleficencia)
Indicar al participante, la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia)
Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico, ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona; sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia)
Garantizamos que la información que usted nos brinde es totalmente confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:
Si tiene preguntas sobre la investigación puede contactar con el Investigador Edith Giuliana Huamani Espino email: ehuamanic@pj.gob.pe

Consentimiento
Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombre y apellidos: SORINA SOTO BERRIÑANO

Nro. DNI: 40810010

Lugar, 25 mayo del 2024

Nota: Obligatorio a partir de los 18 años

Para garantizar la veracidad del origen de la información: en el caso que el consentimiento sea presencial, el encuestado y el investigador debe proporcionar: Nombre y firma. En el caso que sea cuestionario virtual, se debe solicitar el correo desde el cual se envía las respuestas a través de un formulario Google.

Consentimiento Informado

Yo, Edith Giuliana Huamani Espino, estudiante de la Escuela de Posgrado de la Universidad Cesar Vallejo, estoy realizando la investigación de titulada La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023. Por consiguiente, se le invita a participar voluntariamente en dicho estudio. Su participación será de invalorable ayuda para lograr el objetivo de la investigación.

Propósito del estudio
El objetivo del presente estudio es analizar los enfoques actuales de regulación de los delitos informáticos dentro del derecho penal, identificar los desafíos enfrentados en este campo emergente y explorar las perspectivas futuras para mejorar la eficacia legal en la era digital. Esta investigación es desarrollada en la escuela de Posgrado de la Universidad Cesar Vallejo del Campus cono Norte Lima aprobado por la autoridad correspondiente de la Universidad.

Procedimiento
Si usted decide participar en la investigación se realizará lo siguiente:

1. Esta entrevista tendrá un tiempo aproximado de 15 minutos.

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir, si desea participar o no, y su decisión será respetada. Posterior a la aceptación, si no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de no maleficencia)
Indicar al participante, la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia)
Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico, ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona; sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia)
Garantizamos que la información que usted nos brinde es
totalmente confidencial y no será usada para ningún otro propósito fuera de la
investigación. Los datos permanecerán bajo custodia del investigador principal y
pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:
Si tiene preguntas sobre la investigación puede contactar con el Investigador Edith Giuliana Huamani Espino email: ehuamanie@pj.gob.pe

Consentimiento
Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombre y apellidos: Miguel Angel Morales Sandoval

Nro. DNI: 48152582

Lugar, 25 mayo del 2024

Nota: Obligatorio a partir de los 18 años

Para garantizar la veracidad del origen de la información: en el caso que el consentimiento sea presencial, el encuestado y el investigador debe proporcionar: Nombre y firma. En el caso que sea cuestionario virtual, se debe solicitar el correo desde el cual se envía las respuestas a través de un formulario Google

PODER JUDICIAL DEL PERU

Consentimiento Informado

Yo, Edith Giuliana Huamani Espino, estudiante de la Escuela de Posgrado de la Universidad Cesar Vallejo, estoy realizando la investigación de titulada La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023. Por consiguiente, se le invita a participar voluntariamente en dicho estudio. Su participación será de invalorable ayuda para lograr el objetivo de la investigación.

Propósito del estudio
El objetivo del presente estudio es analizar los enfoques actuales de regulación de los delitos informáticos dentro del derecho penal, identificar los desafíos enfrentados en este campo emergente y explorar las perspectivas futuras para mejorar la eficacia legal en la era digital. Esta investigación es desarrollada en la escuela de Posgrado de la Universidad Cesar Vallejo del Campus cono Norte Lima aprobado por la autoridad correspondiente de la Universidad.

Procedimiento
Si usted decide participar en la investigación se realizará lo siguiente:

1. Esta entrevista tendrá un tiempo aproximado de 15 minutos.

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir, si desea participar o no, y su decisión será respetada. Posterior a la aceptación, si no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de no maleficencia)
Indicar al participante, la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia)
Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico, ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona; sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia)
Garantizamos que la información que usted nos brinde es totalmente confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:
Si tiene preguntas sobre la investigación puede contactar con el Investigador Edith Giuliana Huamani Espino email: ehuamanie@pj.gob.pe

Consentimiento
Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombre y apellidos: ...Eva Gabriela De Sanchez.....

Nro. DNI: ...44496586.....

Lugar, 25 mayo del 2024

Nota: Obligatorio a partir de los 18 años

Para garantizar la veracidad del origen de la información: en el caso que el consentimiento sea presencial, el encuestado y el investigador debe proporcionar: Nombre y firma. En el caso que sea cuestionario virtual, se debe solicitar el correo desde el cual se envía las respuestas a través de un formulario Google.

Consentimiento Informado

Yo, Edith Giuliana Huamani Espino, estudiante de la Escuela de Posgrado de la Universidad Cesar Vallejo, estoy realizando la investigación de titulada La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023. Por consiguiente, se le invita a participar voluntariamente en dicho estudio. Su participación será de invalorable ayuda para lograr el objetivo de la investigación.

Propósito del estudio
El objetivo del presente estudio es analizar los enfoques actuales de regulación de los delitos informáticos dentro del derecho penal, identificar los desafíos enfrentados en este campo emergente y explorar las perspectivas futuras para mejorar la eficacia legal en la era digital. Esta investigación es desarrollada en la escuela de Posgrado de la Universidad Cesar Vallejo del Campus cono Norte Lima aprobado por la autoridad correspondiente de la Universidad.

Procedimiento
Si usted decide participar en la investigación se realizará lo siguiente:

1. Esta entrevista tendrá un tiempo aproximado de 15 minutos.

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir, si desea participar o no, y su decisión será respetada. Posterior a la aceptación, si no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de no maleficencia)
Indicar al participante, la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia)

Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico, ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona; sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia)
Garantizamos que la información que usted nos brinde es totalmente confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:
Si tiene preguntas sobre la investigación puede contactar con el Investigador Edith Giuliana Huamani Espino email: ehuamanie@pj.gob.pe

Consentimiento
Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombre y apellidos: Nicolle Carbonel Bellido

Nro. DNI: 70302606

Lugar, 25 mayo del 2024

Nota: Obligatorio a partir de los 18 años

Para garantizar la veracidad del origen de la información: en el caso que el consentimiento sea presencial, el encuestado y el investigador debe proporcionar: Nombre y firma. En el caso que sea cuestionario virtual, se debe solicitar el correo desde el cual se envía las respuestas a través de un formulario Google.

Consentimiento Informado

Yo, Edith Giuliana Huamani Espino, estudiante de la Escuela de Posgrado de la Universidad Cesar Vallejo, estoy realizando la investigación de titulada La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023. Por consiguiente, se le invita a participar voluntariamente en dicho estudio. Su participación será de invalorable ayuda para lograr el objetivo de la investigación.

Propósito del estudio
El objetivo del presente estudio es analizar los enfoques actuales de regulación de los delitos informáticos dentro del derecho penal, identificar los desafíos enfrentados en este campo emergente y explorar las perspectivas futuras para mejorar la eficacia legal en la era digital. Esta investigación es desarrollada en la escuela de Posgrado de la Universidad Cesar Vallejo del Campus cono Norte Lima aprobado por la autoridad correspondiente de la Universidad.

Procedimiento
Si usted decide participar en la investigación se realizará lo siguiente:

1. Esta entrevista tendrá un tiempo aproximado de 15 minutos.

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir, si desea participar o no, y su decisión será respetada. Posterior a la aceptación, si no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de no maleficencia)
Indicar al participante, la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia)

Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico, ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona; sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia)
Garantizamos que la información que usted nos brinde es totalmente confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:
Si tiene preguntas sobre la investigación puede contactar con el Investigador Edith Giuliana Huamani Espino email: ehuamanie@pj.gob.pe

Consentimiento
Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombre y apellidos: Bonilla Frias Jose

Nro. DNI: 28720416

Lugar, 25 mayo del 2024

Nota: Obligatorio a partir de los 18 años

Para garantizar la veracidad del origen de la información: en el caso que el consentimiento sea presencial, el encuestado y el investigador debe proporcionar: Nombre y firma. En el caso que sea cuestionario virtual, se debe solicitar el correo desde el cual se envía las respuestas a través de un formulario Google.

Consentimiento Informado

Yo, Edith Giuliana Huamani Espino, estudiante de la Escuela de Posgrado de la Universidad Cesar Vallejo, estoy realizando la investigación de titulada La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023. Por consiguiente, se le invita a participar voluntariamente en dicho estudio. Su participación será de invalorable ayuda para lograr el objetivo de la investigación.

Propósito del estudio
El objetivo del presente estudio es analizar los enfoques actuales de regulación de los delitos informáticos dentro del derecho penal, identificar los desafíos enfrentados en este campo emergente y explorar las perspectivas futuras para mejorar la eficacia legal en la era digital. Esta investigación es desarrollada en la escuela de Posgrado de la Universidad Cesar Vallejo del Campus cono Norte Lima aprobado por la autoridad correspondiente de la Universidad.

Procedimiento
Si usted decide participar en la investigación se realizará lo siguiente:

1. Esta entrevista tendrá un tiempo aproximado de 15 minutos.

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir, si desea participar o no, y su decisión será respetada. Posterior a la aceptación, si no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de no maleficencia)
Indicar al participante, la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia)

Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico, ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona; sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia)
Garantizamos que la información que usted nos brinde es totalmente confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:
Si tiene preguntas sobre la investigación puede contactar con el Investigador Edith Giuliana Huamani Espino email: ehuamanie@pj.gob.pe

Consentimiento
Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombre y apellidos: Peralta Burda Elsa Alejandra

Nro. DNI: 48429698

Lugar, 25 mayo del 2024

Nota: Obligatorio a partir de los 18 años

Para garantizar la veracidad del origen de la información: en el caso que el consentimiento sea presencial, el encuestado y el investigador debe proporcionar: Nombre y firma. En el caso que sea cuestionario virtual, se debe solicitar el correo desde el cual se envía las respuestas a través de un formulario Google.

Consentimiento Informado

Yo, Edith Giuliana Huamani Espino, estudiante de la Escuela de Posgrado de la Universidad Cesar Vallejo, estoy realizando la investigación de titulada La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023. Por consiguiente, se le invita a participar voluntariamente en dicho estudio. Su participación será de invalorable ayuda para lograr el objetivo de la investigación.

Propósito del estudio
El objetivo del presente estudio es analizar los enfoques actuales de regulación de los delitos informáticos dentro del derecho penal, identificar los desafíos enfrentados en este campo emergente y explorar las perspectivas futuras para mejorar la eficacia legal en la era digital. Esta investigación es desarrollada en la escuela de Posgrado de la Universidad Cesar Vallejo del Campus cono Norte Lima aprobado por la autoridad correspondiente de la Universidad.

Procedimiento
Si usted decide participar en la investigación se realizará lo siguiente:

1. Esta entrevista tendrá un tiempo aproximado de 15 minutos.

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir, si desea participar o no, y su decisión será respetada. Posterior a la aceptación, si no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de no maleficencia)
Indicar al participante, la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia)

Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico, ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona; sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia)
Garantizamos que la información que usted nos brinde es totalmente confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:
Si tiene preguntas sobre la investigación puede contactar con el Investigador Edith Giuliana Huamani Espino email: ehuamanie@pj.gob.pe

Consentimiento
Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombre y apellidos: Tuesta Acuache Luis Alberto

Nro. DNI: 22068573

Lugar, 25 mayo del 2024

Nota: Obligatorio a partir de los 18 años

Para garantizar la veracidad del origen de la información: en el caso que el consentimiento sea presencial, el encuestado y el investigador debe proporcionar: Nombre y firma. En el caso que sea cuestionario virtual, se debe solicitar el correo desde el cual se envía las respuestas a través de un formulario Google.

Consentimiento Informado

Yo, Edith Giuliana Huamani Espino, estudiante de la Escuela de Posgrado de la Universidad Cesar Vallejo, estoy realizando la investigación de titulada La Regulación de los Delitos Informáticos en el Derecho Penal: Desafíos y Perspectivas Futuras, 2023. Por consiguiente, se le invita a participar voluntariamente en dicho estudio. Su participación será de invalorable ayuda para lograr el objetivo de la investigación.

Propósito del estudio
El objetivo del presente estudio es analizar los enfoques actuales de regulación de los delitos informáticos dentro del derecho penal, identificar los desafíos enfrentados en este campo emergente y explorar las perspectivas futuras para mejorar la eficacia legal en la era digital. Esta investigación es desarrollada en la escuela de Posgrado de la Universidad Cesar Vallejo del Campus cono Norte Lima aprobado por la autoridad correspondiente de la Universidad.

Procedimiento
Si usted decide participar en la investigación se realizará lo siguiente:

1. Esta entrevista tendrá un tiempo aproximado de 15 minutos.

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir, si desea participar o no, y su decisión será respetada. Posterior a la aceptación, si no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de no maleficencia)
Indicar al participante, la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia)
Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico, ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona; sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia)
Garantizamos que la información que usted nos brinde es totalmente confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:
Si tiene preguntas sobre la investigación puede contactar con el Investigador Edith Giuliana Huamani Espino email: ehuamanie@pj.gob.pe

Consentimiento
Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombre y apellidos: Kelly Rosario Ylizarbe Tasayco

Nro. DNI: 72860809

Lugar, 25 mayo del 2024

Nota: Obligatorio a partir de los 18 años

Para garantizar la veracidad del origen de la información: en el caso que el consentimiento sea presencial, el encuestado y el investigador debe proporcionar: Nombre y firma. En el caso que sea cuestionario virtual, se debe solicitar el correo desde el cual se envía las respuestas a través de un formulario Google.