UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Aplicación del convenio Budapest y delitos informáticos en el Perú, 2022

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Derecho penal y Procesal penal

AUTOR:

Ocupa Sánchez, Bammy Sharum (orcid.org/0000-0002-1067-512X)

ASESOR:

Dr. Palomino Alvarado, Gabriela del Pilar (orcid.org/0000-0002-2126-2769)

CO-ASESOR:

Dr. Salas Velásquez, Napoleon Armstrong (orcid.org/0000-0002-6784-8335)

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

TARAPOTO – PERÚ

2023

DEDICATORIA

A mi pequeño Alessandro Sebastian, quien a su corta edad tuvo que entender que mamá se estaba desarrollando como profesional y tuvo que multiplicarse para poder ser, mamá, trabajadora y estudiante; su paciencia, comprensión e independencia, me dieron el soporte y fuerzas para lograr con éxito el avance de un siguiente escalón en mi proyecto de vida personal y profesional.

Sharum

AGRADECIMIENTO

Quiero agradecer infinitamente a Dios, por su sabiduría, la vida y salud, a mi madre por impulsar mis sueños y esperanzas, a mi padre por guiarme desde el cielo, y a mi asesora de tesis Dra. Gabriela del Pilar Palomino Alvarado, gracias a su paciencia, por compartir su conocimiento de manera profesional, por su dedicación perseverancia y tolerancia por su apoyo durante la elaboración de esta tesis.

La autora

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La investigación tuvo como objetivo general en analizar de qué manera el Estado peruano aplica el convenio de Budapest para sancionar delitos informáticos en el año 2022. El Convenio de Budapest, ha traído aparentemente la solución a la problemática, debido a que resultaba atractivo una cooperación supranacional para la lucha contra este tipo de delincuencia, la legislación adecuada para prevenir y sancionar estas conductas, la mejoría en las técnicas e instrumentos investigativos que coadyuven a la prevención y sanción de las conductas típicas. La metodología fue de tipo básica con diseño en teoría fundamentada, el enfoque aplicado en la investigación fue cualitativa, los instrumentos de recolección de datos fueron la guía de análisis documental y entrevista a expertos. El resultado indicó la adhesión del convenio ha generado que exista una red de cooperación internacional entre los países suscritos para que se defina y penalice varias conductas delictivas relacionadas con el uso indebido de tecnologías de la información y la comunicación. Llegando a concluir que, a través de la adopción de leyes y regulaciones específicas, se ha logrado tipificar y sancionar los delitos cibernéticos, protegiendo así la privacidad y la seguridad de la información.

Palabras clave: Convenio de Budapest, delitos informáticos, delincuencia ciber informático, tecnologías.

ABSTRACT

The general objective of the investigation was to analyze how the Peruvian State applies the Budapest Convention to punish computer crimes in the year 2022. The Budapest Convention has apparently brought the solution to the problem, because supranational cooperation was attractive. for the fight against this type of crime, the appropriate legislation to prevent and punish these behaviors, the improvement in investigative techniques and instruments that contribute to the prevention and punishment of typical behaviors. The methodology was of a basic type with a grounded theory design, the approach applied in the research was qualitative, the data collection instruments were the documentary analysis guide and interview with experts. The result indicated that the adherence to the agreement has generated the existence of an international cooperation network between the subscribed countries to define and penalize various criminal behaviors related to the improper use of information and communication technologies. Coming to the conclusion that, through the adoption of specific laws and regulations, it has been possible to classify and punish cybercrimes, thus protecting privacy and information security.

Keywords: Budapest Convention, computer crime, cybercrime, technologies

I. INTRODUCCIÓN

En España, ante el incremento de la tecnologización de los artefactos y aparatos electrónicos, la justicia del país ha quedado relegada, hasta quedar obsoleta ante ciertas conductas que generaban perjuicio patrimonial a los sujetos pasibles de aquella acción. El robo y el hurto había llegado a los espacios cibernéticos, donde, a través de publicidad engañosa, fraude informático, virus potencialmente peligrosos, roban la identidad de personas y saquean sus cuentas bancarias, con la finalidad de apropiarse de aquel dinero y, coadyuvados por el anonimato que brinda estar detrás de una pantalla, no poder ser juzgados penalmente por su accionar. Asimismo, la falta de tipificación de estos delitos conllevó a un gran problema que debía contener una respuesta legislativa. Los dispositivos normativos tenían como arquetipo esquelético, la concepción de los robos y hurtos físicos, es decir, el que sustrae a otro mediante la violencia, el que trepa una pared, el que, coadyuvado por la noche, y que esta condición lo ayude a realizar el ilícito, son condiciones de la acción que se adhieren al plano físico, al plano de los sentidos, de sufrir violencia (Dos Santos, 2022).

Argentina, ante el incremento de esta modalidad delictiva, se adhirió a la Convención, ya que el problema no radicaba precisamente en la teoría del delito y la falta de tipificación debido a que existen tipos penales generales, que podían derivar a una sanción penal a pesar de que se haya cometido por una vía diferente a la común, es decir, a través de un aparato tecnológico, en vez de la violencia física o psicológica directa que es como se concebía el delito. El verdadero problema radica que, muchas veces, los perpetradores de estos ilícitos penales, son hackers internacionales, que no se encuentran en el mismo país de donde realizan el robo, hurto, estafa, ayudados por los diversos medios electrónicos y tecnológicos, así como el anonimato que brinda encontrarse detrás de pantallas, direcciones electrónicas, y diversas formas de defraudar al internet en sí, ya que, ésta a pesar de contar con filtros de seguridad para lograr identificar a las personas que se registran en su medio, esta suele ser insuficiente, pues la innovación avanza tan desenfrenadamente que, estos

delincuentes cibernéticos suelen rehusar estos filtros que proporcionan seguridad a los usuarios.

En el Perú, también es pasible de los problemas descritos con anterioridad; la vorágine salvaje del ingente crecimiento de la tecnología, la falta de legislación necesaria para afrontar la ciberdelincuencia. Es por ello que, se necesita soluciones a esta grave problemática que nos acecha a diario, excluyéndonos del buen recaudo inclusive en el seno de nuestros hogares. El Convenio de Budapest ha traído aparentemente la solución a la problemática, debido a que resultaba atractivo una cooperación supranacional para la lucha contra este tipo de delincuencia, la legislación adecuada para prevenir y sancionar estas conductas, la mejoría en las técnicas e instrumentos investigativos que coadyuven a la prevención y sanción de las conductas típicas, y en cierta parte, como punto de partida, lo es. No obstante, la positivización no suele ser el punto final de los problemas que aquejan a una población, debido a que, no basta con reconocer el problema y darles tratativas teóricas.

Considerando el entorno social actual y la evolución de internet en el país, es necesario tener una visión más realista acerca del progreso alcanzado en este ámbito. A pesar de haber superado la idea equivocada de que la tecnología puede resolver todos los problemas, las Tecnologías de la Información y la Comunicación (TIC) son en realidad una base fundamental para el desarrollo. Sin embargo, también han dado lugar a la reproducción de viejos problemas y la aparición de otros nuevos. Entre estos problemas destaca la creciente criminalidad en el ciberespacio, que representa uno de los mayores desafíos del siglo actual, y que se en riesgo la seguridad de los usuarios y entidades de todo el mundo, y desafía el poder de los sistemas de justicia nacionales (Guerrero, 2020).

La presente investigación comienza a partir de la situación previamente descrita y utiliza este contexto como punto de partida para un análisis crítico de la próxima adhesión del Perú al Convenio de Budapest. Este convenio es el más reciente esfuerzo para abordar el problema de la delincuencia informática. El análisis está dentro de un contexto histórico en el cual el país ha establecido su entorno digital, incorporando tecnología, regulaciones y gobernanza,

basándose en enfoques y conceptos predominantes en las naciones desarrolladas. A pesar de esto, ha incorporado elementos adaptativos que han permitido su adopción a corto, medio y largo plazo. El análisis se divide en dos aspectos fundamentales: en primer lugar, se enfoca en el proceso de aplicación del Convenio, mientras que, en segundo lugar, evalúa el impacto que esta implementación tendrá en el país.

Por lo acotado, la investigación contiene el problema general ¿De qué manera el Estado peruano aplica el Convenio Budapest para sancionar los delitos informáticos en el año 2022? Asimismo, se contó con los problemas específicos ¿De qué manera se estudia la aplicación del convenio de Budapest en la legislación peruana? ¿Cuáles son los casos de ciberdelincuencia más comunes en el Perú? ¿Cuáles son los efectos jurídicos – sociales del Convenio Budapest en aplicación a los delitos informáticos en el Perú?

En la justificación por conveniencia se requirió una investigación detallada sobre la aplicación del Convenio de Budapest y la legislación vigente en materia de delitos informáticos para poder determinar su eficacia y las posibles lagunas o vacíos legales que existan. Además, la importancia de este tema radicó en la necesidad de proteger a los ciudadanos de los delitos informáticos que puedan afectar su privacidad, seguridad y patrimonio, así como garantizar el adecuado funcionamiento de las instituciones y empresas.

Asimismo, posee una gran relevancia social debido al creciente uso de la tecnología en la sociedad moderna y el aumento de los delitos informáticos en todo el mundo. En el Perú, los delitos informáticos han ido en aumento en los últimos años, lo que ha generado preocupación en la sociedad y en las autoridades encargadas de mantener el orden y la seguridad en el país.

La fundamentación teórica de la investigación se basó en el análisis detallado de las teorías relevantes al tema en cuestión, así como en la revisión de la jurisprudencia nacional e internacional relacionada con el mismo. Además, se consideró toda la bibliografía pertinente con el objetivo de proporcionar resultados científicos y metodológicos precisos.

La implicancia práctica se diversifica en la contribución a una mejor comprensión de los desafíos y oportunidades que brinda el Convenio de Budapest, y puedan ser utilizados para informar políticas y prácticas que mejoren la eficacia del Convenio con respecto a la ciberdelincuencia; asimismo, en generar literatura pertinente, donde se buscó analizar de qué manera el Estado peruano aplica el convenio de Budapest para sancionar delitos informáticos a través de los enfoques doctrinarios – jurisprudenciales.

La utilidad metodológica se esgrimió en el uso de una investigación cualitativa que permitió recopilar y analizar datos a través de diferentes métodos, como la observación, la guía de análisis documental y entrevistas en profundidad con expertos. Se aplicaron los dispositivos científicos pertinentes para asegurar la validez y la confiabilidad de los resultados obtenidos.

Asimismo, la investigación desarrollo el objetivo general: Analizar de qué manera el Estado peruano aplica el Convenio Budapest para sancionar los delitos informáticos en el año 2022. Mientras que los objetivos específicos fueron: OE1: Estudiar la aplicación del convenio de Budapest en la legislación peruana. OE2: Investigar los casos de ciberdelincuencia más comunes en el Perú. OE3: Identificar los efectos jurídicos – sociales del Convenio Budapest en aplicación a los delitos informáticos en el Perú.

II. MARCO TEÓRICO

En España, Díaz (2020) ha concluido que se ha fortalecido la cooperación internacional; la ciberdelincuencia es un problema global que requiere de la cooperación internacional para combatirla de manera efectiva. Al adherirse al Convenio de Budapest, España se une a otros países que comparten el mismo objetivo de combatir la ciberdelincuencia y se compromete a colaborar con ellos para prevenir y perseguir los delitos informáticos, implicando la adopción de medidas de seguridad que permiten a los ciudadanos españoles navegar por la red de forma más segura. El convenio establece medidas para proteger la privacidad de los usuarios y prevenir el acceso no autorizado a sistemas informáticos.

En México, Almazán (2020) concluyó que, hasta el momento, el convenio de Budapest es el único acuerdo internacional que aborda específicamente la cuestión de los delitos informáticos, incluyendo aquellos que involucran la violación de derechos de propiedad intelectual y afines. La adhesión al convenio promueve una mayor cooperación entre los países miembros, al establecer definiciones comunes de actividades delictivas que involucran el uso de medios electrónicos, permitir el intercambio de información entre las jurisdicciones para identificar a los delincuentes informáticos y establecer procedimientos para sancionar estos delitos.

En Chile, Becker (2020) concluyó que, al analizar el proyecto de ley que pretende reformar la Ley 19.223 y adoptar el Convenio, es posible identificar las alteraciones que se han incorporado al proyecto de ley, junto con algunas sugerencias que pueden ayudar a mejorar la legislación propuesta en la segunda etapa del proceso constitucional, ya que, mediante la evaluación del convenio de Budapest, se puede observar que los países tienen suficiente margen y flexibilidad para aplicar sus disposiciones de acuerdo con las características de su sistema legal.

Asimismo, en el mismo país, Álvarez y Hevia (2020) concluyen que, en términos económicos, la ausencia de excepciones para la investigación en la legislación podría amenazar con asfixiar el incipiente mercado de los servicios y

profesionales en ciberseguridad, al excesivamente regular el mercado, las leyes que permiten el acceso no autorizado sin protecciones legales para la investigación y detección de vulnerabilidades, han sido utilizadas para intentar callar la investigación en el campo de la seguridad digital. En muchas ocasiones, los fabricantes de sistemas con debilidades, al recibir notificaciones, han optado por amenazar con emprender acciones legales para silenciar a los investigadores, a menudo para salvaguardar la reputación de la compañía o para mantener su posición dominante en el mercado.

En Colombia, Ojeda et al. (2019) concluye que, los procesos de globalización, que se han desarrollado a gran velocidad, ofrecen un sinfín de oportunidades y atracciones cada vez más asombrosas para toda la humanidad. Este fenómeno ha sido impulsado por el avance tecnológico de la informática y las comunicaciones, y se ha convertido en el nuevo modelo para las relaciones personales, organizacionales, locales e internacionales, así como para el conocimiento y el progreso. En Colombia, gracias a algunos antecedentes legales relacionados con los derechos de autor, así como algunas normativas adicionales (como el Código Penal y las circulares emitidas por la Superintendencia Financiera), se logró aprobar en 2009 la Ley 1273. Esta ley permitió que Colombia se uniera al grupo de países que cuentan con herramientas más eficaces para combatir las actividades delictivas del cibercrimen, especialmente en sectores clave de la sociedad como el financiero, que son objeto de investigación y estudio por parte de los delincuentes informáticos debido a su vulnerabilidad.

A nivel nacional, Morales (2020) concluye que, en un mundo globalizado, el avance de las tecnologías siempre traerá consigo nuevos y constantes beneficios en diferentes ámbitos de la vida humana. Sin embargo, también conlleva el riesgo de la aparición de nuevas formas de delitos que pueden ser más difíciles de combatir si no existe una legislación que aborde estos aspectos, siendo que Internet ha transformado la historia de la humanidad de la misma manera que otros inventos lo han hecho en el pasado. Su aplicación no solo se limita a actividades laborales, sino también en la comunicación, información y otras áreas, convirtiéndose en una herramienta beneficiosa para

el hombre y todo lo que lo rodea. Sin embargo, a pesar de sus numerosos beneficios, su uso fácil y el crecimiento global también han dado lugar a un lado negativo, como las malas intenciones de algunas personas.

Al respecto, Huamán (2020) concluyó que, el aumento preocupante de los delitos informáticos en Perú se debe a la utilización de diversos y nuevos medios tecnológicos por parte de los ciberdelincuentes, lo que dificulta su identificación y ubicación. Por lo tanto, la adhesión al Convenio de Budapest tiene un impacto relativo en el enfoque hacia los delitos informáticos. El enfoque se centra en la adaptación de nuestra legislación a lo estipulado en dicho Convenio, lo cual implica establecer una lista de delitos, implementar normas procesales que salvaguarden las pruebas digitales y buscar colaboración internacional para examinar la comisión de estos delitos.

Asimismo, Blossiers (2019) concluye que, según las encuestas realizadas, se ha observado que el sistema normativo actual sobre delitos informáticos no es adecuado y no es suficiente para proteger los derechos de las empresas bancarias. Sin embargo, se ha notado que no se necesita una normativa específica para abordar este problema. Por lo que, se ha logrado determinar que los delitos informáticos tienen un efecto económico y social en las entidades bancarias, además de impactar su estabilidad jurídica. En primer lugar, se produce un impacto económico debido a las pérdidas que generan tanto a la empresa como a sus clientes. Esto, a su vez, tiene un impacto social debido a que los clientes experimentan una disminución de la confianza en las instituciones bancarias, lo que a largo plazo podría resultar en pérdidas para estas empresas.

De igual manera, Cubas (2023) concluye que, se colige una disminución de los costos se debe a que en lugar de depositar el microorganismo en cuestión en cada uno de los países donde se haya solicitado la patente, éste podrá ser depositado una sola vez ante una institución depositaria. Por lo tanto, el solicitante ahorrará los costos y tarifas que habría tenido que pagar para depositarlo en cada uno de los países donde se desea obtener protección. El convenio proporciona beneficios al solicitante que presenta una solicitud de patente con alcance internacional, ya que, de acuerdo a los procedimientos

contemplados en el Tratado para el depósito de microorganismos, los costos se reducirán y se aumentará la seguridad.

No se ha logrado advertir trabajos previos a nivel regional sobre el tema versado en el presente trabajo investigativo.

También la investigación cuenta con las teorías que se relaciona con cada categoría de estudio. En génesis debemos partir con la TD. La teoría general del delito se enfrenta inicialmente a la tarea de proporcionar una definición de delito que englobe todas las características esenciales que deben estar presentes en un hecho para que sea considerado como tal y sancionado con una pena. Para lograr esto, es necesario partir del derecho penal en vigencia. Cualquier intento de definir el delito fuera de la normativa penal actual es considerado fuera del ámbito jurídico y se considera como filosofía, religión o moral. La concepción de un delito como una acción sancionada por la ley con una pena se limita únicamente a un aspecto formal y no especifica los elementos necesarios para que dicha acción sea castigada.

Según el apartado 10 del Código Penal español de 1995, se consideran delitos o faltas las acciones y omisiones intencionales o negligentes que están penalizadas por la ley. Aunque esta definición no es únicamente formal, enfatiza que las acciones y omisiones que están sujetas a castigo legal deben ser "intencionales o negligentes", lo que implica una evaluación de aspectos sustantivos más allá de lo puramente formal (Muñoz y García, 2002).

La falta de claridad en las definiciones formales del delito y la insuficiencia de las teorías unitarias. Aunque se ha definido el delito como “conducta punible”, esto no es suficiente ya que se trata de una “ecuación con dos términos desconocidos”. En otras palabras, no sabemos qué es punible y qué es delito, ya que la definición no proporciona información sobre las características del delito. En lugar de utilizar el término “punible”, se deberían especificar las condiciones o características necesarias para que una conducta sea considerada delito en un orden lógico y estratificado. Esto eliminaría la redundancia tautológica de la definición (Zaffaroni, 1981).

Para examinar la teoría del delito, se empleará el enfoque dogmático, que implica la interpretación del dogma, el cual, en el ámbito del derecho penal, se refiere a la ley penal, siendo esta la única fuente legal obligatoria en el derecho penal. Dicha interpretación debe ser coherente y sistemática para lograr una comprensión adecuada. A continuación, se mencionan las características intrínsecas de esta teoría (Peña y Almanza, 2010): este conjunto de conocimientos se considera un sistema debido a su organización y ordenamiento; estas afirmaciones son consideradas hipótesis debido a que su veracidad solo puede ser comprobada de forma indirecta, a través de las implicaciones y resultados que se derivan de ellas. Debido a que forma parte de una ciencia social, existe una tendencia hacia el dogmatismo en el estudio del delito. Además, no hay consenso sobre la perspectiva desde la cual se debe abordar este fenómeno, lo que ha llevado a la existencia de varios sistemas que intentan explicarlo.

La teoría del delito se enfoca en el análisis de cualquier acción que tenga como resultado la imposición de una sanción penal o medida de seguridad, lo que se conoce como consecuencia jurídica penal, asimismo, existen diversas teorías que explican el delito y su estructura orgánica, como lo es la teoría del causalismo naturalista; dicho enfoque considera la acción desde una perspectiva física o naturalista, donde se compone de un movimiento corporal y un cambio en el mundo exterior conectados por un vínculo causal, el análisis del delito se clasifica en etapas internas y externas. Además, se distingue entre elementos objetivos (tipicidad y antijuridicidad) y subjetivos (culpabilidad) del delito. La tipificación se centra exclusivamente en factores externos, sin admitir justificaciones para ninguna acción; mientras que la antijuridicidad se evalúa desde una perspectiva objetiva. En relación a la culpabilidad, se exploran los elementos subjetivos y psicológicos del individuo, donde la imputabilidad se considera un requisito previo (Bacigalupo, 1999).

La teoría del causalismo valorativo se distingue del causalismo clásico al adoptar una perspectiva fundamentada en valores y alejarse del formalismo. En esta teoría, se reconoce la voluntad como un componente humano en la concepción naturalista de la acción. Se consideran tanto los elementos

normativos como los subjetivos del tipo, y se propone la necesidad de tener en cuenta el valor o la intencionalidad en el tipo, en contraposición a una visión puramente objetiva. Además, se redefine la antijuridicidad no solo como una mera contradicción formal con la norma, sino también en términos del daño causado a la sociedad, lo que permite graduar la injusticia y la incorporación de nuevas causas de justificación. En relación con la culpabilidad, se comprende como un juicio de reproche hacia el autor del delito, abarcando aspectos no solo psicológicos, sino también valorativos (Hurtado, 1987).

En cuanto a la teoría del finalismo inició con la definición del concepto de acción como una noción ontológica, que no está limitada al ámbito jurídico y que es finalista, es decir, se basa en la intención y no en la causa. Esta definición fue adoptada por Welzel a partir de la tradición aristotélica-tomista del acto voluntario, influenciado a su vez por las ideas de Brentano y Husserl, quienes hablaban del concepto de “intencionalidad” en todos los actos psíquicos, así como por la "psicología del pensamiento" (López, 2001).

Por lo tanto, en la teoría de la pena, el hecho de que el Estado tenga el monopolio de la acción punitiva (según lo establecido en el apartado 139.1 de la Carta Magna) implica la necesidad de establecer un discurso legitimador basado en la racionalidad de la pena. La racionalidad de la pena se relaciona con su coherencia con los elementos previos del sistema penal. En consecuencia, la función de la pena estatal debe estar en armonía con la función de la norma de conducta y, principalmente, con el propósito último del derecho penal, que es proteger la libertad de acción de las personas como condición para el desarrollo libre y equitativo de la personalidad de todos (Rodríguez, 2019).

Un discurso legitimador de la pena que adopte este enfoque debe ser capaz de enfrentarse a las consecuencias jurídicas que se derivan de la aplicación de la pena. El análisis de la legitimación de la pena no debe tener en cuenta las consecuencias naturales que pueden derivar de su aplicación, como la separación del condenado de su familia o la satisfacción de la víctima al ver que su agresor es condenado. En su lugar, se debe centrar exclusivamente en

evaluar si, cómo y hasta qué punto la pena puede contribuir a garantizar la libertad jurídica y el correcto funcionamiento del sistema jurídico (Meini, 2013).

Se hace referencia a la libertad jurídica, la cual no debe confundirse con la libertad formal que se obtiene de las leyes, ya que esto podría llevar a ignorar los problemas estructurales del sistema punitivo que lo hacen injusto y discriminatorio. En lugar de eso, la libertad que se busca con las sanciones estatales es la que se basa en los valores éticos y sociales que permiten la convivencia pacífica de las personas y les permite diseñar sus proyectos de vida y desarrollar su personalidad sin limitaciones arbitrarias.

El enfoque presentado parte de la premisa de que la legitimidad de la pena se basa en su naturaleza social, es decir, en la necesidad de la sociedad de aplicar una sanción en un caso específico, y no solo en la relación entre el infractor y el Estado. De la misma manera en que la libertad jurídica garantizada por la norma de conducta no solo vincula al destinatario y al Estado, sino a todos los ciudadanos, la aplicación de la pena requiere de una necesidad social adicional a la violación de la norma. Es por eso que, por ejemplo, la prescripción o la aplicación del principio de oportunidad pueden atenuar o eliminar la necesidad social de la pena, como en los casos de infracciones menores o cuando el infractor repara el daño causado (Van, 2018).

En consecuencia, la jurisprudencia del TC 0019-2005-PIITC, utilizan el término “teoría de la unión” para describir su comprensión de la legitimidad y el objetivo de la pena pública. Esta teoría busca combinar diferentes fundamentos y objetivos de la pena, y se considera un término intermedio entre las teorías absolutas y relativas. En una versión más actualizada de la teoría, solo se combinan los objetivos preventivos de la pena, lo que significa que la justificación se busca solo en estos fines. Sin embargo, se argumenta que la retribución de la culpabilidad todavía debe ser considerada en la justificación de la pena, aunque se espera que se limite su impacto como “medio de limitación de la intervención”.

Como resultado, desde esta perspectiva, es posible imponer una pena que sea significativamente menor que la adecuada para la culpabilidad si hay motivos

preventivos que lo justifiquen. No obstante, según esta variante, todavía se considera ilegítimo imponer una pena que exceda la medida apropiada para la culpabilidad. Algunos argumentan que el concepto de retribución de culpabilidad se ve afectado por el problema del libre albedrío, y que la noción misma de culpabilidad es el resultado de las concesiones hechas por la política criminal a ciertas necesidades, tanto reales como imaginarias. Como resultado, la palabra “retribución” es simplemente un término utilizado para el enfoque convencional en la resolución de conflictos, pero esto no implica que haya una relación intrínseca entre la culpabilidad y la retribución (Jakobs, 1998).

Así pues, las teorías absolutas o retributivas, el castigo retributivo es considerado justo para el delincuente. Esta teoría tiene sus raíces en el antiguo principio del talión, que es una forma de venganza en la que la pena es equivalente al daño causado. En la actualidad, la teoría de la retribución se aplica exigiendo una pena que sea proporcionada a la gravedad del delito y la culpabilidad del delincuente, y esto se considera justo. Sin embargo, se critica que la pena no debe ser vista como un fin en sí misma, sino que debe tener un objetivo social como proteger bienes jurídicos o mantener la norma (González, 2015).

Es en ese sentido que, las teorías relativas o preventivas, las teorías que se describen parten del reconocimiento de que la pena tiene un propósito que va más allá de la retribución. Su función es proteger a la sociedad y no se concibe como un fin en sí misma, sino como un medio para prevenir futuros delitos. La prevención busca evitar que el infractor vuelva a delinquir. Existen dos tipos de teorías de prevención: las teorías de prevención general y las teorías de prevención especial (Córdoba y Ruiz, 2009).

Las palabras “imputable”, “inimputable” y “culpable” tienen un significado diferente en la ciencia penal que el que se les da comúnmente. Esto no debería ser sorprendente, ya que en la doctrina se han propuesto varios términos para el juicio de imputación del hecho antijurídico en lugar de la "culpabilidad". Aunque la mayoría de estas propuestas se deben a las deficiencias en la fundamentación de la culpabilidad en el libre albedrío, algunos autores como Mir Puig (1996) sugieren utilizar la locución "imputación personal", Hruschka

(1978) propone el término “imputación de segundo nivel”, otros como Gimbernat (1989) rechazan completamente la culpabilidad y la sustituyen por el "juicio de necesidad de prevención", y otros autores como Maurach (1951) y Roxin (1969) complementan la culpabilidad con el concepto de responsabilidad, aunque lo definen de forma dispar (Reinhart, et al. 1995).

Respecto a la teoría procesal Gozaíni (2013) refiere que se pueden utilizar diferentes enfoques para comprender los contenidos del derecho procesal. A menudo, se enfoca en la técnica y se lo considera como una herramienta instrumental, lo que significa que es un sistema para implementar los derechos subjetivos. En este sentido, se comprende el propósito y los métodos para alcanzarlo. Algunos enfoques de enseñanza del derecho procesal se centran en el papel de los jueces y las partes en el proceso judicial, enfocándose exclusivamente en la ciencia del proceso. En este enfoque, se aprende el arte y la habilidad de litigar y juzgar en sus respectivos ámbitos. Algunos (autores)plantean diversas posturas para abordar el problema, dependiendo de si se interpreta que “lo procesal” es una parte del derecho privado en la cual las personas, al llevar sus conflictos al proceso, solicitan la aplicación del derecho objetivo(citar). Otros (autores), por otro lado, sostienen que el derecho procesal es derecho público, ya que protege los intereses de la comunidad y los bienes jurídicos individuales a través del proceso. Este ámbito se ve influenciado por la política procesal (Gozaíni, 2013).

En un principio, los pueblos se enfocan más en las normas que definen sus derechos que en aquellas que regulan la manera de hacerlos efectivos. A pesar de que el estudio de la ciencia jurídica alcanza altos niveles, todavía se presta poca atención a esta última. El objeto de la ciencia del derecho procesal se define como el estudio de las normas y funciones del poder judicial del Estado, lo que implica un enfoque constitucional. Desde los inicios teóricos de la disciplina ha habido una controversia en torno a la concepción ideológica del proceso, lo que influye en los poderes, deberes y obligaciones de las partes y el tribunal (Echandía, 2000).

Así pues, el estudio teórico de la dogmática jurídica que busca superar limitaciones y ampliar perspectivas más allá del Estado-nación, reconociendo

que todavía es necesario dar importancia al derecho de dicho Estado en el panorama político actual. Se destaca la importancia de que los juristas superen las limitaciones locales y se aventuren por los caminos del derecho de los pueblos más avanzados y sistemas más maduros, reconociendo la necesidad de desempeñarse en un ámbito trasnacional que sea coherente con los fenómenos de un universo plural y multicultural que se avecina (García 2019).

Es en ese sentido que, el derecho procesal se ocupa de procesar el derecho y su objeto de estudio es amplio y no tiene límites. Es un régimen que se encarga de crear, reformar y aplicar el derecho, y su faceta más actual es su capacidad para producir derecho sustancial. Esta faceta del derecho procesal determina la competencia, los actos procesales y la jerarquía de las fuentes, es decir, quién tiene la capacidad de producir derecho sustancial, cómo lo hacen y bajo qué jerarquía. Además, establece la manera en que se producen en el universo jurídico la norma principio constitucional, la norma regla ley, el acto administrativo y la sentencia jurisdiccional (Quintero y Prieto, 1995).

Quintero y Prieto explica cómo, en el ámbito de los estudios jurídicos, se ha acostumbrado a pensar en el derecho civil, penal, comercial, administrativo y laboral como categorías separadas y específicas. Estas categorías se definen en función del concepto más general de derecho, y cada rama del derecho toma prestadas las nociones primitivas que están implícitas en este concepto para expresar sus propias significaciones. Todo este proceso intelectual se produce después de haber determinado el concepto genérico del derecho, que es el tronco común de donde provienen todas estas ramas. White sugiere que este proceso de clasificación puede no ser lógico o sistemático en la vida real, pero es útil para entender y estudiar el derecho (White, 2008).

Para alcanzar todo el potencial de la ciencia del derecho procesal, es esencial desarrollar una sólida parte general que aborde los elementos esenciales presentes en cualquier tipo de proceso, como la acción, la jurisdicción y el procedimiento. Al explorar en mayor profundidad estos conceptos, surge de manera orgánica la idea de una teoría unificada. Sin embargo, Zolezzi destaca que, al examinar la literatura existente, se ha observado que los autores que han identificado estos elementos comunes no aportan nuevas perspectivas al

abordarlos por separado en comparación con aquellos que no se han preocupado por establecer una teoría común (Zolezzi, 1997).

El proceso civil y el proceso penal parecen ser los procesos específicos más opuestos. Algunos autores, sugieren que el único criterio que los distingue es si el tribunal tiene la intención de imponer una pena a través del proceso o no. En otras palabras, la diferencia entre un proceso penal y uno civil es si hay o no una pena involucrada (Montero, 1991).

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo

Se empleó un método de tipo básico, lo que significó que se comenzó por abordar un problema y buscar una solución basada en los enfoques planteados en el contenido de la investigación (Arias y Covinos, 2021). Por tanto, el objetivo de la tesis se basó en analizar la implementación del Convenio de Budapest y la legislación en materia de delitos informáticos en el contexto peruano.

Diseño

El diseño de la investigación se llevó a cabo utilizando las teorías fundamentadas en razón a la búsqueda de generar teorías inductivamente a partir de los datos recopilados durante el estudio; este enfoque permitió una comprensión más profunda y rica del fenómeno estudiado, ya que se centró en las experiencias y perspectivas de los participantes en el estudio (Núñez, 2008).

Se empleó un enfoque cualitativo en la investigación, debido a la orientación de la interpretación de realidades subjetivas. Aunque existen algunas diferencias, los datos obtenidos a través de métodos cualitativos tienen un valor epistemológico comparable al de los datos cuantitativos, y su extracción se lleva a cabo de manera estricta (Morlote,2004).

3.2. Categorías, Subcategorías y Matriz de Categorización

Categoría 1: Convenio Budapest
Subcategorías:

- Principio de legalidad
- Teoría de la pena
- Enfoque jurídico

Categoría 2: Delitos informáticos
Subcategorías:

- Violaciones de seguridad de red

- Aspectos criminológicos
- Fraude informático

3.3. Escenario de estudio

Este estudio consideró como marco el Perú, además, se recopiló la información científica a través del análisis de marco jurídico del Convenio de Budapest y su aplicación en los delitos informáticos, se han utilizado varias fuentes de información, tales como estudios nacionales e internacionales, jurisprudencia, libros y artículos científicos de autores de prestigio, que han servido para respaldar el trabajo investigativo.

3.4. Participantes

Los participantes de esta investigación son 03 expedientes y con cinco operadores jurídicos.

Expertos entrevistados
• Oblitas Cubas, Junior • Vela Chávez, Katty Jhuliana • Talavera Argomedo, Danny Miguel • Prado Ramos, Ronald Adolfo • Vivar Huamán, Jorge Luis

3.5. Técnicas e instrumentos de recolección de datos

Técnicas: Las técnicas de investigación son fundamentales para asegurar la secuencia correcta de los datos. De acuerdo con las ideas de Castañeda, et al (2021), estas técnicas son procedimientos sistemáticos que buscan resolver problemas prácticos. En el caso de esta investigación, se utilizó dos técnicas: el análisis de documentos y la técnica de la entrevista.

Instrumento: El instrumento que se utilizó fue la guía del análisis documental, junto con la guía de entrevista. Estas herramientas se basaron en un análisis exhaustivo de libros, artículos, informes y otros documentos que fueron de vital importancia para el desarrollo adecuado

de la investigación. Por otro lado, las entrevistas se realizaron utilizando preguntas abiertas, lo que permitió que cada entrevistado se exprese libremente y proporcione información precisa que luego se contrastó con los resultados obtenidos en el trabajo investigativo.

3.6. Procedimiento

La investigación se llevó a cabo siguiendo el procedimiento del método científico, que se aplicó con el propósito de alcanzar los objetivos establecidos. Por lo tanto, se ha considerado necesario delimitar el área de investigación para poder definir claramente el problema que se abordó, así como los objetivos y fundamentos necesarios para lograr los propósitos académicos:

Método Descriptivo - Explicativo, ya sea que se trate de debilidades o falacias. Se llevó a cabo un estudio científico para abordar este tema en particular y, dentro de este proceso, se presentaron soluciones relacionadas con la materia en cuestión (Arias, 2012).

Método Histórico. En este método se incluyen y desarrollan los trabajos previos o antecedentes relacionados con la investigación, con el objetivo de evaluar las categorías del tema investigado y de esta forma promover una mejor comprensión y aprehensión intrínseca de saberes (Calduch, 2010).

3.7. Rigor científico

Se considera: i. La sostenibilidad lógica se refiere a la coherencia entre las distintas categorías y subcategorías que se presentan en el marco teórico de la investigación (Aponte, et al. 2020). ii. La credibilidad es el grado de confianza que deben tener las diferentes fuentes de información utilizadas, las cuales serán recolectadas de artículos científicos (Baeza, et al. 2014). iii. La conformabilidad de los resultados que se obtuvo en base a los documentos y entrevistas aplicadas a los expertos (Villabella, 2000). iv. Transferibilidad se refiere a la capacidad de las conclusiones obtenidas en una investigación para ser aplicadas en otro contexto similar,

extendiendo así el alcance de las mismas a futuras investigaciones científicas. (Fernández, et al. 2004).

3.8. Método de análisis de datos

Se utilizó el método de análisis teórico para abordar a fondo el problema planteado en la investigación. El investigador empleó su experiencia y capacidad profesional para sintetizar y sistematizar los conocimientos adquiridos y establecer la estructura del marco teórico. Este método implicó el uso de procedimientos técnicos para analizar el tema en cuestión y desarrollar una síntesis clara y coherente de los conocimientos teóricos relevantes (Rodríguez et al. 2005). Para el procesamiento de la información recopilada a través de las entrevistas se aplicó el sofwareAtlas ti, para la sistematización de la información cuyos resultados se presentaron en redes de datos.

3.9. Aspectos éticos

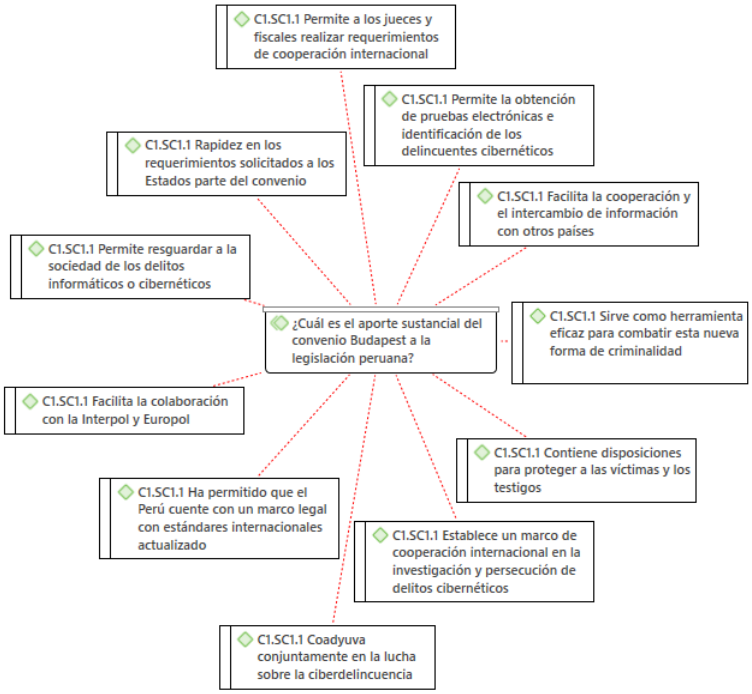
El presente estudio se adhiere a los principios éticos que rigen cualquier tipo de investigación, ya que se ha utilizado información confiable y basada en la ciencia a lo largo de todo el proceso. Para el consentimiento informado, los participantes deben ser completamente informados sobre los objetivos, procedimientos, posibles riesgos y beneficios de la investigación antes de dar su consentimiento para participar. La integridad científica, el investigador lleva a cabo su trabajo de manera honesta y precisa; evitando la manipulación o fabricación de datos, así como el plagio. Los resultados deben presentarse de manera imparcial y sin distorsiones.

IV. RESULTADOS Y DISCUSIÓN

Con respecto al objetivo específico primero que es: Estudiar la aplicación del convenio de Budapest en la legislación peruana.

Figura 1:

Aporte del convenio de Budapest a la legislación peruana



Fuente: Entrevista a operadores jurídicos – Maestros en Derecho Penal y Procesal Penal

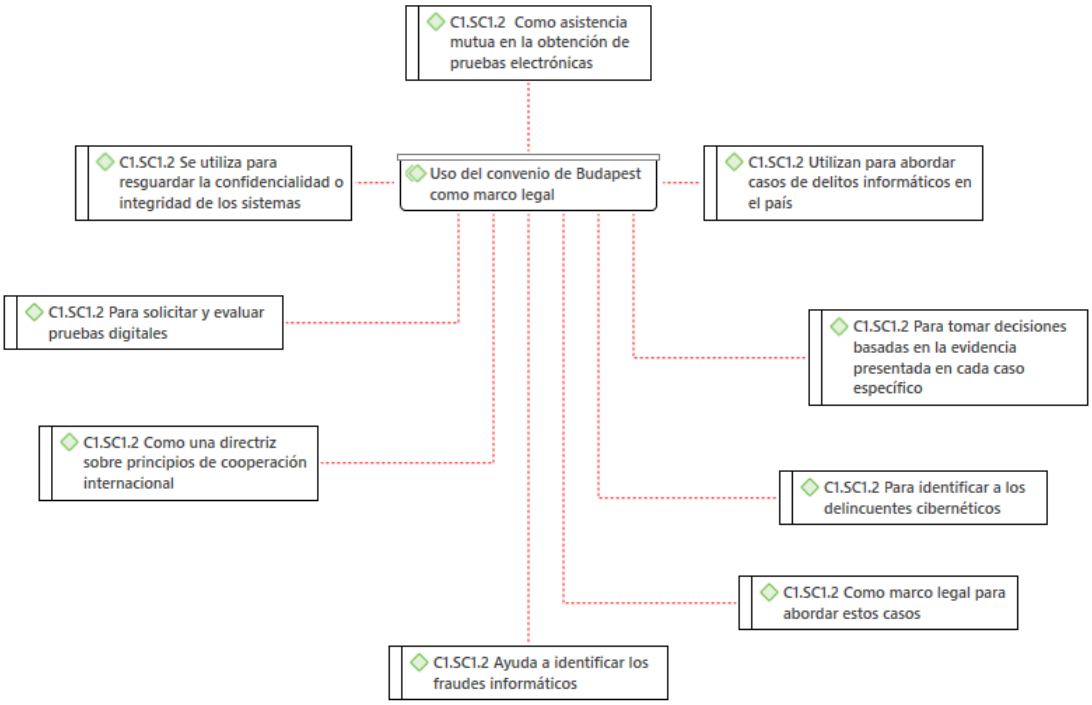
Interpretación

La figura 1 muestra la opinión de los operadores jurídicos respecto a la pregunta: ¿Considera que la aplicación del convenio de Budapest ha aportado sustancialmente a la legislación peruana? ¿Por qué?

Al respecto, mencionan que la adopción del Convenio de Budapest ha fortalecido la lucha contra el ciberdelito en Perú al proporcionar un marco legal actualizado y armonizado con estándares internacionales. Ha facilitado la cooperación y el intercambio de información con otros países, mejorando la investigación y persecución de delitos cibernéticos. Además, el convenio ha impulsado el progreso de técnicas de investigación y la colaboración internacional, protegiendo a las víctimas y testigos con medidas de confidencialidad y seguridad en los procesos judiciales. El convenio ha sido fundamental para la legislación peruana al permitir la cooperación internacional en delitos informáticos y agilizar los requerimientos entre países participantes.

Figura 2:

Utilización del convenio de Budapest como marco legal



Fuente: Entrevista a operadores jurídicos – Maestros en Derecho Penal y Procesal Penal

Interpretación

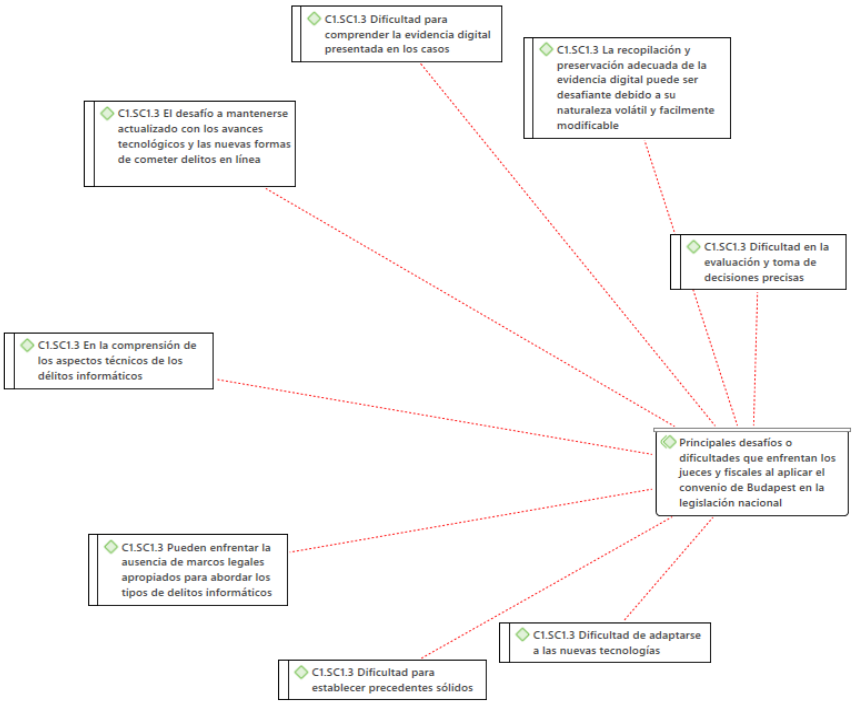
La figura 2 muestra la opinión de los operadores jurídicos respecto a la pregunta: ¿En qué medida los jueces peruanos utilizan el convenio de Budapest como marco legal para abordar casos de delitos informáticos?

Los abogados refieren que, los jueces utilizan el convenio de Budapest en casos de delitos informáticos, ya que les proporciona principios de cooperación internacional. Los jueces pueden solicitar pruebas electrónicas y la identificación de delincuentes cibernéticos con base en las disposiciones del convenio. Sin embargo, la aplicación concreta en la jurisprudencia peruana depende de la interpretación individual de los jueces y los esfuerzos del sistema judicial para adaptar su legislación a los estándares del convenio. La adhesión al convenio ayuda al país a obtener colaboración internacional y ser más efectivos en la prevención y sanción de delitos informáticos. Los jueces utilizan tanto el convenio como las leyes nacionales, como la Ley de Delitos

Informáticos, para abordar casos específicos, tomando decisiones basadas en la evidencia presentada y contribuyendo a la disminución de la impunidad.

Figura 3:

Utilización del convenio de Budapest como marco legal



Fuente: Entrevista a operadores jurídicos – Maestros en Derecho Penal y Procesal Penal

Interpretación

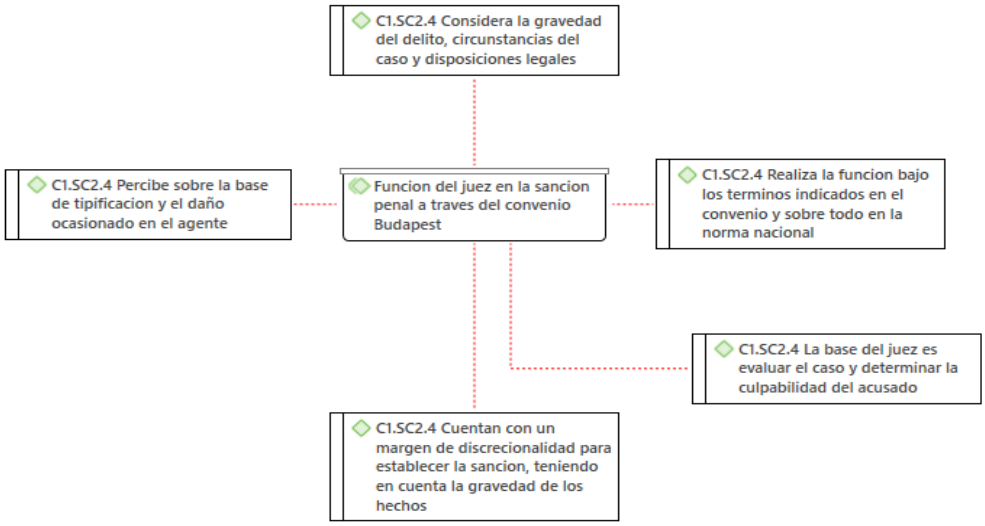
La figura 3 muestra la opinión de los operadores jurídicos teniendo en cuenta la ratificación del convenio regulado en la legislación en la Ley N.°30171 ¿Cuáles son los principales desafíos o dificultades que enfrentan los jueces y fiscales al aplicar el convenio de Budapest en la legislación nacional?

Al respecto refieren que, los delitos informáticos presentan desafíos técnicos para los jueces y fiscales, quienes pueden tener dificultades para comprender plenamente los aspectos técnicos y la evidencia digital en los casos. La recopilación y preservación adecuada de la evidencia digital también puede ser complicada debido a su naturaleza volátil. Además, la falta de marcos legales actualizados puede generar incertidumbre en la interpretación y aplicación de la ley. Los jueces deben considerar el código penal, las leyes relacionadas y los convenios internacionales al determinar la sanción para los delitos

informáticos. Mantenerse actualizados con los avances tecnológicos y recibir capacitación continua es crucial para abordar de manera efectiva los delitos informáticos en constante evolución.

Figura 4:

Sanción penal bajo la aplicación del convenio Budapest en la legislación peruana



Fuente: Entrevista a operadores jurídicos – Maestros en Derecho Penal y Procesal Penal

Interpretación

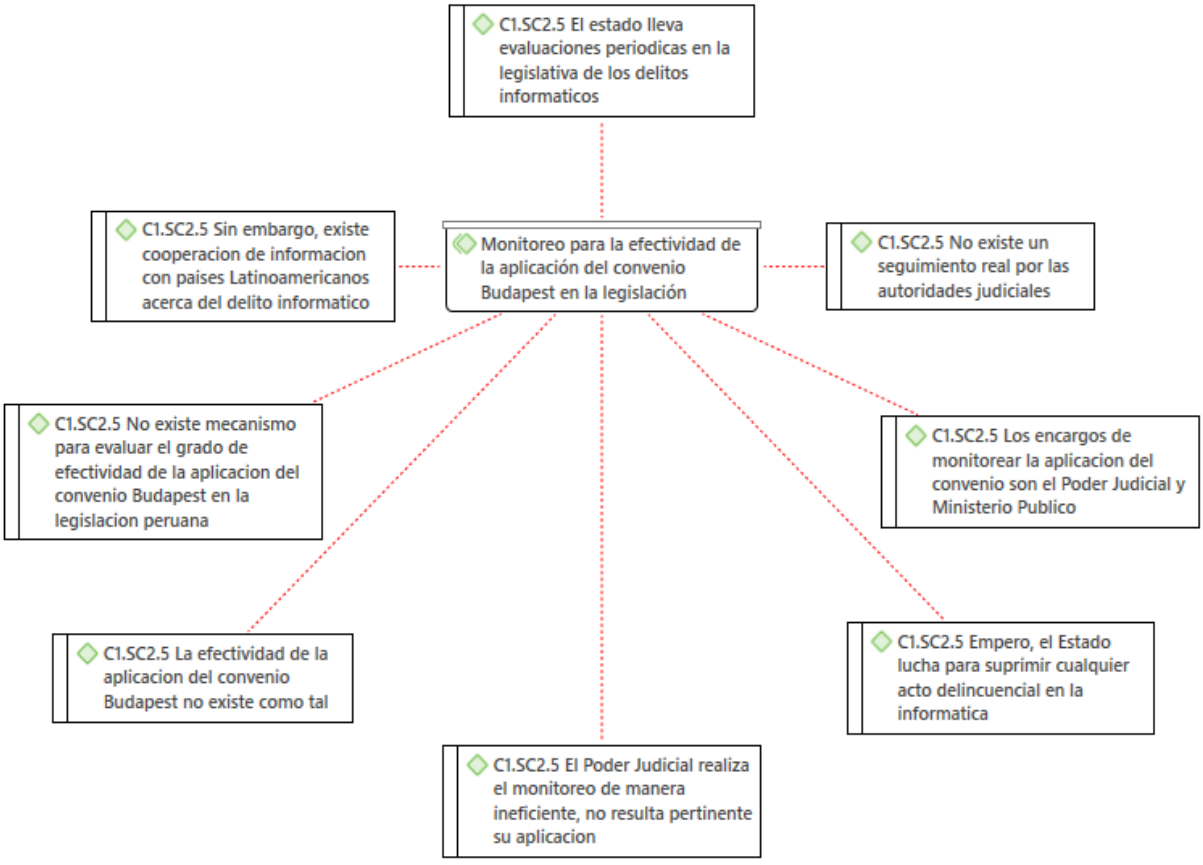
La figura 4 muestra la opinión de los operadores jurídicos teniendo en cuenta la interpretación del juez en la sanción penal ¿De qué manera el juez realiza la función de la sanción penal o pena tiene asignada sobre la base de la aplicación del convenio?

En ese sentido, el juez peruano realiza la función de la sanción penal o pena asignada sobre la base de la legislación nacional, considerando la gravedad del delito, las circunstancias del caso y las disposiciones legales vigentes. En principio, tiene la base de la normativa nacional y, en aplicación del Convenio realiza estrategias legales para contrarrestar el delito, sancionando penalmente a quien corresponda. Es decir, debe tomar en cuenta diversos elementos que pueden influir en la decisión, como la gravedad del delito, los antecedentes penales del acusado y su grado de implicación en la comisión del delito.

Asimismo, el juez al tener la potestad sancionadora realiza dicha función de manera objetiva, teniendo presente las bases para considerar si tipifica o no el delito en el código penal, las leyes que también estén vinculadas a dicho delito y en aplicación al convenio que el país a firmado, ya que el fenómeno de la ciberdelincuencia percibe el conjunto de delitos que tienen a las TIC como su objetivo principal que son los ciberdelitos esenciales, como aquellos otros en los que las tecnologías constituyen parte de la comisión del hecho punible que son los delitos tradicionales facilitados por las tecnologías. Cuando un juez peruano evalúa un caso de delito informático y determina la culpabilidad del acusado, se basa en la evidencia presentada y en la legislación aplicable para imponer una sanción penal. Debido a que, se debe aplicar el principio de legalidad.

Figura 5:

Monitoreo para la efectividad de la aplicación del convenio Budapest en la legislación



Fuente: Entrevista a operadores jurídicos – Maestros en Derecho Penal y Procesal Penal

Interpretación

La figura 5 muestra la opinión de los operadores jurídicos teniendo en cuenta la pregunta planteada ¿Se han establecido mecanismos de monitoreo y evaluación para evaluar la efectividad de la aplicación del convenio de Budapest por parte de los jueces peruanos?

Obteniendo que las instituciones encargadas de la administración de justicia en Perú, como el Poder Judicial y el Ministerio Público pueden llevar a cabo un seguimiento y análisis de los informes y estadísticas relacionados con los casos de delitos informáticos. Esto permite evaluar la frecuencia, la eficacia y la consistencia de la aplicación del Convenio de Budapest por parte de los jueces. Por otra parte, el siguiente entrevistado manifiesta que en el Perú se puede evidenciar que no existe un seguimiento – vigilancia para los jueces en aplicación de este instrumento. Incluso se podría indicar que la ejecución de esto se merma de manera diferenciada en algunas jurisdicciones del país. Por lo tanto, la efectividad como tal no existe a grandes rasgos pero que su aplicación contribuye en la sanción penal de quien corresponde. Sin embargo, se debe tener en cuenta que, el Estado peruano, a través de sus instituciones pertinentes, lleva a cabo evaluaciones periódicas de la implementación legislativa relacionada con los delitos informáticos. Esto implica revisar y analizar si las leyes y regulaciones nacionales están en consonancia con los estándares y principios del Convenio de Budapest.

Tabla 1:

Análisis a la Ley N° 30096 que regula los delitos informáticos - Aplicación en el Perú.

Ley N° 30096	Resumen	Análisis	Resultado parcial
Ley N° 30096, modificada mediante Ley N°30171	La Ley N° 30096 es una ley diseñada para la prevención y sanción de la ciberdelincuencia, esta consta de 7 capítulos y un capítulo aparte de las disposiciones comunes. Dicha Ley tiene diversos ilícitos que encuentran vinculación intrínseca con el Código Penal y Procesal Penal, a pesar que esta se encuentre en una ley separada, ya que, esta se rige a los mismos artículos para el proceso penal en sí, desde la investigación, diligencias, formas y posteriores acusaciones y juicios orales. La Ley en mención sigue lo postulado por el Convenio de Budapest, que el Perú está adherido, ya que este convenio busca que los Estados miembros coadyuven en la mitigación de estos actos ilícitos novísimos, para la	Los denominados delitos informáticos en un inicio se encontraban tipificados en el catálogo del Código Penal peruano, donde se le consignó a estos como una modalidad agravada del delito de hurto, posteriormente se creó la Ley N°30096, que tiene por objeto prevenir y sancionar aquella conductas que se realizan a través de las nuevas TICS, sin embargo, ante la creación del Convenio de Budapest (Convenio sobre la ciberdelincuencia) y la posterior adhesión del país, se creó la ley N°30171, donde se obtuvo que la ley primigenia, se adecue a lo dispuesto por el Convenio, en los extremos que, deliberada e ilegítimamente se incurran en dichos actuares delictivos, posibilitando que fiscales y jueces realicen solicitudes de asistencia internacional relacionadas con crímenes informáticos, los cuales están regulados por la Ley	Perú es uno de los países que ha ratificado el Convenio de Budapest y ha tomado medidas para incorporar sus disposiciones en su legislación nacional. Al ratificar el convenio, Perú se comprometió a adoptar medidas para prevenir y combatir el ciberdelito, así como para establecer la cooperación internacional en este ámbito. El Convenio de Budapest contrajo consigo que Perú también ha tomado medidas para fortalecer la capacidad de las instituciones encargadas de la aplicación de la ley en la lucha contra el ciberdelito. Se han establecido unidades especializadas dentro de la Policía Nacional y el Ministerio Público para investigar y enjuiciar los delitos informáticos. Estas unidades reciben capacitación especializada y colaboran con otros países en la cooperación internacional en la

	protección de la sociedad.	N.° 30096 según la legislación peruana.	investigación de delitos cibernéticos.

Resultado General:

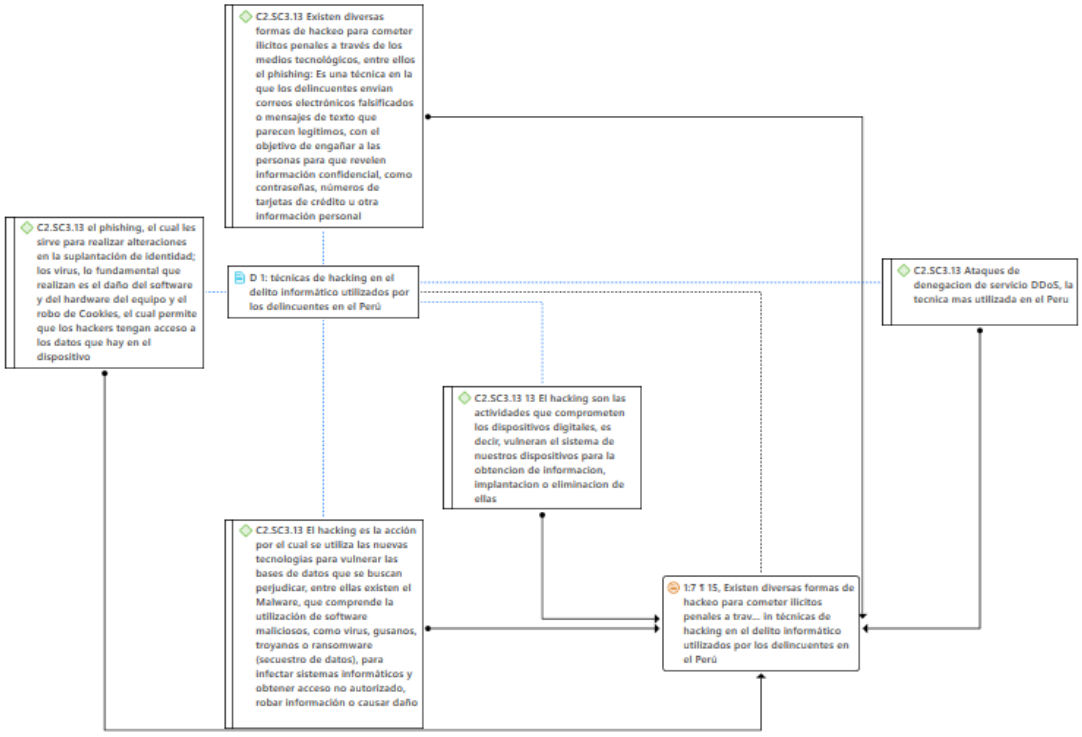
El Convenio de Budapest es un instrumento que se implementó en el Perú, haciendo que el Estado peruano tenga este instrumento para la implementación de diversos mecanismos para prevenir, mitigar, sancionar e intentar erradicar la ciberdelincuencia, generando las directrices adecuadas para que las autoridades policiales, fiscales, judiciales, puedan enfocarse de mejor manera hacia su mitigación. Asimismo, esta adhesión ha generado que exista una red de cooperación internacional entre los países suscritos para que se defina y penalice varias conductas delictivas relacionadas con el uso indebido de tecnologías de la información y la comunicación. Estos delitos incluyen el acceso no autorizado a sistemas informáticos, la interferencia ilegal en datos, la falsificación informática, el fraude informático, la pornografía infantil en línea, entre otros.

Fuente: elaboración propia

En relación al segundo objetivo específico: Investigar los casos de ciberdelincuencia más comunes en el Perú, se tuvo como resultado de la siguiente manera:

Figura 6:

Técnicas de hacking más utilizados por los delincuentes en el Perú



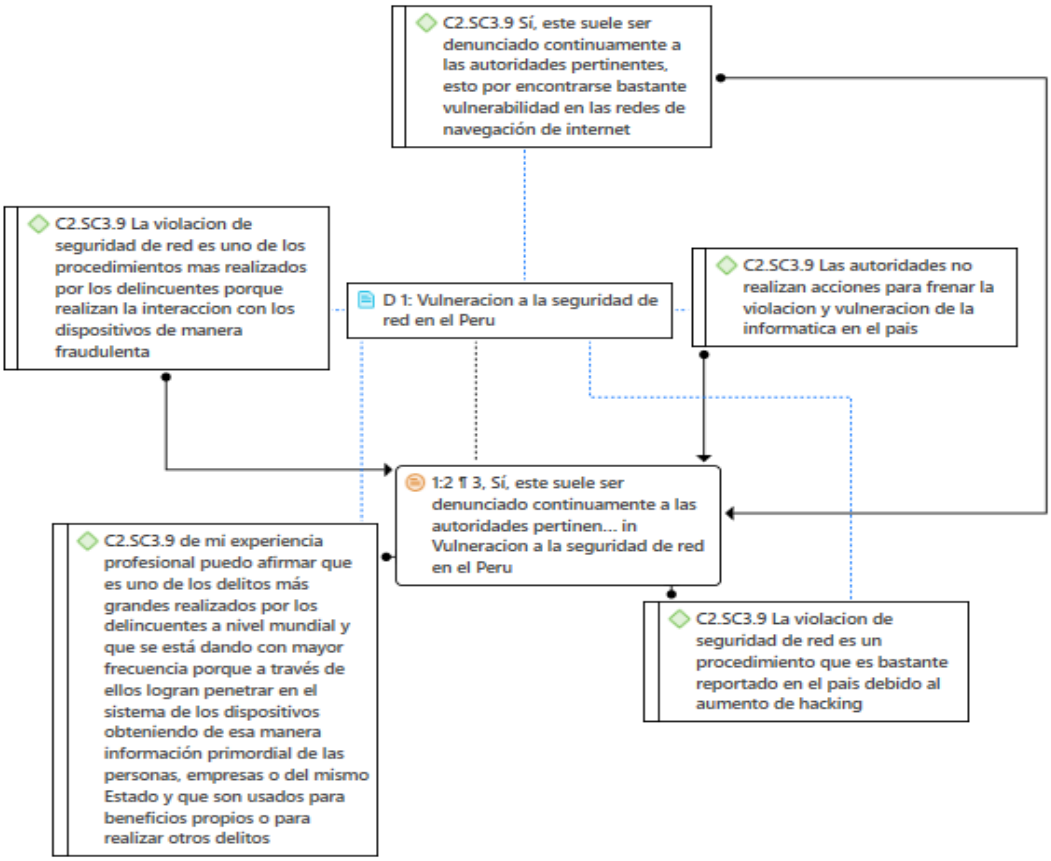
Fuente: Entrevista a operadores jurídicos – Maestros en Derecho Penal y Procesal Penal

Interpretación

De acuerdo a la figura 6 muestra la opinión de los operadores jurídicos teniendo en cuenta la pregunta planteada ¿Qué es y cuáles son las técnicas de hacking en el delito informático utilizados por los delincuentes en el Perú? que, existen diversas técnicas de hacking, entre estos se encuentran los ataques de denegación de servicio (DDoS): Los hackers pueden utilizar una red de dispositivos comprometidos para inundar un sistema o sitio web con una gran cantidad de tráfico, lo que provoca su sobrecarga y la imposibilidad de responder a las solicitudes legítimas. Asimismo, el phishing, el cual les sirve para realizar alteraciones en la suplantación de identidad.

Figura 7:

Vulneración a la seguridad de red en el Perú



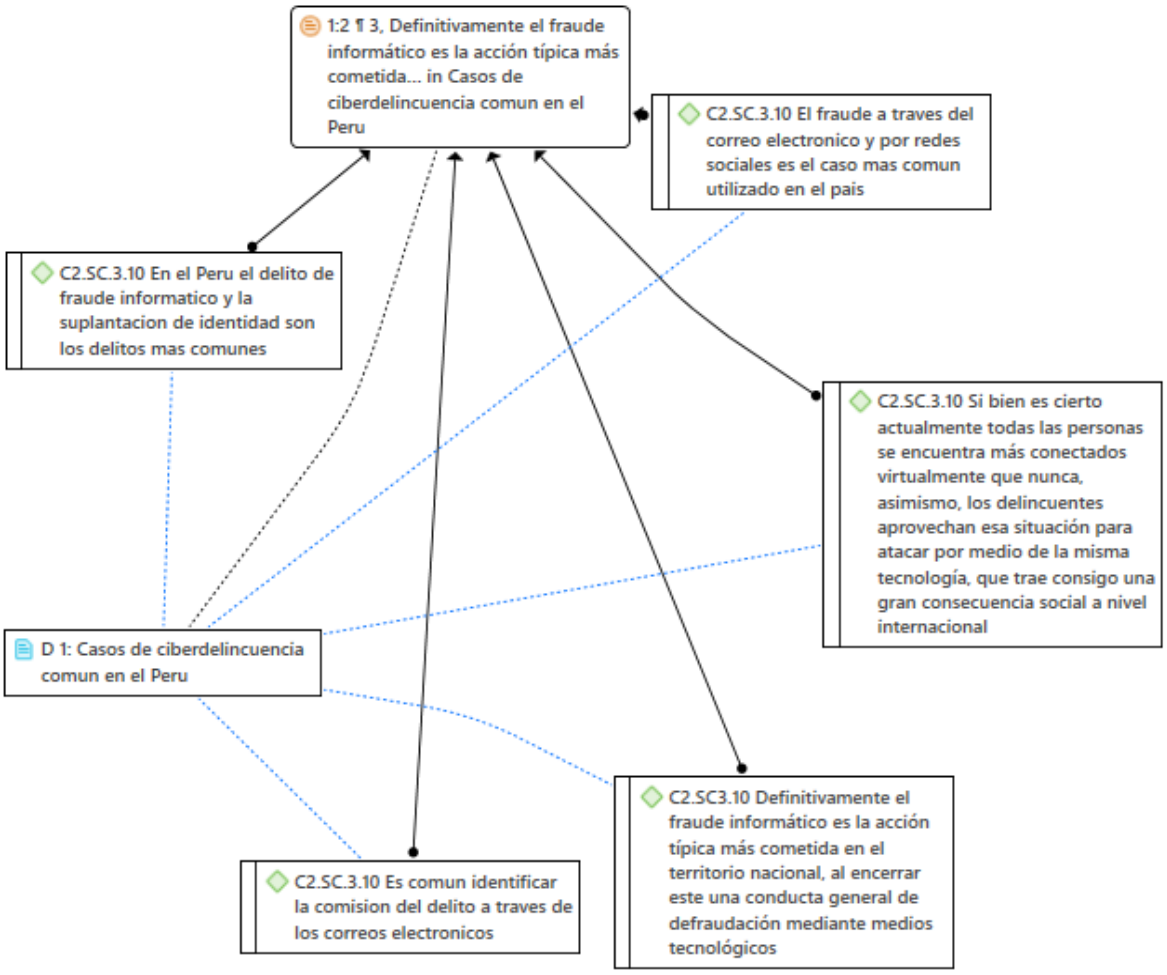
Fuente: Entrevista a operadores jurídicos – Maestros en Derecho Penal y Procesal Penal

Interpretación

La figura 7 muestra la opinión de los operadores jurídicos teniendo en cuenta la pregunta planteada ¿Considera que la violación de seguridad de red es un procedimiento común en el país?;De acuerdo al resultado obtenido, es menester indicar que, la violación de seguridad de red es uno de los procedimientos más realizados por los delincuentes porque realizan la interacción con los dispositivos de manera remota teniendo con ello el total anonimato, entre las víctimas y los delincuentes siendo su principal escudo para la realización de esos delitos. Además, debido a que con el aumento del uso de Internet y la dependencia de las redes para actividades personales y empresariales, aumenta el número de posibles puntos de vulnerabilidad para los ciberdelincuentes, al encontrar en estos puntos mucho rédito económico, ante el desconocimiento del uso de las TICs por parte de las personas comunes y corrientes sin ningún o poco conocimiento en estas nuevas tecnologías.

Figura 8:

Casos de ciberdelincuencia en el Perú



Fuente: Entrevista a operadores jurídicos – Maestros en Derecho Penal y Procesal Penal

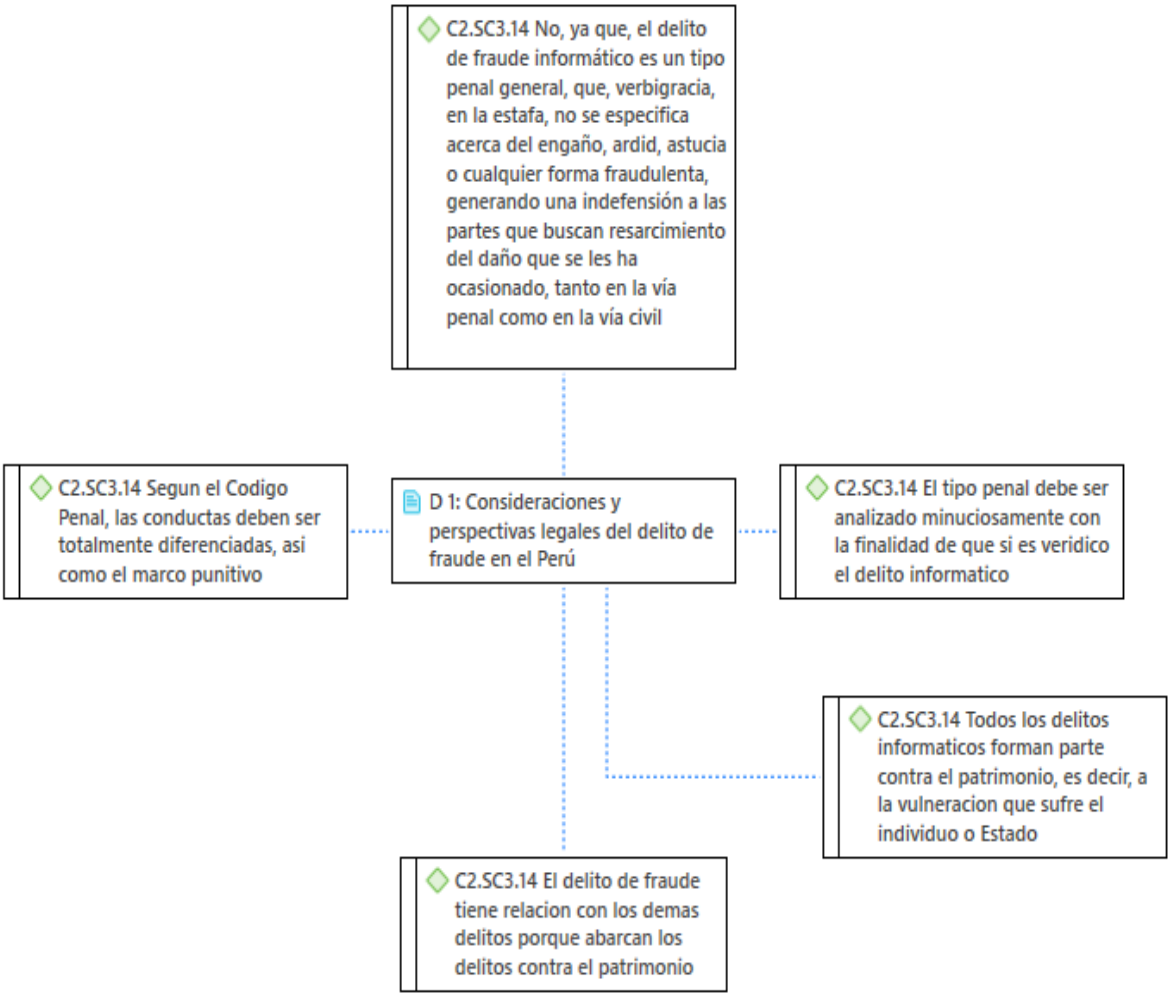
Interpretación

La figura 8 muestra la opinión de los operadores jurídicos teniendo en cuenta la pregunta planteada ¿Cuáles son los casos de ciberdelincuencia mas comunes que se han reportado en el Perú?; La ciberdelincuencia es uno de los movimientos delictivos que tiene mayor celeridad y crecimiento a nivel mundial por la misma necesidad que tienen las personas de estar conectados y eso es aprovechado por los delincuentes, siendo los casos más comunes de ciberdelincuencia que se han reportado en el Perú son: el fraude a través del correo electrónico y por redes sociales, fraude de identidad, robo de datos financieros o de pagos con tarjetas, robo y venta de datos corporativos, la ciber extorsión y el sexting no consentido. Por otra parte, el fraude informático y la

suplantación de identidad son los delitos más comunes conforme a la investigación realizada.

Figura 9:

Consideraciones y perspectivas legales del delito de fraude en el Perú



Fuente: Entrevista a operadores jurídicos – Maestros en Derecho Penal y Procesal Penal

Interpretación

El delito de fraude tiene relación con los demás delitos mencionados porque abarcan los delitos contra el patrimonio, por lo que la realización de dicho delito tiene a fines con las conductas tipificadas para que se considere como tal. Por otra parte, en el Código Penal, las conductas deben ser totalmente diferenciadas, así como el marco punitivo del mismo, debido a que, desde la teoría preventiva general negativa, los operadores legislativos estarían dando

un mensaje incorrecto a la población, de que, si alguien utiliza un medio tecnológico para estafar es lo mismo como si este hubiese hurtado, contradiciendo a la legislación nacional ya existente en delitos comunes.

Tabla 2:

Resultados del segundo objetivo específico – casuística

Jurisprudencia	Resumen	Análisis	Resultado parcial
Sentencia N°01189-2019-PHC/TC LIMA	El abogado del sentenciado interpone demanda de habeas corpus alegando que se ha vulnerado el derecho a la libertad ambulatoria de su patrocinado porque se le ha condenado indebidamente con una ley que no se encontraba en vigencia al momento de ocurrido los hechos, no obstante, el Tribunal Constitucional desestimó su demanda en cuanto los hechos producto de litigio ocurrieron ya entrada en vigencia la ley penal N°30096, que sanciona el fraude informático.	El delito de fraude informático se consignó como delito con la entrada en vigencia de dicha ley, por lo que, en concordancia con la irretroactividad de la ley penal, no se le puede imputar ni mucho menos condenar por una ley que no estaba positivizada al ocurrir los hechos. No obstante, lo alegado por el abogado del beneficiario no fue suficiente, ya que, en sede judicial ya se corroboró que este cometió el delito con la norma en vigencia, y como el TC no es una instancia de sede probatoria, condiciéndose en un fallo correcto.	El delito de fraude informático es el delito más común de ciberdelincuencia reportado en el país, no siendo la presente una excepción, por lo tanto, el Tribunal Constitucional ha fallado conforme al debido proceso, a la sana crítica y los principios constitucionales vigentes.
Casación N°206-2019, LIMA	Se imputó el delito de fraude informático por haber sustraído dinero del fondo de las cuentas bancarias de tarjetas de débito y de crédito del Banco BCP, por lo que, se impuso una reparación civil de S/.5000 (cinco mil con 00/100 soles), esta llegó a instancia	La decisión de la instancia casatoria de aumentar la reparación civil de S/.5000 a S/.20,000 indica que se consideró necesario incrementar la compensación para adecuarla al daño causado, en la medida	Los delitos informáticos, a pesar de no estar regulados propiamente en el código penal, y sí en una ley independiente y especial, esta también se rige a lo estipulado en los parámetros del

	casatoria, declarando haber nulidad de la resolución, reformándola a S/.20,000.00 (veinte mil con 00/100 soles).	que la ciberdelincuencia, aunque fuese delito de peligro abstracto, es merecedora de responsabilidad civil.	Derecho Penal, por lo tanto, en este caso en el delito de fraude informático, también los encontrados culpables son merecedores de reparar civilmente los daños ocasionados, muy a parte del cumplimiento de sus penas que les impongan.
, Recurso de Nulidad N°1220-2022 LIMA	Se imputó al procesado, que era el encargado de embozar los plásticos que contenían información de tarjetas de crédito, copiando los códigos del mismo, clonando 3000 tarjetas de crédito, obteniendo un rédito de $131 306,68 (ciento treinta y un mil trescientos seis con 68/100 dólares), la parte agraviada y la fiscalía superior solicitaron la nulidad de la sentencia que absuelve al acusado, siendo la Corte Suprema la que anula dicha sentencia, y devuelve ordena que otro colegiado para que emita su pronunciamiento.	Se ha logrado advertir que no se ha valorado todos los medios probatorios presentados por fiscalía, estos de modo arbitrario y sin motivación alguna, incurriendo la sala en contravención al debido proceso, es por ello que, de manera correcta y adherida al principio de legalidad, artículo 298 del Código Adjetivo penal.	La Corte Suprema ha fallado de forma correcta, en el sentido que, en el caso en concreto de fraude informático, no se ha valorado las pruebas de manera conjunta sobre los hechos ocurridos, por lo tanto, un nuevo colegiado debe juzgar los mismos, esto en concordancia, a que no se deje de efectuar la acción penal en contra de la ciberdelincuencia y todas sus modalidades.

Resultado General:

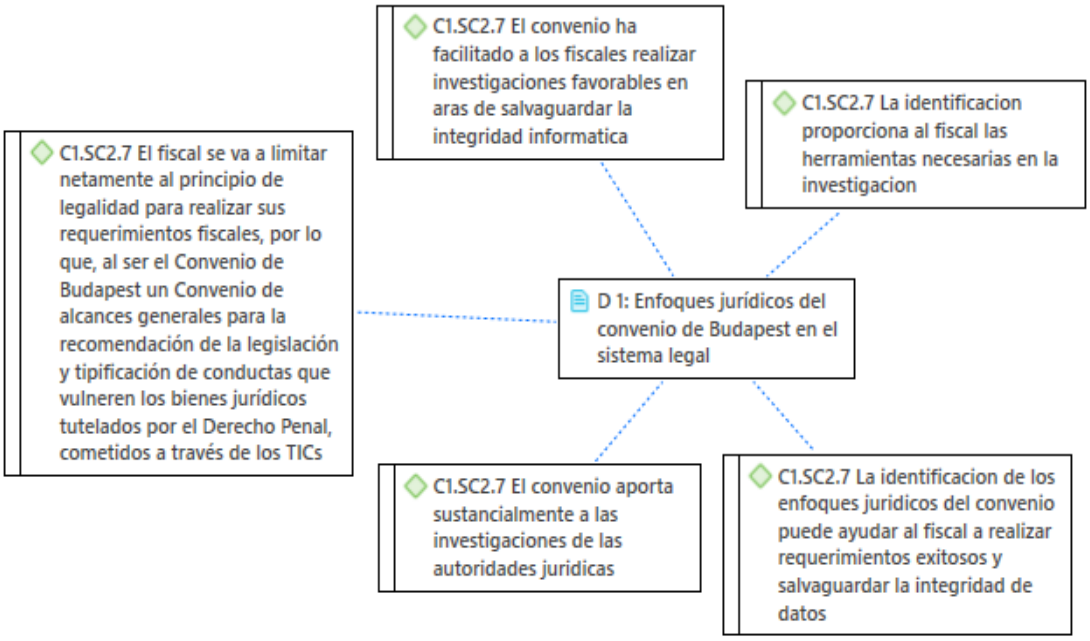
La ciberdelincuencia es un fenómeno que, gracias a la creación de la Ley 30096, tiene menores rasgos de acción, por lo que, el Estado Peruano a través de sus diversos órganos, en este caso, el Poder Judicial, sanciona estos actuares. Se logró colegir que, el delito más común es el de Fraude Informático, al comprender este tipo penal una amplia gama de verbos rectores y supuestos, así como ser la predilecta por los sujetos activos por tener un gran rédito económico y difícil ubicación por lo que comprende cometer estos delitos por la distancia y anonimato que confieren las nuevas tecnologías de la información.

Fuente: elaboración propia

Por último, el tercer OE en: Identificar los efectos jurídicos – sociales del Convenio Budapest en aplicación a los delitos informáticos en el Perú.

Figura 10:

Enfoques jurídicos del convenio de Budapest en el sistema legal



Fuente: Entrevista a operadores jurídicos – Maestros en Derecho Penal y Procesal Penal

Interpretación

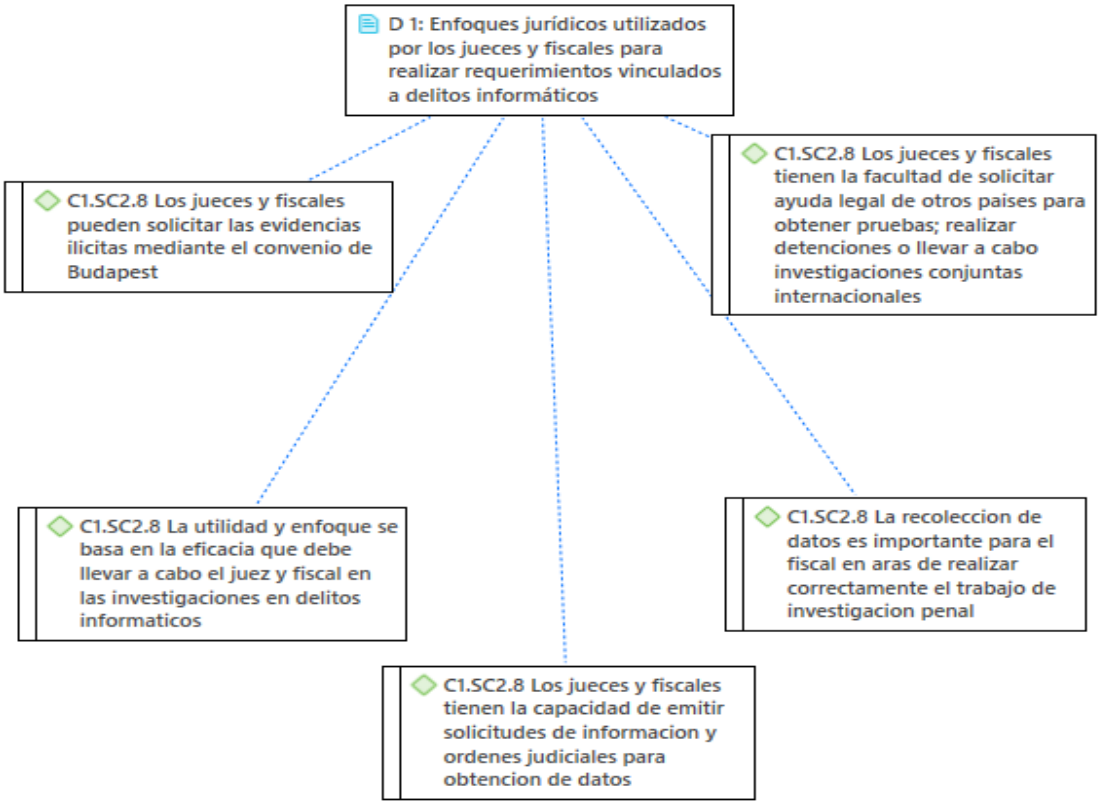
Respecto a la interrogante ¿la identificación de los enfoques jurídicos a través del convenio de Budapest permite al fiscal realizar requerimiento exitoso y salvaguardar la integridad de datos y sistemas informáticos?

La identificación de los enfoques jurídicos a través del Convenio de Budapest puede ayudar al fiscal a realizar requerimientos exitosos y salvaguardar la integridad de datos y sistemas informáticos. El instrumento, además, establece principios y disposiciones legales para combatir el cibercrimen, incluyendo la protección de datos y sistemas informáticos. Estos enfoques jurídicos permiten a los fiscales solicitar información y evidencia digital a través de la cooperación internacional, lo que aumenta las posibilidades de éxito en la obtención de pruebas y la persecución de los responsables. La entrada en vigor en el país del Convenio de Budapest ha facilitado que fiscales a cargo de la investigación

de un ciberdelito puedan requerir a las empresas proveedoras de servicios en internet información necesaria y confidencial.

Figura 11:

Enfoques jurídicos utilizados por los jueces y fiscales para realizar requerimientos vinculados a delitos informáticos



Fuente: Entrevista a operadores jurídicos – Maestros en Derecho Penal y Procesal Penal

Interpretación

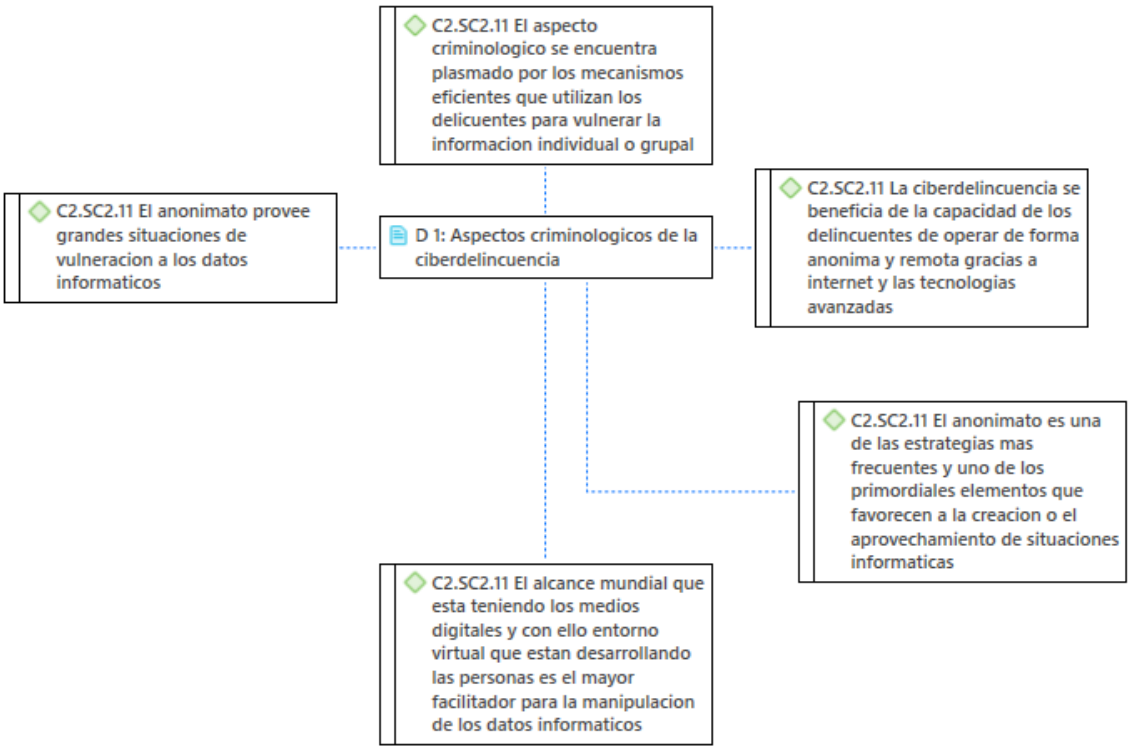
Ante la interrogante ¿Cuáles son los enfoques jurídicos utilizados por los jueces y fiscales para realizar requerimientos vinculados a delitos informáticos en aplicación del convenio de Budapest en la legislación?

El Convenio de Budapest promueve la cooperación internacional en la lucha contra el ciberdelito. Los jueces y fiscales tienen la facultad de solicitar ayuda legal de otros países para obtener pruebas, realizar detenciones o llevar a cabo investigaciones conjuntas en casos de delitos informáticos transfronterizos. Además, utilizan las pruebas recolectadas durante la investigación para llevar a cabo el procesamiento y enjuiciamiento de los presuntos delincuentes. Esto

implica presentar cargos, presentar pruebas ante el tribunal y defender los intereses de la sociedad en el correspondiente juicio. Los jueces y fiscales pueden solicitar a las autoridades competentes que recojan evidencia digital relevante en relación con el delito informático.

Figura 12:

Aspectos criminológicos de la ciberdelincuencia



Fuente: Entrevista a operadores jurídicos – Maestros en Derecho Penal y Procesal Penal

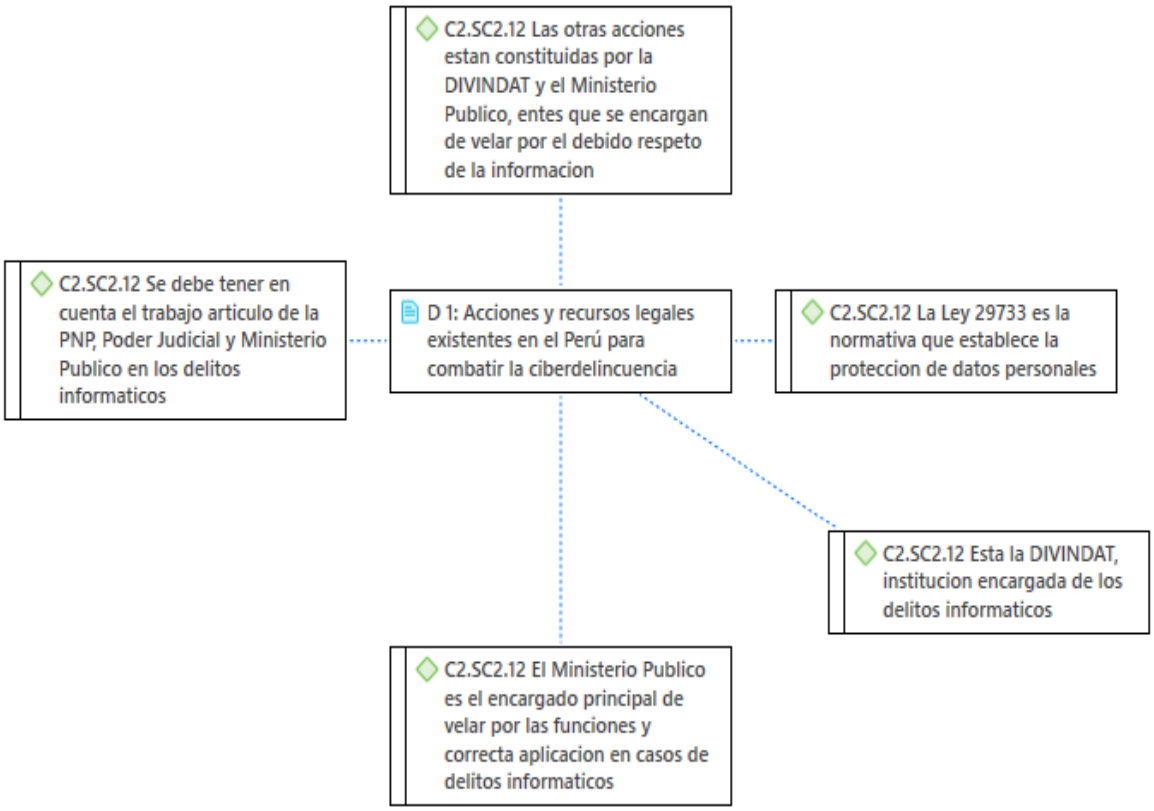
Interpretación

Respecto a la pregunta ¿Cuáles son los aspectos criminológicos de la ciberdelincuencia más utilizada en el país? se ha logrado obtener el resultado en que, un aspecto criminológico bastante ligado con la ciberdelincuencia, es que esta desconoce fronteras y los sujetos activos de estos delitos pueden operar desde cualquier lugar del mundo. Esto crea desafíos adicionales para la investigación y persecución de los delitos, ya que puede requerir la cooperación y coordinación internacional para llevar a los delincuentes ante la justicia. El anonimato es una de las estrategias más frecuentes y uno de los primordiales

elementos que favorecen a la creación o el aprovechamiento de situaciones favorables para la ciberdelincuencia, y que está siendo estudiada por la criminología porque con ello se realiza el encubrimiento de la auténtica identidad de los ciberdelincuentes.

Figura 13:

Acciones y recursos legales existentes en el Perú para combatir la ciberdelincuencia



Fuente: Entrevista a operadores jurídicos – Maestros en Derecho Penal y Procesal Penal

Interpretación

Ante la interrogante ¿Qué otras acciones y recursos legales existen en el Perú para combatir la ciberdelincuencia y proteger a las víctimas?;Las acciones legales se encuentran La División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (DIVINDAT), también el Ministerio Público, a través de sus fiscalías penales corporativas y su Fiscalía Corporativa

Especializada en Ciberdelincuencia de Lima Centro. Como dispositivos legales, a parte de la Ley 30171, existe en el Perú la Ley 30096, Ley de Delitos Informáticos, así como la Ley 29733, Ley de Protección de Datos Personales. Asimismo, como acciones legales se encuentra la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (DIVINDAT), también el Ministerio Público, a través de sus fiscalías penales corporativas y su Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro.

4.2. Discusión

La discusión de resultados de la investigación es una etapa crucial en el proceso de comunicar los hallazgos y conclusiones de un estudio; esta sección permitió al investigador analizar e interpretar los datos obtenidos, compararlos con la literatura existente y evaluar su significado en el contexto de los objetivos de investigación planteada; esto implicó presentar los datos relevantes de manera organizada y destacar los resultados más significativos. En ese sentido, la investigación contó con el objetivo principal de analizar de qué manera el Estado peruano aplica el convenio de Budapest para sancionar delitos informáticos en el año 2022.

Para ello, se parte por la obtención del resultado obtenido del primer objetivo específico, teniendo que el Convenio de Budapest es un instrumento que se implementó en el Perú, haciendo que el Estado peruano tenga este instrumento para la implementación de diversos mecanismos para prevenir, mitigar, sancionar e intentar erradicar la ciberdelincuencia, generando las directrices adecuadas para que las autoridades policiales, fiscales, judiciales, puedan enfocarse de mejor manera hacia su mitigación. Asimismo, esta adhesión ha generado que exista una red de cooperación internacional entre los países suscritos para que se defina y penalice varias conductas delictivas relacionadas con el uso indebido de tecnologías de la información y la comunicación. Estos delitos incluyen el acceso no autorizado a sistemas informáticos, la interferencia ilegal en datos, la falsificación informática, el fraude informático, la pornografía infantil en línea, entre otros.

Dicho resultado se vincula directamente con lo acotado por el autor Huamán (2020), el cual intuye que, el aumento preocupante de los delitos informáticos en Perú se debe a la utilización de diversos y nuevos medios tecnológicos por parte de los ciberdelincuentes, lo que dificulta su identificación y ubicación. Por lo tanto, la adhesión al Convenio de Budapest tiene un impacto relativo en el enfoque hacia los delitos informáticos. El enfoque se centra en la adaptación de nuestra legislación a lo estipulado en dicho Convenio, lo cual implica establecer una lista de delitos, implementar normas procesales que salvaguarden las pruebas digitales y buscar colaboración internacional para examinar la comisión de estos delitos.

En ese sentido, el Convenio de Budapest ha sido fundamental en la adopción de leyes y regulaciones relacionadas con la ciberdelincuencia en el Perú; gracias a este convenio, el país ha adoptado disposiciones legales para la identificación y penalización de delitos cibernéticos, así como para salvaguardar la privacidad y seguridad de la información. Por lo tanto, se ha promovido la cooperación entre Perú y otros Estados Parte en la lucha contra la ciberdelincuencia, lo que implica el intercambio de información, la asistencia recíproca en investigaciones y procesos judiciales, y la posibilidad de extraditar a personas acusadas de cometer delitos informáticos.

Del mismo modo, la teoría que vincula el resultado y antecedente planteado con antelación, es la teoría del delito que se enfoca en el análisis de cualquier acción que tenga como resultado la imposición de una sanción penal o medida de seguridad, lo que se conoce como consecuencia jurídica penal, asimismo, existen diversas teorías que explican el delito y su estructura orgánica, como lo es la teoría del causalismo naturalista; dicho enfoque considera la acción desde una perspectiva física o naturalista, donde se compone de un movimiento corporal y un cambio en el mundo exterior conectados por un vínculo causal, el análisis del delito se clasifica en etapas internas de ideación, deliberación, resolución y externas como la exteriorización, preparación, ejecución.

Esto genera que, la teoría del delito desempeña un papel fundamental en la aplicación del Convenio de Budapest en el Perú, proporcionando los fundamentos legales necesarios para identificar, tipificar y sancionar los delitos

cibernéticos. Esto implica analizar los elementos de conducta, tipicidad, antijuridicidad y culpabilidad para determinar la responsabilidad de los autores de estos delitos en el ámbito digital.

De acuerdo al resultado obtenido del segundo objetivo específico, parte transcendentalmente en que la ciberdelincuencia es un fenómeno que, gracias a la creación de la Ley 30096, tiene menores rasgos de acción, por lo que, el Estado Peruano a través de sus diversos órganos, en este caso, el Poder Judicial, sanciona estos actuares. Se logró colegir que, el delito más común es el de Fraude Informático, al comprender este tipo penal una amplia gama de verbos rectores y supuestos, así como ser la predilecta por los sujetos activos por tener un gran rédito económico y difícil ubicación por lo que comprende cometer estos delitos por la distancia y anonimato que confieren las nuevas tecnologías de la información.

Cabe precisar, además, el delito de fraude tiene relación con los demás delitos mencionados porque abarcan los delitos contra el patrimonio, por lo que la realización de dicho delito tiene a fines con las conductas tipificadas para que se considere como tal. Por otra parte, en el Código Penal, las conductas deben ser totalmente diferenciadas, así como el marco punitivo del mismo, debido a que, desde la teoría preventiva general negativa, los operadores legislativos estarían dando un mensaje incorrecto a la población, de que, si alguien utiliza un medio tecnológico para estafar es lo mismo como si este hubiese hurtado, contradiciendo a la legislación nacional ya existente en delitos comunes.

El resultado en mención se encuentra vinculado directamente con lo acotado por el antecedente de los autores Álvarez y Hevia (2020), que, en términos económicos, la ausencia de excepciones para la investigación en la legislación podría amenazar con asfixiar el incipiente mercado de los servicios y profesionales en ciberseguridad, al excesivamente regular el mercado, las leyes que permiten el acceso no autorizado sin protecciones legales para la investigación y detección de vulnerabilidades, han sido utilizadas para intentar callar la investigación en el campo de la seguridad digital. En muchas ocasiones, los fabricantes de sistemas con debilidades, al recibir notificaciones, han optado por amenazar con emprender acciones legales para silenciar a los

investigadores, a menudo para salvaguardar la reputación de la compañía o para mantener su posición dominante en el mercado.

Asimismo, la teoría del delito, el mismo que también se encuentra vinculado con el resultado del segundo objetivo específico; pues, la teoría del delito aplicada a los delitos informáticos es una herramienta que busca entender y explicar la comisión de este tipo de delitos en el ámbito digital. Esta teoría se basa en los elementos fundamentales del delito tradicional y los adapta al entorno virtual. En los delitos informáticos, se identifican los mismos elementos que en cualquier otro delito: la acción, la tipicidad, la antijuridicidad, la culpabilidad y la punibilidad. La acción se refiere a los actos realizados por una persona que afectan de manera ilícita los sistemas informáticos o la información almacenada en ellos.

La tipicidad se relaciona con la descripción legal de los actos que constituyen un delito informático. Se establecen leyes y normativas específicas que definen qué conductas son consideradas delictivas en el ámbito digital, como el acceso no autorizado a sistemas informáticos, la divulgación o manipulación de datos sin consentimiento, el fraude electrónico, entre otros. La antijuridicidad se refiere a la contradicción entre la conducta realizada y el ordenamiento jurídico. En el caso de los delitos informáticos, esta antijuridicidad se establece cuando se vulneran normas y derechos relacionados con la seguridad y privacidad de la información, el acceso indebido a sistemas protegidos o el daño a infraestructuras informáticas.

En los delitos informáticos, se evalúa si el autor actuó con intención y conocimiento de la ilicitud de su conducta, o si existió negligencia o imprudencia en su accionar; respecto a la punibilidad, es la posibilidad de imponer una sanción o pena al autor del delito. En los delitos informáticos, las sanciones pueden incluir multas, penas de prisión u otras medidas legales, dependiendo de la gravedad y las circunstancias del delito.

Los resultados del tercer objetivo específico, se ha obtenido en concordancia que, los enfoques jurídicos a través del Convenio de Budapest pueden ayudar al fiscal a realizar requerimientos exitosos y salvaguardar la integridad de datos

y sistemas informáticos. El instrumento, además, establece principios y disposiciones legales para combatir el cibercrimen, incluyendo la protección de datos y sistemas informáticos. Estos enfoques jurídicos permiten a los fiscales solicitar información y evidencia digital a través de la cooperación internacional, lo que aumenta las posibilidades de éxito en la obtención de pruebas y la persecución de los responsables.

El Convenio de Budapest promueve la cooperación internacional en la lucha contra el ciberdelito. Los jueces y fiscales tienen la facultad de solicitar ayuda legal de otros países para obtener pruebas, realizar detenciones o llevar a cabo investigaciones conjuntas en casos de delitos informáticos transfronterizos. Además, utilizan las pruebas recolectadas durante la investigación para llevar a cabo el procesamiento y enjuiciamiento de los presuntos delincuentes. Esto implica presentar cargos, presentar pruebas ante el tribunal y defender los intereses de la sociedad en el correspondiente juicio. Los jueces y fiscales pueden solicitar a las autoridades competentes que recojan evidencia digital relevante en relación con el delito informático.

Los aspectos criminológicos bastantes ligados con la ciberdelincuencia, es que esta desconoce fronteras y los sujetos activos de estos delitos pueden operar desde cualquier lugar del mundo. Esto crea desafíos adicionales para la investigación y persecución de los delitos, ya que puede requerir la cooperación y coordinación internacional para llevar a los delincuentes ante la justicia. El anonimato es una de las estrategias más frecuentes y uno de los primordiales elementos que favorecen a la creación o el aprovechamiento de situaciones favorables para la ciberdelincuencia, y que está siendo estudiada por la criminología porque con ello se realiza el encubrimiento de la auténtica identidad de los ciberdelincuentes.

El resultado en mención, se vincula por lo esbozado por el autor Huamán (2020), al indicar que, con el aumento preocupante de los delitos informáticos en Perú se debe a la utilización de diversos y nuevos medios tecnológicos por parte de los ciberdelincuentes, lo que dificulta su identificación y ubicación. Por lo tanto, la adhesión al Convenio de Budapest tiene un impacto relativo en el enfoque hacia los delitos informáticos. El enfoque se centra en la adaptación

de nuestra legislación a lo estipulado en dicho Convenio, lo cual implica establecer una lista de delitos, implementar normas procesales que salvaguarden las pruebas digitales y buscar colaboración internacional para examinar la comisión de estos delitos.

Asimismo, la teoría de la pena es la vinculante con el resultado obtenido, debido a que se advierte la prevención general, la imposición de penas en los delitos informáticos tiene como objetivo principal prevenir que otros potenciales delincuentes cometan actos similares. La pena debe enviar un mensaje claro y disuasorio a la sociedad en general, mostrando las consecuencias negativas y el rechazo social que conlleva la comisión de estos delitos. Asimismo, la prevención especial que, la pena también tiene como finalidad la prevención especial, es decir, la reeducación y resocialización del delincuente informático. A través de medidas de rehabilitación, se busca que el autor del delito adquiera conciencia sobre la gravedad de sus acciones y se reintegre de manera positiva a la sociedad, evitando así la reincidencia.

V. CONCLUSIONES

5.1. La primera conclusión abarca el estudio de la aplicación del convenio Budapest en la legislación nacional, el mismo que ha sido de suma importancia para fortalecer la respuesta del país frente a la ciberdelincuencia. A través de la adopción de leyes y regulaciones específicas, se ha logrado tipificar y sancionar los delitos cibernéticos, protegiendo así la privacidad y la seguridad de la información. Asimismo, esta aplicación ha facilitado la cooperación con otros Estados en la lucha contra la ciberdelincuencia, permitiendo cambios radicales en la sanción penal contra el acusado por dicho delito. Por ello, la esta integración del Convenio de Budapest en la legislación nacional, el Perú ha dado pasos significativos para combatir la ciberdelincuencia y garantizar la seguridad en el ámbito digital.

5.2. La segunda conclusión respecto al estudio de la aplicación del convenio de Budapest en la legislación peruana muestra la importancia y el compromiso de Perú en la lucha contra los delitos informáticos. La adopción y adaptación de este convenio internacional ha permitido fortalecer el marco legal y normativo del país en materia de ciberdelincuencia, proporcionando herramientas efectivas para combatir y prevenir este tipo de delitos. La legislación peruana ha incorporado los principios y disposiciones del Convenio de Budapest en sus leyes y reglamentos relacionados con los delitos informáticos. Esto incluye la definición de nuevos tipos penales, la mejora de los mecanismos de investigación y persecución, así como la promoción de la cooperación internacional en la lucha contra la ciberdelincuencia.

5.3. La tercera conclusión acerca de los casos de ciberdelincuencia más comunes en el Perú incluye el fraude electrónico, el robo de datos personales y la suplantación de identidad, para ello, es necesario que las autoridades peruanas fortalezcan los mecanismos de prevención, investigación y persecución de la ciberdelincuencia. Esto implica una colaboración estrecha entre el sector público, el sector privado y la

sociedad civil para abordar de manera efectiva estos delitos y proteger la integridad y privacidad de los ciudadanos peruanos en el entorno digital.

5.4. La cuarta conclusión respecto a la identificación de los efectos jurídicos – sociales del Convenio Budapest en aplicación a los delitos informáticos en el Perú; la adopción de este convenio ha permitido fortalecer la legislación y los mecanismos legales en el país para hacer frente a la ciberdelincuencia, así como para promover la cooperación internacional en este ámbito. Desde un punto de vista jurídico, la implementación del Convenio de Budapest ha facilitado la definición y tipificación de nuevos delitos informáticos en la legislación peruana. Esto ha permitido una mejor protección D° de las víctimas y una mayor eficacia en la persecución y sanción de los responsables. En términos sociales, la aplicación del Convenio de Budapest ha contribuido a crear conciencia sobre los riesgos y desafíos de la ciberdelincuencia en la sociedad peruana. Se ha promovido la educación en seguridad digital y la adopción de medidas de protección por parte de los ciudadanos y las empresas, lo que ha llevado a un mayor nivel de precaución y prevención frente a los delitos informáticos.

VI. RECOMENDACIONES

6.1. Al estado peruano, solicitar asistencia y cooperación en la investigación y enjuiciamiento de delitos informáticos a otros Estados que también hayan ratificado el Convenio de Budapest. De igual manera, Perú también puede brindar asistencia y cooperación a otros países en casos de delitos informáticos.

6.2. Se recomienda al área académica del Ministerio de Justicia realizar la instrumentalidad del convenio Budapest en aras de ayudar de la protección a la sociedad de los riesgos asociados con los delitos cibernéticos, como el robo de datos, el fraude en línea y la violación de la privacidad. Al establecer mecanismos legales efectivos, se fomenta un ambiente digital más seguro y confiable para todos los peruanos. Además, esto contribuirá a fortalecer la confianza en el entorno digital, tanto a nivel nacional como internacional, lo que a su vez fomentará el desarrollo del comercio electrónico, la innovación tecnológica y el crecimiento del sector digital en el país.

6.3. Se recomienda a la Policía Nacional del Perú en proporcionar información continua y especializada a los agentes encargados de investigar delitos informáticos. Esto incluye la actualización constante sobre las últimas técnicas y tendencias en ciberdelincuencia, así como el conocimiento de las disposiciones del Convenio de Budapest y su implementación en la legislación peruana.

6.4. Se recomienda al Poder Legislativo actualizar y adaptar la normativa vigente ya que la tecnología evoluciona constantemente, por lo que es fundamental que el Estado peruano mantenga actualizada su Ley de Delitos Informáticos para hacer frente a los nuevos retos y amenazas que surjan en el ámbito digital.

REFERENCIAS

Almazán, L. (2020). Implicaciones legales en materia de propiedad intelectual en México en caso de la adopción del convenio de Budapest. *Infotec posgrados*. Obtenido de https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/310/3/INFOTEC_MDTIC_LAAM_21102019.pdf

Álvarez, D; Hevia, A. (2020). Protección legal para la búsqueda y notificación de vulnerabilidades de ciberseguridad en Chile. *Dialnet*. Obtenido de https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000200001&lang=es

Arias, F. (2012). El proyecto de investigación: Introducción a la metodología científica. *Editorial Episteme*. Obtenido de https://abacoenred.com/wp-content/uploads/2019/02/El-proyecto-de-investigaci%C3%B3n-F.G.-Arias-2012-pdf-1.pdf

Arias, J; Covinos, M. (2021). Diseño y Metodología de la Investigación. *Enfoques consulting EIRL*. Obtenido de http://repositorio.concytec.gob.pe/bitstream/20.500.12390/2260/1/Arias-Covinos-Dise%c3%b1o_y_metodologia_de_la_investigacion.pdf

Bacigalupo, E. (1999). Derecho penal; parte general. *Hammurabi*. Obtenido de https://proyectozero24.com/wp-content/uploads/2021/09/Bacigalupo-1999-Derecho-Penal.-Parte-General.pdf

Basantes, S. (2014). *Modelo de Gestión Administrativa y la Calidad en el Servicio al Cliente en el Gobierno Autónomo Descentralizado Municipalidad de Ambato.* Ambato: Universidad Técnica de Ambato.

Becker, S. (2020). La implementación del Convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223. *Dialnet*. Obtenido de https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-591X2020000200075&lang=es

Blossiers, J. (2019). El delito informático y su incidencia en la empresa bancaria. *Universidad Nacional Federico Villarreal*. Obtenido de https://www.congreso.gob.pe/Docs/comisiones2020/CE-Tribunal-Constitucional/files/postulantes/exp037/tesis.pdf

Cabrero, E., & Mendoza, D. (2014). *Los gobiernos municipales a debate: Un análisis de la institución municipal a través de la Encuesta INEGI 2009* (1 era ed.). México: Ink.

Calduch, R. (2010). Métodos y técnicas de investigación en relaciones internacionales. *Universidad Complutense de Madrid*. Obtenido de https://www.ucm.es/data/cont/media/www/pag-55163/2Metodos.pdf

Campos, S., & Loza, P. (2011). *incidencia de la gestión administrativa de la biblioteca municipal "Pedro Moncayo" de la ciudad de Ibarra en mejora de la calidad de servicios y atención a los usuarios en el año 2011. Propuesta alternativa.* Ibarra: Universidad Técnica del Norte.

Ceja, G. (1994). *Planeación y organización de empresas* (Octava ed.). México: Mc Graw Hill.

Chiavenato, I. (2006). *Introducción a la teoría general de la Administración* (8a ed.). México: Mexicana.

Córdoba, M; Ruiz, C. (2009). Teoría de la pena, Constitución y Código Penal. *Redalyc*. Obtenido de https://dialnet.unirioja.es/descarga/articulo/5312256.pdf

Cubas, O. (2023). Tratado de Budapest sobre el reconocimiento internacional del depósito de microorganismos a los fines del procedimiento en materia de patentes. *Redalyc*. Obtenido de https://www.wipo.int/export/sites/www/treaties/es/registration/budapest/pdf/wo_inf_12.pdf

De la Torre, J. (2014). *Reforma municipal y capacidad de gestión de los gobiernos municipales en México: un estudio comparado en seis municipios del estado*

de San Luis Potosí, México (1983-2000). Madrid: Universidad Complutense de Madrid.

Díaz, A. (2020). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio Budapest. *Universidad de la Rioja*. Obtenido de https://www.unirioja.es/dptos/dd/redur/numero8/diaz.pdf

Echandía, D. (2000). Teoría General del Proceso. *Editorial Universidad*. Obtenido de https://andrescusi.files.wordpress.com/2020/06/teoria-general-del-proceso-devis-echandia.pdf

Everardo, B. (2011). *Recaudación fiscal y certificación profesional: enlace de dos políticas públicas. Dilemas de las Políticas en públicas en Latinoamérica* (1 era ed.). México: FLACSO / UABC.

Fayol, H. (1916). *Administración industrial y general.* Paris: El Ateneo.

García, J. (2019). ¿Dogmática penal sistémica? Sobre la influencia de Luhmann en la teoría penal. *Dialnet*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=2337396

George, D., & Mallery, P. (2003). *SPSS for Windows step by step: A simple guide and reference. 11.0 update* (4th ed.). Boston: Allyn & Bacon.

González, M. (2015). La Ley del Talión: una aproximación. *Universidad de Vigo*. Obtenido de https://caumas.org/wp-content/uploads/2017/11/La-Ley-del-Talio%CC%81n.pdf

Gozaíni, O. (2013). Elementos del Derecho Procesal Civil. *Dialnet*. Obtenido de https://gozaini.com/wp-content/uploads/2018/08/Elementos-de-DPC-Ediar.pdf

Hernández Sampieri, R. (2016). *Metodología de la Investigación.* Lima: Mc Graw Hill.

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

https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/4116/Marleny_Tesis_bachiller_2020.pdf?sequence=1&isAllowed=y

Hurtado, J. (1987). Manual del Derecho Penal. *EDDILI*. Obtenido de https://perso.unifr.ch/derechopenal/assets/files/obrasjuridicas/oj_20080609_04.pdf

Jakobs, G. (1998). Sobre la Teoría de la Pena. *Centro de Investigaciones de Derecho Penal y Filosofía del Derecho*. Obtenido de https://perso.unifr.ch/derechopenal/assets/files/articulos/a_20170508_03.pdf

Koontz, H., & Weihrich, H. (2007). *Elementos de Administración: Un enfoque internacional y de innovación* (7ma ed.). México: MGraw Hill Internacional.

Koontz, H., O Donnell, C., & Weihrich, H. (1986). *Administración.* México: McGraw-Hill.

López, J. (2001). Derecho penal: parte general. *Dialnet*. Obtenido de https://es.scribd.com/document/134130984/Autoria-y-participacion-Lopez-Barja-de-Quiroga

Louffat, E. (2012). *Administración: Fundamentos del proceso administrativo* (3era ed.). Buenos Aires: Cengage Learning.

Marin, R., Barreix, A., & Machado, R. (2015). *Recaudar para crecer: bases para la reforma tributaria en Centroamérica* (1era ed.). México: IDB.

Meini, I. (2013). La pena: función y presupuestos. *Editorial PUCP*. Obtenido de https://revistas.pucp.edu.pe/index.php/derechopucp/article/view/8900/9305

Melinkoff, R. (2005). *Los procesos administrativos.* Caracas: Panapo.

Merino, A., Sáenz, E., & Silva, M. (2016). *La influencia de la gestión administrativa en la satisfacción del usuario de la municipalidad de comas, 2016.* Lima: Universidad Inca Garcilaso de la Vega.

Montero, J. (1991). Derecho jurisdiccional: parte general. *J.M. Bosch Editor*, pag. 468.

Morales, D. (2020). La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú. *Universidad Señor de Sipán*. Obtenido de https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/3161/MORALES_DELGADO_DEIVID_1%20YULY-1.%20turnitin.pdf?sequence=6&isAllowed=y

Mori, P. (2018). *Relación de la recaudación tributaria con el desarrollo local gestionado por la municipalidad distrital de Barranquita, 2018.* Tarapoto: Universidad César Vallejo.

Morlote, N; Celiseo, R. (2004). Metodología de la investigación. *McGrawHill*. Obtenido de http://cotana.informatica.edu.bo/downloads/Metodologia-de-la-investigacion-cuaderno%20de%20trabajo.pdf

Munch, L. (2014). *Administración: Gestión organizacional, enfoques y proceso administrativo* (2da ed.). México: Mexicana.

Muñoz, F; García, M. (2002). Derecho Penal, Parte General. *Tirant lo blanch Valencia*. Obtenido de https://www.derechopenalenlared.com/libros/Derecho_Penal_Parte_General_Munoz_Conde_Mercedes_Aran.pdf

Ñañez, O. (2017). *Gestión administrativa en las Municipalidades de Azángaro y Chocos - Lima, 2016.* Lima: Universidad César Vallejo.

Ñaupas, H. (2009). *Metodología de la Investigación científica y asesoramiento de tesis.* Lima - Perú.

Ojeda, J; Arias, M; Rincón, F; Daza, L. (2019). Delitos informáticos y entorno jurídico vigente en Colombia. *Redalyc*. Obtenido de https://www.redalyc.org/articulo.oa?id=383668928003

Paucar, Y. (2018). *Relación de la gestión administrativa con la recaudación tributaria en la Municipalidad Provincial de Moyobamba, año 2016.* Tarapoto: Universidad César Vallejo.

Peña, O; Almanza, F. (2010). Teoría del Delito; manual práctico para su aplicación en la teoría del caso. *Asociación Peruana de Ciencias Jurídicas y Conciliación*. Obtenido de https://static.legis.pe/wp-content/uploads/2019/06/Teoria-del-delito.pdf

Pinedo, A. (2013). *Recaudación municipal y su relación con la ejecución de obras gestionadas por administración directa periodo 2008 – 2013.* Tarapoto: Universidad Cesar Vallejo.

Playor, S. (2008). *Gestión empresarial* (3era ed.). Lima: Editorial hemisferio.

Quintero, B; Prieto, E. (1995). Teoría General del Proceso. *Editorial Temis*. Obtenido de https://corteidh.or.cr/tablas/17525.pdf

Reinhart, M; Gossel, K; Heinz, Z. (1995). Derecho penal. Parte general. *Astrea*, 146-148.

Rodríguez, C; Lorenzo, O; Herrera, L. (2005). Teoría y práctica del análisis de datos cualitativos. Proceso general y criterios de calidad. *Universidad de Granada*. Obtenido de https://www.redalyc.org/articulo.oa?id=65415209

Rodríguez, D. (2019). Pena (Teoría de la). *Universidad Autónoma de Madrid*. Obtenido de https://e-revistas.uc3m.es/index.php/EUNOM/article/download/4701/3176/

Santillán, J., & Villanueva, D. (2013). *Propuesta de sistema de gestión administrativo para la compañía Poison S.A.* Guayaquil: Universidad Laica Vicente Rocafuerte de Guayaquil.

Santolaya, M. (2011). *Supuestos prácticos de recaudación tributaria* (1era ed.). México: CISS.

Soto, R. (2017). *El liderazgo y la gestión administrativa de la municipalidad distrital San Pedro de Chaná – Huari, en el año 2017.* Huacho: Universidad Nacional José Faustino Sánchez Carrión.

Terry, G., & Franklin, S. (1994). *Administración.* México: Continental.

Valdera, J. (2016). *Relación entre la recaudación tributaria y la inversión en el desarrollo local ejecutado por la Municipalidad Provincial Alto Amazonas, 2015.* Yurimaguas: Universidad César Vallejo.

Valderrama, S. (2016). *Pasos para elaborar proyectos de investigación científica* (6 ta ed.). Lima: San Marcos.

Van, A. (2018). Optimización de la autonomía y deberes penales de solidaridad. *Dialnet*. Obtenido de https://www.scielo.cl/pdf/politcrim/v13n26/0718-3399-politcrim-13-26-01074.pdf

Villabella, C. (2000). Los métodos en la investigación jurídica. Algunas precisiones. *Dialnet*. Obtenido de https://archivos.juridicas.unam.mx/www/bjv/libros/8/3983/46.pdf

White, O. (2008). Teoría General del Proceso. *Escuela Judicial*. Obtenido de https://www.pensamientopenal.com.ar/system/files/2014/12/doctrina40381.pdf

Zaffaroni, E. (1981). Tratado de Derecho Penal. *Sociedad Anónima Editorial de Derecho*. Obtenido de https://www.salapenaltribunalmedellin.com/images/doctrina/libros01/Tratado_De_Derecho_Penal_-_Parte_General-III.pdf

Zolezzi, L. (1997). La teoría general del proceso. *Dialnet*. Obtenido de file:///C:/Users/nixso/Downloads/Dialnet-LaTeoriaGeneralDelProceso-5002618.pdf

ANEXOS

Anexo 1: Matriz de categorización

Categoría de estudio	Definición conceptual	Categoría	Subcategorías	Códigos
Convenio Budapest	Consiste en el único acuerdo internacional sobre delitos informáticos que, fundamentalmente, hace hincapié en las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de seguridad de red.	**Convenio Budapest**	Principio de legalidad Teoría de la pena Enfoque jurídico	C1 C1.SC1.1 C1.SC2.2 C1.SC3.3
Delitos informáticos	Sanciona a toda persona que procura a través de las tecnologías de la información o de la comunicación, un beneficio o provecho ilícito para sí o para otro en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia.	**Delitos informáticos**	Violaciones de seguridad de red Aspectos criminológicos Fraude informático	C2 C2.SC1.4 C2.SC1.5 C2.SC1.6 C2.SC1.8 C2.SC2.9

Anexo 2: Matriz de consistencia: Aplicación del convenio de Budapest y delitos informáticos en el Perú, 2022.

<table>
<tr><th>Formulación del Problema</th><th>Objetivos</th><th colspan="2">Hipótesis</th><th>Técnicas e Instrumentos</th></tr>
<tr><td>Problema general
¿De qué manera el Estado peruano aplica el Convenio Budapest para sancionar los delitos informáticos en el año 2022?

Problemas específicos
¿De qué manera se estudia la aplicación del convenio de Budapest en la legislación peruana?
¿Cuáles son los casos de ciberdelincuencia más comunes en el Perú?
¿Cuáles son los efectos jurídicos – sociales del Convenio Budapest en aplicación a los delitos informáticos en el Perú?</td><td>Objetivo general
Analizar de qué manera el Estado peruano aplica el Convenio Budapest para sancionar los delitos informáticos en el año 2022.

Objetivos específicos
OE1: Estudiar la aplicación del convenio de Budapest en la legislación peruana.
OE2: Investigar los casos de ciberdelincuencia más comunes en el Perú.
OE3: Identificar los efectos jurídicos – sociales del Convenio Budapest en aplicación a los delitos informáticos en el Perú.</td><td colspan="2">En la investigación cualitativa puede prescindirse del planteamiento de la hipótesis porque no se hacen suposiciones previas, se busca indagar desde lo subjetivo la interpretación de las personas acerca de los fenómenos de la realidad que se investigan y por no existir mediciones posibles. Por lo tanto, la investigación no cuenta con hipótesis por encontrarse desarrollado a través del enfoque cualitativo siendo no mediable la información contenida.</td><td rowspan="3">Técnica:
Entrevista
Análisis de datos

Instrumentos:
Guía de análisis documental.
Guía de entrevista</td></tr>
<tr><th>Diseño de investigación</th><th>Escenario de estudio y Participantes</th><th colspan="2">Categorías y Subcategorías</th></tr>
<tr><td rowspan="2">Tipo de investigación:
Básica
Se caracteriza porque se origina en un marco teórico y permanece en él. El objetivo es incrementar los conocimientos científicos, pero sin contrastarlos con ningún aspecto práctico.
Diseño de la investigación:
Teoría fundamentada
enfatiza el papel del investigador como un instrumento activo en la construcción de la teoría. Los investigadores deben ser reflexivos y conscientes de sus propias influencias y preconcepciones</td><td rowspan="2">Escenario de estudio:
El escenario de estudio es a nivel nacional según jurisprudencia identificadas.

Participantes:
- 03 expedientes
- 05 abogados litigantes</td><td>Categorías:</td><td>Subcategorías:</td></tr>
<tr><td rowspan="3">Convenio Budapest</td><td>Principio de legalidad</td></tr>
<tr><td>Teoría de la pena</td></tr>
<tr><td>Enfoque jurídico</td></tr>
<tr><td rowspan="4">Delitos informáticos</td><td>violaciones de seguridad de red</td></tr>
<tr><td>Aspectos criminológicos</td></tr>
<tr><td>Fraude informático</td></tr>
<tr><td></td></tr>
</table>

Anexo 3: Guía de entrevista a expertos

Abogados, maestros en Derecho Penal y Procesal Penal

Es grato dirigirme a Usted con la finalidad de indicar lo siguiente:

Ocupa Sánchez, Bammy Sharum, identificado con Documento Nacional de Identidad N° 71883708, estudiante de la Escuela de Posgrado, de programa de Maestría en Derecho Penal y Procesal Penal de la Universidad César Vallejo SAC - Tarapoto. En esta oportunidad, me encuentro realizando una guía de preguntas para formalizar de manera efectiva el trabajo de investigación titulada *"Aplicación del convenio Budapest y delitos informáticos en el Perú en el 2022".*

Agradezco a Usted se sirva contestar las preguntas planteadas con la mayor sinceridad posible. Gracias por su amabilidad.

Entrevistado :

Grado académico :

Centro laboral :

Objetivo general: Analizar de qué manera el Estado peruano aplica el convenio de Budapest para sancionar delitos informáticos en el año 2022.

Categoría 1. Convenio de Budapest

1. Desde su experiencia profesional ¿Considera que la aplicación del convenio de Budapest ha aportado sustancialmente a la legislación peruana? ¿Por qué?

   ……

   ……
2. ¿En qué medida los jueces peruanos utilizan el convenio de Budapest como marco legal para abordar casos de delitos informáticos?

   ……

   ……

   ……

3. Teniendo en cuenta la ratificación del convenio regulado en la legislación en la Ley N.°30171 ¿Cuáles son los principales desafíos o dificultades que enfrentan los jueces y fiscales al aplicar el convenio de Budapest en la legislación nacional?

   ……
   ……
   ……

4. ¿De qué manera el juez realiza la función de la sanción penal o pena tiene asignada sobre la base de la aplicación del convenio?

   ……
   ……
   ……

5. ¿Se han establecido mecanismos de monitoreo y evaluación para evaluar la efectividad de la aplicación del Convenio de Budapest por parte de los jueces peruanos? Ejemplifique

   ……
   ……

6. ¿Cómo se considera la teoría de la pena en la legislación peruana para los delitos informáticos en aplicación a través del convenio de Budapest?

   ……
   ……

7. ¿La identificación de los enfoques jurídicos a través del convenio de Budapest permite al fiscal realizar requerimientos exitosos y salvaguardar la integridad de datos y sistemas informáticos?

   ……
   ……

8. ¿Cuáles son los enfoques jurídicos utilizados por los jueces y fiscales para realizar requerimientos vinculados a delitos informáticos en aplicación del convenio de Budapest en la legislación?

……
……

Categoría 2. Delitos informáticos

9. ¿Considera que la violación de seguridad de red es un procedimiento común en el país? ¿Por que?

……
……

10. ¿Cuáles son los casos de ciberdelincuencia más comunes que se han reportado en el Perú?

……
……

11. ¿Cuáles son los aspectos criminológicos de la ciberdelincuencia más utilizada en el país?

……
……

12. Teniendo en cuenta la Ley N° 30171 ¿Qué otras acciones y recursos legales existen en el Perú para combatir la ciberdelincuencia y proteger a las víctimas?

    ……
    ……

13. ¿Qué es y cuáles son las técnicas de hacking en el delito informático utilizados por los delincuentes en el Perú??

……
……

Anexo 4: Matriz de evaluación por juicio de expertos

Nº	ÍTEMS	Claridad[1]				Coherencia[2]				Relevancia[3]				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
	Categoría: Convenio Budapest													
01	Desde su experiencia profesional ¿Considera que la aplicación del convenio de Budapest ha aportado sustancialmente a la legislación peruana? ¿Por qué?			X					X				X	
02	¿En qué medida los jueces peruanos utilizan el convenio de Budapest como marco legal para abordar casos de delitos informáticos?			X					X				X	
03	Teniendo en cuenta la ratificación del convenio regulado en la legislación en la Ley N.°30171 ¿Cuáles son los principales desafíos o dificultades que enfrentan los jueces y fiscales al aplicar el convenio de Budapest en la legislación nacional?			X					X				X	
04	¿De qué manera el juez realiza la función de la sanción penal o pena tiene asignada sobre la base de la aplicación del convenio?			X					X				X	
05	¿Se han establecido mecanismos de monitoreo y evaluación para evaluar la efectividad de la aplicación del Convenio de Budapest por parte de los jueces peruanos? Ejemplifique			X					X				X	
06	¿Cómo se considera la teoría de la pena en la legislación peruana para los delitos informáticos en aplicación a través del convenio de Budapest?			X					X				X	
07	¿La identificación de los enfoques jurídicos a través del convenio de Budapest permite al fiscal realizar requerimientos exitosos y salvaguardar la integridad de datos y sistemas informáticos?			**X**					X				**X**	
08	¿Cuáles son los enfoques jurídicos utilizados por los jueces y fiscales para realizar requerimientos vinculados a delitos informáticos en aplicación del convenio de Budapest en la legislación?				X				X				X	
Nº	**Categoría: Delitos informáticos**													
01	¿Considera que la violación de seguridad de red es un procedimiento común en el país? ¿Por qué?			X					X				X	
02	¿Cuáles son los casos de ciberdelincuencia más comunes que se han reportado en el Perú?				X				X				X	
03	¿Cuáles son los aspectos criminológicos de la ciberdelincuencia más utilizada en el país?			X					X				X	

04	Teniendo en cuenta la Ley N° 30171 ¿Qué otras acciones y recursos legales existen en el Perú para combatir la ciberdelincuencia y proteger a las víctimas?			X					X				X	
05	¿Qué es y cuáles son las técnicas de hacking en el delito informático utilizados por los delincuentes en el Perú?			X					X				X	
06	¿Considera que el delito de fraude, cometido completa o parcialmente en línea, es suficiente para cubrir otras conductas como el hurto, la estafa, los delitos financieros y delitos relacionados con los medios de pago electrónico? ¿Por qué?			X					X				X	

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1. No cumple con el criterio	2. Bajo nivel	3. Moderado nivel	4. Alto nivel

Observaciones (precisar si hay suficiencia). Si, considero que los ítems son suficientes.

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador: Barbarán Mozo Hipólito Percy **DNI:** 01100672

Especialidad del validador (a): Docente de Investigación / Profesor de Matemática /Posgrado en gestión, docencia educativa y Ciencias de la Educación

[1]**Claridad:** El ítem se comprende fácilmente, es decir, su sintáctica y semántica sonadecuadas.

[2]**Coherencia: El ítem tiene relación lógica con la dimensión o indicador que está midiendo**

[3]**Relevancia:** El ítem es esencial o importante, es decir debe ser incluido.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Moyobamba, 07 de junio de 2023

MATRIZ DE EVALUACIÓN POR JUICIO DE EXPERTOS

Nº	ÍTEMS	Claridad[1]				Coherencia[2]				Relevancia[3]				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
	Categoría: Convenio Budapest													
01	Desde su experiencia profesional ¿Considera que la aplicación del convenio de Budapest ha aportado sustancialmente a la legislación peruana? ¿Por qué?				X				X				X	
02	¿En qué medida los jueces peruanos utilizan el convenio de Budapest como marco legal para abordar casos de delitos informáticos?				X				X				X	
03	Teniendo en cuenta la ratificación del convenio regulado en la legislación en la Ley N.°30171 ¿Cuáles son los principales desafíos o dificultades que enfrentan los jueces y fiscales al aplicar el convenio de Budapest en la legislación nacional?				X				X				X	
04	¿De qué manera el juez realiza la función de la sanción penal o pena tiene asignada sobre la base de la aplicación del convenio?				X				X				X	
05	¿Se han establecido mecanismos de monitoreo y evaluación para evaluar la efectividad de la aplicación del Convenio de Budapest por parte de los jueces peruanos? Ejemplifique				X				X				X	
06	¿Cómo se considera la teoría de la pena en la legislación peruana para los delitos informáticos en aplicación a través del convenio de Budapest?				X				X				X	
07	¿La identificación de los enfoques jurídicos a través del convenio de Budapest permite al fiscal realizar requerimientos exitosos y salvaguardar la integridad de datos y sistemas informáticos?				X				X				**X**	
08	¿Cuáles son los enfoques jurídicos utilizados por los jueces y fiscales para realizar requerimientos vinculados a delitos informáticos en aplicación del convenio de Budapest en la legislación?				X				X				X	
Nº	**Categoría: Delitos informáticos**													
01	¿Considera que la violación de seguridad de red es un procedimiento común en el país? ¿Por qué?				X				X				X	
02	¿Cuáles son los casos de ciberdelincuencia más comunes que se han reportado en el Perú?				X				X				X	
03	¿Cuáles son los aspectos criminológicos de la ciberdelincuencia más utilizada en el país?				X				X				X	

04	Teniendo en cuenta la Ley N° 30171 ¿Qué otras acciones y recursos legales existen en el Perú para combatir la ciberdelincuencia y proteger a las víctimas?				X				X				X	
05	¿Qué es y cuáles son las técnicas de hacking en el delito informático utilizados por los delincuentes en el Perú?				X				X				X	
06	¿Considera que el delito de fraude, cometido completa o parcialmente en línea, es suficiente para cubrir otras conductas como el hurto, la estafa, los delitos financieros y delitos relacionados con los medios de pago electrónico? ¿Por qué?				X				X				X	

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1. No cumple con el criterio	2. Bajo nivel	3. Moderado nivel	4. Alto nivel

Observaciones (precisar si hay suficiencia). Si, considero que los ítems son suficientes.

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador: Mgtr. Ivo M. Encomenderos Bancallán **DNI:** 17623582

Especialidad del validador (a): Economista, Magister en docente universitaria, Docente de investigación

[1]**Claridad:** El ítem se comprende fácilmente, es decir, su sintáctica y semántica sonadecuadas.

[2]**Coherencia: El ítem tiene relación lógica con la dimensión o indicador que está midiendo**

[3]**Relevancia:** El ítem es esencial o importante, es decir debe ser incluido.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Moyobamba, 07 de junio de 2023

MATRIZ DE EVALUACIÓN POR JUICIO DE EXPERTOS

Nº	ÍTEMS	Claridad[1]				Coherencia[2]				Relevancia[3]				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
	Categoría: Convenio Budapest													
01	Desde su experiencia profesional ¿Considera que la aplicación del convenio de Budapest ha aportado sustancialmente a la legislación peruana? ¿Por qué?			X					X				X	
02	¿En qué medida los jueces peruanos utilizan el convenio de Budapest como marco legal para abordar casos de delitos informáticos?			X					X				X	
03	Teniendo en cuenta la ratificación del convenio regulado en la legislación en la Ley N.°30171 ¿Cuáles son los principales desafíos o dificultades que enfrentan los jueces y fiscales al aplicar el convenio de Budapest en la legislación nacional?			X					X				X	
04	¿De qué manera el juez realiza la función de la sanción penal o pena tiene asignada sobre la base de la aplicación del convenio?			X					X				X	
05	¿Se han establecido mecanismos de monitoreo y evaluación para evaluar la efectividad de la aplicación del Convenio de Budapest por parte de los jueces peruanos? Ejemplifique			X					X				X	
06	¿Cómo se considera la teoría de la pena en la legislación peruana para los delitos informáticos en aplicación a través del convenio de Budapest?			X					X				X	
07	¿La identificación de los enfoques jurídicos a través del convenio de Budapest permite al fiscal realizar requerimientos exitosos y salvaguardar la integridad de datos y sistemas informáticos?			**X**					X				**X**	
08	¿Cuáles son los enfoques jurídicos utilizados por los jueces y fiscales para realizar requerimientos vinculados a delitos informáticos en aplicación del convenio de Budapest en la legislación?			X					X				X	
Nº	**Categoría: Delitos informáticos**													
01	¿Considera que la violación de seguridad de red es un procedimiento común en el país? ¿Por qué?			X					X				X	
02	¿Cuáles son los casos de ciberdelincuencia más comunes que se han reportado en el Perú?			X					X				X	
03	¿Cuáles son los aspectos criminológicos de la ciberdelincuencia más utilizada en el país?			X					X				X	

04	Teniendo en cuenta la Ley N° 30171 ¿Qué otras acciones y recursos legales existen en el Perú para combatir la ciberdelincuencia y proteger a las víctimas?			X					X				X	
05	¿Qué es y cuáles son las técnicas de hacking en el delito informático utilizados por los delincuentes en el Perú?			X					X				X	
06	¿Considera que el delito de fraude, cometido completa o parcialmente en línea, es suficiente para cubrir otras conductas como el hurto, la estafa, los delitos financieros y delitos relacionados con los medios de pago electrónico? ¿Por qué?			X					X				X	

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1. No cumple con el criterio	2. Bajo nivel	3. Moderado nivel	4. Alto nivel

Observaciones (precisar si hay suficiencia). Si, considero que los ítems son suficientes.

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador: Santa Cruz Coronel Raúl **DNI:** 43123997

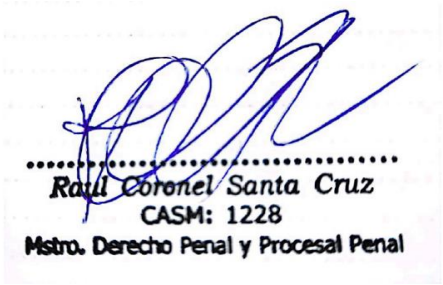
Especialidad del validador (a): Maestro en Derecho Penal y Procesal Penal, docente universitario, doctorando en Derecho

[1]**Claridad:** El ítem se comprende fácilmente, es decir, su sintáctica y semántica sonadecuadas.

[2]**Coherencia: El ítem tiene relación lógica con la dimensión o indicador que está midiendo**

[3]**Relevancia:** El ítem es esencial o importante, es decir debe ser incluido.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión



Moyobamba, 08 de junio de 2023

MATRIZ DE EVALUACIÓN POR JUICIO DE EXPERTOS

Nº	ÍTEMS	Claridad[1]				Coherencia[2]				Relevancia[3]				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
	Categoría: Convenio Budapest													
01	Desde su experiencia profesional ¿Considera que la aplicación del convenio de Budapest ha aportado sustancialmente a la legislación peruana? ¿Por qué?				X				X				X	
02	¿En qué medida los jueces peruanos utilizan el convenio de Budapest como marco legal para abordar casos de delitos informáticos?				X				X				X	
03	Teniendo en cuenta la ratificación del convenio regulado en la legislación en la Ley N.°30171 ¿Cuáles son los principales desafíos o dificultades que enfrentan los jueces y fiscales al aplicar el convenio de Budapest en la legislación nacional?				X				X				X	
04	¿De qué manera el juez realiza la función de la sanción penal o pena tiene asignada sobre la base de la aplicación del convenio?				X				X				X	
05	¿Se han establecido mecanismos de monitoreo y evaluación para evaluar la efectividad de la aplicación del Convenio de Budapest por parte de los jueces peruanos? Ejemplifique				X				X				X	
06	¿Cómo se considera la teoría de la pena en la legislación peruana para los delitos informáticos en aplicación a través del convenio de Budapest?				X				X				X	
07	¿La identificación de los enfoques jurídicos a través del convenio de Budapest permite al fiscal realizar requerimientos exitosos y salvaguardar la integridad de datos y sistemas informáticos?				X				X				**X**	
08	¿Cuáles son los enfoques jurídicos utilizados por los jueces y fiscales para realizar requerimientos vinculados a delitos informáticos en aplicación del convenio de Budapest en la legislación?				X				X				X	
Nº	**Categoría: Delitos informáticos**													
01	¿Considera que la violación de seguridad de red es un procedimiento común en el país? ¿Por qué?				X				X				X	
02	¿Cuáles son los casos de ciberdelincuencia más comunes que se han reportado en el Perú?				X				X				X	
03	¿Cuáles son los aspectos criminológicos de la ciberdelincuencia más utilizada en el país?				X				X				X	

04	Teniendo en cuenta la Ley N° 30171 ¿Qué otras acciones y recursos legales existen en el Perú para combatir la ciberdelincuencia y proteger a las víctimas?				X				X				X	
05	¿Qué es y cuáles son las técnicas de hacking en el delito informático utilizados por los delincuentes en el Perú?				X				X				X	
06	¿Considera que el delito de fraude, cometido completa o parcialmente en línea, es suficiente para cubrir otras conductas como el hurto, la estafa, los delitos financieros y delitos relacionados con los medios de pago electrónico? ¿Por qué?				X				X				X	

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1. No cumple con el criterio	2. Bajo nivel	3. Moderado nivel	4. Alto nivel

Observaciones (precisar si hay suficiencia). Si, considero que los ítems son suficientes.

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador: Mas Guivin Juan Carlos **DNI:** 43525796

Especialidad del validador (a): Maestro en Derecho Penal y Procesal Penal, investigador, docente universitario, doctorando en Derecho

[1]**Claridad:** El ítem se comprende fácilmente, es decir, su sintáctica y semántica sonadecuadas.

[2]**Coherencia: El ítem tiene relación lógica con la dimensión o indicador que está midiendo**

[3]**Relevancia:** El ítem es esencial o importante, es decir debe ser incluido.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Moyobamba, 08 de junio de 2023

MATRIZ DE EVALUACIÓN POR JUICIO DE EXPERTOS

Nº	ÍTEMS	Claridad[1]				Coherencia[2]				Relevancia[3]				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
	Categoría: Convenio Budapest													
01	Desde su experiencia profesional ¿Considera que la aplicación del convenio de Budapest ha aportado sustancialmente a la legislación peruana? ¿Por qué?				X			X					X	
02	¿En qué medida los jueces peruanos utilizan el convenio de Budapest como marco legal para abordar casos de delitos informáticos?				X			X					X	
03	Teniendo en cuenta la ratificación del convenio regulado en la legislación en la Ley N.°30171 ¿Cuáles son los principales desafíos o dificultades que enfrentan los jueces y fiscales al aplicar el convenio de Budapest en la legislación nacional?				X			X					X	
04	¿De qué manera el juez realiza la función de la sanción penal o pena tiene asignada sobre la base de la aplicación del convenio?				X			X					X	
05	¿Se han establecido mecanismos de monitoreo y evaluación para evaluar la efectividad de la aplicación del Convenio de Budapest por parte de los jueces peruanos? Ejemplifique				X			X					X	
06	¿Cómo se considera la teoría de la pena en la legislación peruana para los delitos informáticos en aplicación a través del convenio de Budapest?				X			X					X	
07	¿La identificación de los enfoques jurídicos a través del convenio de Budapest permite al fiscal realizar requerimientos exitosos y salvaguardar la integridad de datos y sistemas informáticos?				X			X					X	
08	¿Cuáles son los enfoques jurídicos utilizados por los jueces y fiscales para realizar requerimientos vinculados a delitos informáticos en aplicación del convenio de Budapest en la legislación?				X			X					X	
Nº	**Categoría: Delitos informáticos**													
01	¿Considera que la violación de seguridad de red es un procedimiento común en el país? ¿Por qué?				X			X					X	
02	¿Cuáles son los casos de ciberdelincuencia más comunes que se han reportado en el Perú?				X			X					X	
03	¿Cuáles son los aspectos criminológicos de la ciberdelincuencia más utilizada en el país?				X			X					X	

04	Teniendo en cuenta la Ley N° 30171 ¿Qué otras acciones y recursos legales existen en el Perú para combatir la ciberdelincuencia y proteger a las víctimas?				X			X					X	
05	¿Qué es y cuáles son las técnicas de hacking en el delito informático utilizados por los delincuentes en el Perú?				X			X					X	
06	¿Considera que el delito de fraude, cometido completa o parcialmente en línea, es suficiente para cubrir otras conductas como el hurto, la estafa, los delitos financieros y delitos relacionados con los medios de pago electrónico? ¿Por qué?				X			X					X	

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1. No cumple con el criterio	2. Bajo nivel	3. Moderado nivel	4. Alto nivel

Observaciones (precisar si hay suficiencia). Si, considero que los ítems son suficientes.

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador: Bellido Navarro Milagros **DNI:** 45919072

Especialidad del validador (a): Maestro en Derecho Penal y Procesal Penal, docente universitario

[1]**Claridad:** El ítem se comprende fácilmente, es decir, su sintáctica y semántica sonadecuadas.

[2]**Coherencia: El ítem tiene relación lógica con la dimensión o indicador que está midiendo**

[3]**Relevancia:** El ítem es esencial o importante, es decir debe ser incluido.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Moyobamba, 08 de junio de 2023

Anexo 5: Validez de Aiken de 5 expertos

CATEGORÍA 1:		Convenio Budapest													
		CLARIDAD					COHERENCIA					RELEVANCIA			
		J1	J2	J3	J4	J5	J1	J2	J3	J4	J5	J1	J2	J3	J4	J5
SC1 Principio de legalidad	P1	3	4	3	4	4	4	4	4	4	3	4	4	4	4	4
	P2	3	4	3	4	4	4	4	4	4	3	4	4	4	4	4
	P3	3	4	3	4	4	4	4	4	4	3	4	4	4	4	4
SC2 Teoría de la pena	P4	3	4	3	4	4	4	4	4	4	3	4	4	4	4	4
	P5	3	4	3	4	4	4	4	4	4	3	4	4	4	4	4
	P6	3	4	3	4	4	4	4	4	4	3	4	4	4	4	4
SC3 Enfoque jurídico	P7	3	4	3	4	4	4	4	4	4	3	4	4	4	4	4
	P8	4	4	3	4	4	4	4	4	4	3	4	4	4	4	4

V de Ayken	0.94

Validez de Aiken de 5 expertos

CATEGORÍA 2:		Delitos informáticos														
		CLARIDAD					COHERENCIA					RELEVANCIA				
		J1	J2	J3	J4	J5	J1	J2	J3	J4	J5	J1	J2	J3	J4	J5
SC1: Violación de seguridad de la red	P1	3	4	3	4	4	4	4	4	4	3	4	4	4	4	4
	P2	4	4	3	4	4	4	4	3	4	3	4	4	3	4	4
SC2: Aspectos tecnológicos	P3	3	4	3	4	4	4	4	4	4	3	4	4	4	4	4
	P4	3	4	3	4	4	4	4	4	4	3	4	4	4	4	4
SC3: Fraude informático	P5	3	4	3	4	4	4	4	4	4	3	4	4	4	4	4
	P6	3	4	3	4	4	4	4	4	4	3	4	4	4	4	4

V de Ayken	0.93

Anexo 06: consentimiento informado

Título de la investigación: Aplicación del convenio de Budapest y delitos informáticos en el Perú en el 2022.
Investigador (a): Ocupa Sánchez, Bammy Sharum.

Propósito del estudio

Le invitamos a participar en una investigación titulada “Aplicación del convenio de Budapest y delitos informáticos en el Perú en el 2022”, cuyo objetivo de la investigación es analizar de qué manera el Estado peruano aplica el convenio de Budapest para sancionar delitos informáticos en el año 2022. Esta investigación es desarrollada por estudiantes de posgrado de la maestría en Derecho Penal y Procesal Penal de la Universidad César Vallejo del campus San Martín y filial Tarapoto, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la institución.

Problema: El Perú no es ajeno al problema de la delincuencia; la vorágine salvaje del ingente crecimiento de la tecnología, la falta de legislación necesaria para afrontar la ciberdelincuencia. Es por ello que, se necesita soluciones a esta grave problemática que nos acecha a diario, excluyéndonos del buen recaudo inclusive en el seno de nuestros hogares. El Convenio de Budapest, ha traído aparentemente la solución a la problemática, debido a que resultaba atractivo una cooperación supranacional para la lucha contra este tipo de delincuencia, la legislación adecuada para prevenir y sancionar estas conductas, la mejoría en las técnicas e instrumentos investigativos que coadyuven a la prevención y sanción de las conductas típicas, y en cierta parte, como punto de partida, lo es. No obstante, la positivización no suele ser el punto final de los problemas que aquejan a una población, debido a que, no basta con reconocer el problema y darles tratativas teóricas.

Procedimiento

Si usted decide participar en la investigación se realizará los siguientes procedimientos:

1. Se realizará una entrevista donde se recogerán datos personales y algunas preguntas sobre la investigación titulada: “Aplicación del convenio de Budapest y delitos informáticos en el Perú en el 2022”.
2. Esta entrevista será remitida por el estudiante a través de su correo institucional de la Universidad César Vallejo a los correos electrónicos de cada participante – entrevistado con la finalidad de obtener las evidencias correspondientes.
3. Las respuestas de la guía de entrevista serán codificadas usando un número de identificación y, por lo tanto, serán anónimas.

* Obligatorio a partir de los 18 años

Participación voluntaria (principio de autonomía):

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 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 algún beneficio económico ni de ninguna otra índole. El estudio no va 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):

Los datos recolectados deben ser anónimos y no tener ninguna forma de identificar al participante. 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 Ocupa Sánchez, Bammy Sharum; email: bocupas@ucvvirtual.edu.pe y Docente Asesor Palomino Alvarado Gabriela del Pilar; email: dpalominoal@ucvvirtual.edu.pe.

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

Nombre y apellidos: Danny Miguel Talavera Argomedo

Fecha y hora: 28/06/2022 ,15:00

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

ACTA DE SUSTENTACION DE TESIS

TARAPOTO, 04 de Julio del 2023

Siendo las 16:05 horas del 31/07/2023, el jurado evaluador se reunió para presenciar el acto de sustentación de Tesis titulada: "Aplicación del convenio Budapest y delitos informáticos en el Perú, 2022", presentado por el autor OCUPA SÁNCHEZ BAMMY SHARUM egresado MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL.

Concluido el acto de exposición y defensa de Tesis, el jurado luego de la deliberación sobre la sustentación, dictaminó:

Autor	Dictamen
BAMMY SHARUM OCUPA SÁNCHEZ	(16)Cum Laude

Se firma la presente para dejar constancia de lo mencionado

Firmado electrónicamente por:
CCHANAMECA el 31 Jul 2023 16:23:44

CESAR AUGUSTO CHAMBERGO CHANAME
PRESIDENTE

Firmado electrónicamente por: SALASVNA
el 31 Jul 2023 16:23:27

NAPOLEON ARMSTRONG SALAS VELASQUEZ
SECRETARIO

Firmado electrónicamente por:
DPALOMINOAL el 31 Jul 2023 16:24:00

GABRIELA DEL PILAR PALOMINO ALVARADO
VOCAL(ASESOR)

Código documento Trilce: TRI - 0571033

* Para Pre y posgrado los rangos de dictamen se establecen en el Reglamento de trabajos conducentes a grados y títulos

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Autorización de Publicación en Repositorio Institucional

Yo, OCUPA SÁNCHEZ BAMMY SHARUM identificado con N° de Documento N° 71883708 (respectivamente), estudiante de la ESCUELA DE POSGRADO y MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL de la UNIVERSIDAD CÉSAR VALLEJO SAC - TARAPOTO, autorizo (X), no autorizo ( ) la divulgación y comunicación pública de mi Tesis: "Aplicación del convenio Budapest y delitos informáticos en el Perú, 2022".

En el Repositorio Institucional de la Universidad César Vallejo, según esta estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art. 23 y Art. 33.

Fundamentación en caso de NO autorización:

TARAPOTO, 18 de Julio del 2023

Apellidos y Nombres del Autor	Firma
OCUPA SÁNCHEZ BAMMY SHARUM **DNI:** 71883708 **ORCID:** 0000-0002-1067-512X	Firmado electrónicamente por: BOCUPAS el 18-07-2023 15:06:41

Código documento Trilce: TRI - 0600525

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Declaratoria de Autenticidad de los Asesores

Nosotros, PALOMINO ALVARADO GABRIELA DEL PILAR, docente de la ESCUELA DE POSGRADO MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL de la UNIVERSIDAD CÉSAR VALLEJO SAC - TARAPOTO, asesores de Tesis titulada: "Aplicación del convenio Budapest y delitos informáticos en el Perú, 2022", cuyo autor es OCUPA SÁNCHEZ BAMMY SHARUM, constato que la investigación tiene un índice de similitud de 16.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

Hemos 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, asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual nos sometemos a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

TARAPOTO, 04 de Agosto del 2023

Apellidos y Nombres del Asesor:	**Firma**
PALOMINO ALVARADO GABRIELA DEL PILAR **DNI:** 00953069 **ORCID:** 0000-0002-2126-2769	Firmado electrónicamente por: DPALOMINOAL el 05-08-2023 17:23:53
SALAS VELASQUEZ NAPOLEON ARMSTRONG **DNI:** 01311595 **ORCID:** 0000-0002-6784-8335	Firmado electrónicamente por: SALASVNA el 05-08-2023 22:20:46

Código documento Trilce: TRI - 0641408

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Declaratoria de Originalidad del Autor

Yo, OCUPA SÁNCHEZ BAMMY SHARUM estudiante de la ESCUELA DE POSGRADO MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL de la UNIVERSIDAD CÉSAR VALLEJO SAC - TARAPOTO, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Aplicación del convenio Budapest y delitos informáticos en el Perú, 2022", 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**
BAMMY SHARUM OCUPA SÁNCHEZ **DNI:** 71883708 **ORCID:** 0000-0002-1067-512X	Firmado electrónicamente por: BOCUPAS el 04-07-2023 13:39:55

Código documento Trilce: TRI - 0571035

INVESTIGA UCV