UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa - 2022.

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Derecho Penal y Procesal Penal

AUTOR:

Acosta Zavaleta, Jean Carlos (orcid.org/0000-0002-5139-6143)

ASESORAS:

Mg. Moreno Nuñez, Patricia Janet (orcid.org/0000-0001-8801-8069)

Dra. Alva Díaz, Lyda Palmira (orcid.org/0000-0002-3230-2981)

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

CHIMBOTE – PERÚ

2024

DEDICATORIA

A mis amados padres y a mi querida familia,

Este trabajo de grado es el fruto de mucho tiempo de esfuerzo, sacrificio y amor incondicional que me han brindado. A ustedes, mis padres, les debo la persona que soy hoy y cada logro que he alcanzado. Cada regla, valor y buena costumbre que me han inculcado ha sido mi brújula en este viaje académico y personal.

Gracias por ser mi fuente de inspiración constante, por motivarme a alcanzar mis anhelos y por ser los pilares inquebrantables que me han sostenido en cada desafío. Este logro es tanto suyo como mío, y dedico este trabajo a la familia que siempre ha creído en mí.

Jean Carlos Acosta Zavaleta

AGRADECIMIENTO

Agradezco de todo corazón a Dios, quien me ha bendecido con una familia maravillosa. Su apoyo incondicional, creencia constante en mí y ejemplos de superación, humildad y sacrificio han sido la luz que ilumina mi camino. Me han enseñado a valorar cada aspecto de mi vida y han cultivado en mí el deseo innato de superación y éxito.

A mi familia, le dedico este logro significativo en mi vida profesional. Su influencia ha sido fundamental para alcanzar este hito, y espero seguir contando siempre con su valioso e incondicional apoyo en las etapas futuras.

Asimismo, expreso mi profundo agradecimiento a mis asesoras de tesis. Su paciencia, orientación y enseñanzas ha sido fundamental en el desarrollo de este trabajo. Gracias por su dedicación y por compartir su sabiduría, contribuyendo de manera excepcional a mi crecimiento académico y profesional. Con gratitud sincera.

Jean Carlos Acosta Zavaleta

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Declaratoria de Autenticidad de los Asesores

Nosotros, ALVA DIAZ LYDA PALMIRA , MORENO NUÑEZ PATRICIA JANET, docente de la ESCUELA DE POSGRADO MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL de la UNIVERSIDAD CÉSAR VALLEJO SAC - CHIMBOTE, asesores de Tesis titulada: "Efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa - 2022.", cuyo autor es ACOSTA ZAVALETA JEAN CARLOS, constato que la investigación tiene un índice de similitud de 6.00%, 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.

CHIMBOTE, 17 de Enero del 2024

Apellidos y Nombres del Asesor:	**Firma**
ALVA DIAZ LYDA PALMIRA **DNI:** 06240404 **ORCID:** 0000-0002-3230-2981	Firmado electrónicamente por: ADIAZLP el 18-01-2024 17:41:55
MORENO NUÑEZ PATRICIA JANET **DNI:** 18099921 **ORCID:** 0000-0001-8801-8069	Firmado electrónicamente por: PMORENONU el 24-01-2024 23:43:55

Código documento Trilce: TRI - 0734101

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Declaratoria de Originalidad del Autor

Yo, ACOSTA ZAVALETA JEAN CARLOS estudiante de la ESCUELA DE POSGRADO del programa de MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL de la UNIVERSIDAD CÉSAR VALLEJO SAC - CHIMBOTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa - 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
ACOSTA ZAVALETA JEAN CARLOS **DNI:** 45230793 **ORCID:** 0000-0002-5139-6143	Firmado electrónicamente por: JACOSTAZ el 06-02-2024 20:03:05

Código documento Trilce: INV - 1473232

INVESTIGA UCV

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

RESUMEN

La investigación tuvo como objetivo general determinar los efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022. Se realizó una investigación básica, de diseño cualitativo no experimental, se contó con 10 participantes entre jueces y fiscales, asimismo se revisaron 12 carpetas fiscales. Se empleó la entrevista como técnica y la revisión documental, como instrumentos se emplearon la guia de entrevista y la guia de observación documental respectivamente. Respecto a los hallazgos, los participantes reconocieron la influencia de la normativa internacional del Convenio de Budapest, pero enfatizaron la necesidad de mejorar la tipificación del delito para una implementación más efectiva. Asimismo se logró determinar que la falta de legislación adecuada impactó negativamente en la detección, investigación y sanción del delito de estafa cibernética en el distrito, con menor capacidad para prevenir, detectar e investigar, resultando en acusaciones limitadas y condenas desproporcionadas. Se observó un mayor riesgo de impunidad y menor protección a las víctimas, mientras que la legislación ambigua dificultó el trabajo de fiscales y jueces. Es necesario adaptar y fortalecer la legislación, proteger a las víctimas y facilitar la cooperación transfronteriza en la persecución del delito de estafa cibernética en el distrito.

Palabras clave: Ciberdelitos, delito, estafa cibernética, persecución penal.

ABSTRACT

The research aimed to determine the effects of insufficient prosecutorial legislation on cyber fraud in the Santa judicial district in 2022. A basic, non-experimental qualitative study was conducted with 10 participants, including judges and prosecutors. Additionally, 12 legal files were reviewed. The interview was employed as a technique, and documentary review was utilized. The interview guide and the documentary observation guide were the respective instruments used. Regarding the findings, participants acknowledged the influence of the international Budapest Convention but emphasized the need to improve the criminal classification of the offense for more effective implementation. It was also determined that the lack of adequate legislation had a negative impact on the detection, investigation, and punishment of cyber fraud in the district. There was a reduced capacity to prevent, detect, and investigate, resulting in limited charges and disproportionate convictions. A higher risk of impunity and reduced protection for victims was observed, while ambiguous legislation complicated the work of prosecutors and judges. Hence, it was suggested to adapt and strengthen the legislation to achieve effective deterrence, protect victims, and facilitate cross-border cooperation in the prosecution of cyber fraud in the district.

Keywords: Cybercrimes, crime, cyber fraud, criminal prosecution.

I. INTRODUCCIÓN

En la actualidad, nuestra sociedad se halla inmersa en un entorno donde el tejido cotidiano de las actividades humanas se encuentra irrevocablemente entrelazado con las redes digitales y el vasto ciberespacio. La era de la globalización ha actuado como catalizador de esta transformación, cuyos efectos se han vuelto aún más evidentes durante la pandemia. En este período sin precedentes, las Tecnologías de la Información y la Comunicación (TIC) han emergido como la columna vertebral que sustenta las interacciones humanas, desde la esfera personal hasta la empresarial (Vilchez, 2020)

Hoy en día internet se ha transformado en un medio altamente utilizado para llevar a cabo actividades personales, así como para cometer un hecho delictivo, lo que afecta los derechos de las personas (Casado, 2017). Si bien las ventajas de las TIC´s no puede negarse, tampoco puede obviarse el hecho de que el internet ha reforzado la ciberdelincuencia, y con ello los agravios que se cometen contra individuos o entidades empresariales, quienes llevan a cabo, a través del internet, la comercialización de un bien o servicio; situación que se ha agravado aún más en razón al desconocimiento en torno al manejar y resguardar los datos de índole personal.

Montes (2022) señala que según los reportes del FBI entre el 2020 y 2021, Reino Unido es de los países que mayor cantidad de ciberdelitos ha reportado (4.783 víctimas); EE.UU. se sitúa en segundo lugar con 1.494 víctimas, aun su índice disminuyó al 13% si se compara con las cifras del 2020 y finalmente el tercer país es Canadá, con 174 que advierte un 7% más que antes; y en Latinoamérica, Ecuador ha sido el país que ha enfrentado más ataques cibernéticos hasta agosto del año 2021. (DPL News, 2022)

Considerando lo acotado líneas antes, podemos inferir que, a través del comercio electrónico, puntualmente el comerciar mediante redes sociales, han facilitado y ayudado a desarrollarse todo tipo de actividades comerciales, tanto para quien consume como para quien provee; sin embargo, ello de alguna manera

también ha ocasionado que se vean repotenciadas las actividades delictivas, pues los estafadores han encontrado plataformas que les facilita la comisión del ilícito (González, 2020). Ejemplo de ello son los casos divulgados por la fiscalía de Colombia, como el caso de "@shoppingcolombia.com.co", en donde se estafaron a muchas personas con la compra online de productos electrónicos de marcas con gran popularidad y reconocimiento, pero a un menor precio (Durán, 2023)

El Perú no se encuentra exento de esta problemática mundial, razón por la que la cibercriminalidad fue tipificada en la legislación desde 1991 en el CP; no obstante, es hasta el 2000 que se incorpora al ordenamiento legal la Ley N° 27309, a través de la que se estableció en el cuerpo normativo penal a los delitos informáticos como parte de los que se cometen en afectación del patrimonio; la misma que estuvo vigente por 13 años, pues en octubre del 2013 se emitió la Ley N° 30096 (que se modificó a través de la Ley N° 30171, y por la Ley N° 30838) para regular y sancionar la ciberdelincuencia (Ávalos, 2022). Además, aunque la PNP fue el primero en dar una respuesta especializada en torno a la ciberdelincuencia; siendo que en 2005 pudo ser creada la DIVINDAT–PNP dentro de la DIRINCRI– PNP (Ministerio del Interior, 2016); las denuncias por ciberdelincuencia recepcionados en la PNP se cuadruplicaron entre 2018 y 2021, resaltando el fraude informático y la suplantación de la identidad, siendo La Libertad una de las regiones con mayores índices (El Peruano, 2022).

El comercio electrónico peruano, en el año 2020 tuvo un crecimiento del 50% con respecto al año anterior, según la CAPECE, debido a las restricciones de la pandemia; y, aun cuando esta clase de comercio es de suma importancia para elevar la venta de productos o el ofrecimiento de servicios; de un modo u otro facilita la comisión de fraudes o estafas a través de medios electrónicos (El Comercio, 2022). Según la ASBANC, durante el primer año de pandemia se pudo registrar un 38 % de robos digitales a tarjetas de crédito y débito, sustrayéndose más de 6 millones de soles a causa de las estafas online (Gómez, 2021).

Asimismo, la estafa cobro notable protagonismo, por ello se pudo identificas las 5 estafas más usadas en Perú en 2022: Una estafadora de Tinder se hacía pasar

por profesional para robar a hombres; un ex policía montó una estafa piramidal en Puno y huyó con el dinero de 7,000 personas; Pamela Cabanillas vendía entradas falsas usando códigos QR y escapó a España; una modalidad de estafa ofrecía trabajos atractivos pero desaparecía con el dinero después de pedir pagos por certificados y cursos; 'Sonia' prometió enviar una maleta con objetos valiosos desde Singapur, pidió dinero para gastos locales y el envío nunca llegó. (El Comercio, 2022).

A pesar de la alta incidencia de estafas, son pocos quienes presentan denuncias. Factores como la cuantía, la novedad del delito, la desinformación o la vergüenza influyen en la baja tasa de denuncias. Según la Defensoría del Pueblo (2023) la tasa de ciberdelitos por cada 100,000 habitantes que aumentó del 10% al 39%.

En este contexto, a pesar de que varios países han promulgado legislaciones basadas en acuerdos e instrumentos internacionales para hacer frente a la ciberdelincuencia, como el "Convenio de Budapest" (Alonso y Esparza, 2017), al cual el Perú se ha adherido, la realidad del distrito judicial del Santa no difiere de lo que se observa a nivel nacional. Durante la pandemia, en nuestra ciudad intensificaron su participación en el comercio electrónico, lo que brindó oportunidades a los estafadores. Estos delincuentes, aprovechando su pericia en el ámbito digital, el anonimato y la clandestinidad del ciberespacio, llevaron a cabo actividades ilícitas empleando diversos medios electrónicos

Ante dicha realidad, la persecución penal de estos delitos, se torna sustancial, dada a la gravedad de estos (Usaqui, 2021), así como entender su funcionamiento a nivel legal es imperativo; aun cuando se vislumbran falencias, vacíos legales y tecnológicos que no permite llegar a encarcelar a estos delincuentes, es así que la Interpol (2020) advierte que es sumamente probable que siga en aumento la ciberdelincuencia, pues los delincuentes amplían sus actividades y mejoran sus modus opernandi volviéndolos cada vez más avanzados y complejos, por ello como mencionan Mayer y Oliver (2020) se requiere regular los delitos cibernéticos en torno

a: verificar la conducta típica; segundo, la provocación de un resultado típico y, por último verificar el ánimo de lucro.

Teniendo en cuenta lo expresado antes, se plantea como problema de investigación: ¿Cuáles son los efectos de la insuficiente legislación persecutoria del delito de estafa cibernética del distrito fiscal del Santa, 2022?

El estudio posee una *(a) justificación teórica*, en razón a que se puede brindar conocimiento y teorías innovadoras en torno a las variables, lo que permitirá conocer como una variable influye en la otra, lo que es sustancial para la sociedad en general como la jurídica; asimismo, los hallazgos serán una fuente de conocimiento, a la que podrán recurrir quienes lleven a cabo estudios posteriores a éste; *(b) se justifica en lo metodológico,* ya que las variables se desarrollarán a través de parámetros de índole científico para contrastar la hipótesis planteada mediante un enfoque cualitativo; *(c) una justificación práctica,* en razón a que de acuerdo a los objetivos y el resultado que se obtendrán , se podrá podrán hallar respuestas a la problemática detectada; esto es, que ciberdelincuentes, aprovechando su conocimiento especializado, el anonimato y la clandestinidad del ciberespacio, han estafado mediante medios electrónicos a personas naturales o jurídicas, por lo los efectos de la insuficiente legislación de este delito, se torna sustancial, dada a la gravedad de estos, así como entender su funcionamiento a nivel legal es imperativo; aun cuando se vislumbran falencias, vacíos legales y tecnológicos que no permite llegar a encarcelar a estos delincuentes, pues es sumamente probable que siga en aumento, que los ciberdelincuentes amplían sus actividades y mejoran sus modus opernandi volviéndolos cada vez más avanzados y complejos; *(d) Tiene viabilidad*, en razón a que podrá accederse a todos aquellos que se requieran para desarrollar el estudio; y *(f) se justifica en lo social,* pues aborda la creciente amenaza de la estafa cibernética mediante la mejora de respuestas legales y legislativas. Se busca fortalecer la legislación, capacidades investigativas y concientización para proteger a las víctimas, disuadir a los perpetradores, y fomentar la colaboración entre instituciones y ciudadanos.

La investigación se orientará por un objetivo general, que será: Determinar los efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022; y por objetivos específicos: OE1. Determinar la aplicación de la normativa internacional en la legislación nacional persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022. OE2. Determinar las principales deficiencias de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022. OE3. Determinar los efectos de la insuficiente legislación persecutoria en la detección del delito de estafa cibernética en el distrito fiscal del Santa, 2022. OE4. Determinar los efectos de la insuficiente legislación persecutoria en la investigación del delito de estafa cibernética en el distrito fiscal del Santa, 2022; y OE5. Determinar los efectos de la insuficiente legislación persecutoria en la sanción del delito de estafa cibernética en el distrito fiscal del Santa, 2022.

II. MARCO TEÓRICO

Entre los referentes teóricos clave que sustentan la investigación se encuentra el estudio doctoral realizado por Quevedo (2017) quien analizó la influencia del Internet en el surgimiento de la cibercriminalidad en España. Mediante un enfoque explicativo, el autor determinó que la red ha tenido un impacto considerable en la evolución de los delitos informáticos. Por lo tanto, la persecución efectiva de este tipo de crímenes demanda un profundo entendimiento de las técnicas básicas relacionadas con las tecnologías de la información, dado que éstas facilitan la comisión de actividades ilegales en el entorno digital.

El artículo escrito por Sain (2018) se enfocó en examinar la estrategia gubernamental de Argentina para combatir el cibercrimen en el país. Utilizando un enfoque doctrinal, el autor identificó una serie de desafíos relacionados con la investigación de la cibercriminalidad, destacando la falta de comprensión y la fragilidad de las pruebas informáticas. Este aspecto se debe a que gran parte de los delitos cibernéticos ocurren en un entorno virtual que simula representaciones de objetos físicos.

El estudio de Domínguez y Vera (2022) evaluó la incidencia de la ciberdelincuencia en Tamaulipas, México, utilizando un enfoque descriptivo y exploratorio. Mediante el análisis de patrones de llamadas y la aplicación del coeficiente de localización, identificaron que Tamaulipas es vulnerable a delitos cibernéticos, especialmente relacionados con el robo de contraseñas en redes sociales. Concluyeron que es crucial implementar políticas públicas a nivel nacional y local para abordar eficazmente el crecimiento de la ciberdelincuencia en la región.

En la investigación de Arias (2021) sobre la cibercriminalidad en El Salvador, se identificaron limitaciones en la regulación de técnicas de investigación y evidencia digital por parte de la Ley Especial contra Delitos Informáticos y Conexos. Esta legislación se enfoca principalmente en establecer normas para las conductas constitutivas de ciberdelitos. Además, se observó que El Salvador está en proceso

de ratificación del Convenio de Budapest, sin planes definidos para suscribir acuerdos que aborden más eficazmente la problemática de la cibercriminalidad.

Ávalos (2021) destaca la necesidad de especialización en la lucha contra la cibercriminalidad a nivel nacional. En un enfoque teórico, la autora resalta la urgencia de capacitar a operadores judiciales, peritos y la Policía Nacional del Perú en temas de cibercriminalidad y el uso de tecnologías de la información y comunicación (TIC). Además, destaca la importancia de establecer acuerdos estratégicos con empresas proveedoras de servicios tecnológicos y entidades financieras para mejorar la investigación fiscal. Finalmente, enfatiza la necesidad de adecuar la legislación peruana al Convenio de Budapest en este ámbito.

El estudio de Usaqui (2022) examinó la relación entre la capacitación efectiva y la incidencia de delitos de cibercriminalidad en Lima. A través de encuestas a 20 fiscales, 15 abogados y policías, se identificó una correlación significativa respaldada por un valor de Chi cuadrado de 2,191. La conclusión sugiere que la fiscalía debe proporcionar capacitación especializada para mejorar las técnicas de investigación y persecución en delitos cibernéticos, facilitando así la obtención de pruebas sólidas y la identificación eficaz de los autores.

El estudio de Vilca (2022) buscó determinar la relación entre las competencias en ciberseguridad y la investigación de delitos cibernéticos en el ámbito penal. A través de un enfoque cuantitativo correlacional y encuestas, se identificó una correlación negativa y muy baja entre estas variables. Se concluye que es fundamental que los profesionales del ámbito legal desarrollen competencias en ciberseguridad para abordar eficientemente la investigación de la cibercriminalidad desde sus respectivas funciones.

Tras revisar los antecedentes más relevantes sobre el tema, es importante establecer el marco teórico que orientará esta investigación, partiendo por conceptualizar la eficacia del sistema judicial. Al respecto, Martínez (2022) define la eficacia judicial como la capacidad de resolver los casos de forma oportuna, asegurando así un proceso legal accesible para los ciudadanos. Dicha eficacia debe

abarcar todas las etapas procesales, tal como lo sugirieron las investigaciones anteriores.

Asimismo, la persecución penal, responsabilidad estatal, comprende la investigación, identificación de responsables, juzgamiento y aplicación de sanciones (Diccionario panhispánico del español jurídico, 2023; Flores, 2016). La fiscalía, como ente clave, se encarga de investigar delitos, recolectar pruebas y fundamentar la culpabilidad (Ríos, 2001). La efectividad en cada fase, desde la investigación hasta la imposición de sanciones, es esencial para asegurar resultados justos (Ore y Loza, 2017).

En el contexto contemporáneo, la expansión tecnológica, acelerada por la pandemia, ha impulsado el aumento significativo de la cibercriminalidad (Zevallos, 2020). La creciente actividad en línea ha dado lugar a nuevas formas de fraudes electrónicos (Ibáñez, 2022), evidenciadas por un preocupante aumento en las denuncias. En 2021, se reportaron 18,596 denuncias, un incremento del 92.9% respecto a 2020. La Policía Nacional del Perú también registró un aumento del 65% en denuncias de crímenes cibernéticos, alcanzando 14,671 casos en 2021. En los primeros cuatro meses de 2022, se presentaron 7,297 denuncias, y se cerró el año con un total de 11,970 denuncias (Infobae, 2022; Castro et al., 2023). (Ver figura Nº 1, Anexo Nº 4)

Es evidente que la ciberdelincuencia está en constante aumento y representa una nueva forma de delincuencia que está causando daños a la economía y a miles de peruanos (Núñez y Carhuancho, 2020). Por lo tanto, es necesario analizar esta creciente problemática desde una perspectiva jurídica y social.

Pero que entendemos por ciberdelincuencia, según Mateos (2013) es el conjunto de acciones realizadas a través de sistemas informáticos que resultan en actividades ilícitas. Es una ampliación de la delincuencia convencional que se vale de las nuevas tecnologías para expandirse de forma exponencial. (Núñez y Carhuancho, 2020). Este tipo de delito ocurre en el ciberespacio, un entorno no físico

donde se llevan a cabo comunicaciones electrónicas y se almacenan datos digitales (Mayer, 2018).

La cibercriminalidad, según la Defensoría del Pueblo (2023) y la UNDOC (2022), se refiere a los delitos llevados a cabo mediante el uso de tecnologías de la información y la comunicación (TIC). Esta categoría engloba diversas actividades ilícitas impulsadas por Internet que afectan bienes jurídicos, como el honor, la intimidad y el patrimonio, según Di Piero (2013) y el Consejo Nacional de Política Criminal (2020). Así, la cibercriminalidad abarca una amplia gama de delitos en el ciberespacio con impacto en diferentes aspectos legales y sociales (Villavicencio, 2014).

Los delitos informáticos, según Parker (citado en Romeo, 1996), son acciones ilegales que requieren conocimiento especializado en tecnología informática para su comisión, investigación o acusación. Implican el uso de computadoras como medio o fin, siendo consideradas conductas típicas, antijurídicas y culpables (Téllez, 1996). En términos más concretos, la Defensoría del Pueblo (2023) los define como acciones ilícitas que utilizan dispositivos electrónicos e internet para causar daño a los bienes de terceros.

Bramont-Arias (1997) categoriza los delitos informáticos en: (1) Manipulación de datos de entrada, (2) Manipulación de programas, (3) Manipulación de datos de salida y (4) Manipulación remota (hacking). Por su parte La Interpol (2021) señala que los factores digitales que afectan la ciberdelincuencia incluyen cualquier elemento en el entorno digital que facilite o estimule la actividad criminal en línea. Entre estos factores, se destaca el anonimato (UNDOC, 2022). Otros seis factores identificados son: (i) conectividad, (ii) movilidad, (iii) interconectividad, (iv) sofisticación, (v) falta de información sobre la magnitud y alcances del fenómeno, y (vi) investigaciones complejas y transfronterizas (Interpol, 2021).

En Perú, los delitos cibernéticos más comunes, según el informe del Ministerio de Justicia y Derechos Humanos (2022), incluyen fraudes informáticos, que abarcan actividades como transferencias financieras y compras en línea, así como la

suplantación de identidad, que implica hacerse pasar por otra persona con el propósito de cometer un acto delictivo.

En el actual contexto de aumento de la cibercriminalidad, la estafa cibernética emerge como un tema central. La Plataforma Única del Estado Peruano (2023) ha identificado diversos ciberdelitos en aumento, como fraude informático, estafa agravada mediante el uso de medios electrónicos (incluyendo redes sociales, correos electrónicos y WhatsApp), suplantación de identidad e incitación a actividades sexuales con menores a través de la tecnología.

La estafa cibernética, un delito en constante crecimiento, se destaca como un fenómeno delictivo relevante (Acuario, 2016). Para comprender este fenómeno, comenzaremos explorando la figura jurídica de la estafa. En el Derecho Penal peruano, la estafa se encuentra regulada en el Código Penal, específicamente en el capítulo V que comprende los artículos 196 y 196-A, titulado "Estafa y otras defraudaciones".

Bramont-Arias (1997) quien establece que este delito se caracteriza por su naturaleza fraudulenta. En otras palabras, la estafa implica el uso de artimañas engañosas con el fin de inducir a error a la víctima, todo ello con el propósito de obtener un beneficio económico a expensas de su patrimonio.

Sin embargo, para que se configure legalmente el delito de estafa, es fundamental que se cumplan los cuatro elementos fundamentales. Buompadre (2012) señala que estos componentes esenciales comprenden el engaño, la astucia, el ardid y otras formas fraudulentas, cuya existencia es determinante en la construcción de la figura delictiva de la estafa. En lo que respecta a la tipicidad subjetiva, se requiere que el autor del delito actúe con dolo, es decir, con la intención y el conocimiento de su acción delictiva. (Cisneros y Jiménez , 2021)

Es relevante destacar que, aunque la persona engañada puede ser diferente de quien sufre el menoscabo económico, el sujeto pasivo del delito es aquel que realmente experimenta dicho perjuicio. (Aranguren, 2022).

Los datos estadísticos son alarmantes y evidencian un preocupante aumento exponencial en la comisión del delito de estafa entre los años 2021 y 2022. Según el reporte oficial del PNP, en 2021 se registraron 15.183 denuncias por estafa y otras defraudaciones, mientras que para 2022 esta cifra creció sustancialmente a 20.352 casos, lo cual representa un alza del 33.78% (Ver figura Nº 2, anexo Nº 4)

Como se ha destacado previamente, la estafa cibernética se ha convertido en una cuestión de gran relevancia en la actualidad, a pesar de la notable ausencia de una regulación específica en el ámbito legal. A pesar de que el Perú es signatario del Convenio de Budapest, el cual define la estafa informática como actos ilícitos que ocasionan daños patrimoniales a través de la manipulación de datos o sistemas con el propósito de obtener ganancias ilícitas (López, 2018), es necesario resaltar que hasta el momento no se ha incluido una tipificación precisa de este delito en la legislación peruana.

No obstante, Bramont-Arias (1997) ya había anticipado esta definición, caracterizándola como la aplicación de los elementos tradicionales de la estafa en el entorno digital, implicando engaño, inducción al error, disposición patrimonial y perjuicio económico. Esta concepción adquiere relevancia en medio del creciente panorama de la ciberdelincuencia.

En el ámbito nacional, es relevante destacar que el delito de estafa cibernética mantiene índices delictivos, según la Divindat (2023), en su reporte correspondiente al año 2021, señala que se presentaron 5,620 denuncias por este ilícito, logrando capturar a 135 personas. No obstante, para 2022 se aprecia una disminución en las denuncias, con 3,946 casos, a la vez que se incrementaron considerablemente las capturas al alcanzar las 229 personas. (Ver figura Nº 3, anexo Nº 4)

La estafa cibernética o estafa informática ha cobrado un rol destacado en el ámbito de la ciberdelincuencia, conformando la base primordial de este tipo de delitos (Ministerio de Justicia y Derechos Humanos, 2022). Por ello, para la presente investigación, basando en el informe de la Defensoría del Pueblo (2023) se ha

establecido dos categorías de estudio: (i) insuficiente legislación y (ii) efectos de la persecución penal del delito de estafa.

La primera categoría de la investigación “insuficiente legislación”, que en la persecución penal, se refiere a la carencia de un marco regulatorio sólido y coherente en el sistema legal (Martín, 2016). La ausencia de una normativa adecuada, facilita la discrecionalidad en el abandono o retiro del ejercicio de la acción penal (Rodríguez, 2013). Este panorama pone de manifiesto la urgente necesidad de perfeccionar la legislación con el propósito de garantizar que el ejercicio de la acción penal sea mandatorio y coherente con el derecho sustantivo, con el fin de prevenir el posible abuso de la discrecionalidad en el proceso penal (Ashworth, 2009).

Dentro de esta categoría, se explorarán las restricciones y desafíos inherentes a la legislación vigente en lo que atañe a la estafa cibernética. Asimismo, se abordarán las siguientes subcategorías:

Convenio de la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest): El Convenio de Budapest sobre Ciberdelincuencia, creado por el Consejo de Europa, es un tratado internacional que ha estado en vigor por más de una década y es esencial en la lucha contra la ciberdelincuencia a nivel global (Clough, 2019), el cual ha influido en la formulación de leyes nacionales sobre delito cibernético en numerosos países. Su énfasis en la cooperación internacional lo convierte en un instrumento fundamental (Golman, 2021).

El Convenio de Budapest busca armonizar las leyes sobre delitos cibernéticos y fomentar la cooperación internacional para combatirlos, reconociendo la interconexión de la tecnología moderna. Ha tenido un impacto global y ha influenciado la legislación en países del Pacífico a través de incentivos estatales (Golman, 2021). Este tratado proporciona un marco integral para abordar el delito cibernético, proteger derechos individuales y promover la cooperación internacional. Además, se enfoca en desarrollar la capacidad de los países para combatir eficazmente el delito cibernético (Clough, 2019).

Sin embargo, a pesar de la estrecha relación entre la estafa y la ciberdelincuencia, la legislación nacional, como destaca Bramont-Arias (1997) establece una distinción notable entre el fraude informático y la estafa. En el ámbito de la persecución penal de la estafa, esta se considera solamente como un agravante del delito de estafa, ya que abarca una amplia gama de actividades fraudulentas que no necesariamente involucran tecnología.

El Informe situacional de cibercriminalidad de la Defensoría del Pueblo (2023) refleja esta distinción al clasificar la estafa como un ciberdelito contra el patrimonio, particularmente en su forma agravada (artículo 196-A, numeral 5). Esto ocurre cuando el autor utiliza el engaño para acceder a información de tarjetas de ahorro o crédito con el fin de obtener ganancias ilegítimas a expensas de terceros.

En cuanto a la Normativa Legal Nacional Vigente, la regulación de los crímenes cibernéticos en Perú tiene su origen en el año 2000 con la promulgación de la Ley N°27309, que introdujo un nuevo capítulo en el Código Penal relacionado con delitos en el ámbito patrimonial y tecnológico. Posteriormente, en 2013, la Ley N°30096 amplió el alcance de las conductas ilícitas vinculadas a la tecnología. En 2018, la Ley N°30838 incorporó disposiciones referentes a delitos que involucran propuestas a menores con fines sexuales a través de medios tecnológicos. Además, en 2019, Perú ratificó el Convenio de Budapest, marcando un hito en la legislación relacionada con la cibercriminalidad del país (Zevallos, 2020).

La Ley N° 30096, comúnmente conocida como la legislación de crímenes cibernéticos en Perú, abarca diversas categorías de delitos. Estas incluyen transgresiones relacionadas con datos y sistemas informáticos, crímenes cibernéticos que afectan la integridad y la libertad sexual, infracciones que vulneran la privacidad y el secreto de las comunicaciones, delitos informáticos que causan daño al patrimonio y conductas delictivas en línea que socavan la confianza pública. Esta ley proporciona un marco integral para abordar los desafíos de seguridad en el ámbito digital en Perú.

Dentro de la segunda categoría, “Persecución Penal de la Estafa Cibernética", de acuerdo al Diccionario panhispánico del español jurídico (2023), engloba la investigación de estos delitos, la identificación de los responsables, el juzgamiento y la imposición de sanciones. Esta es una responsabilidad pública del Estado (Flores, 2016), donde la Fiscalía desempeña un papel fundamental en este proceso, ya que tiene la exclusiva responsabilidad de investigar los delitos, reunir pruebas y fundamentar la culpabilidad del presunto autor (Ríos, 2001).

En la persecución penal del delito de estafa cibernética se enfrentan obstáculos en el proceso legal. Estos obstáculos abarcan barreras jurisdiccionales y la complejidad asociada con la persecución de delitos asistidos por tecnología (López, 2018). Un desafío adicional está relacionado con el costo financiero que conlleva el procesamiento de casos de fraude en línea, que a menudo involucran a múltiples víctimas ubicadas en diferentes lugares geográficos. En ocasiones, este costo supera los recursos presupuestarios disponibles, lo que resulta en la desestimación de casos.

Es importante notar que, a pesar de los esfuerzos en seguridad cibernética, el cibercrimen continúa en aumento (Mayer et al., 2020). La globalización y la sofisticación de los sistemas de tecnología de la información hacen que la captura de ciberdelincuentes sea más difícil, y algunos argumentan que las sanciones actuales carecen de severidad disuasoria (Smith-Ditizio y Smith, 2017).

En resumen, la persecución penal del delito de estafa cibernética comprende diversas etapas, desde la investigación hasta la imposición de sanciones, y enfrenta retos importantes en el proceso debido a factores como la complejidad tecnológica y los recursos financieros limitados disponibles (Ore y Loza, 2017). En virtud de lo señalado, para esta categoría se discutirán las siguientes subcategorías:

Subcategoría detección, de la estafa cibernética implica identificar y revelar actividades fraudulentas en entornos digitales. Este proceso utiliza diversas técnicas, como análisis forense de ciberataques, monitoreo del tráfico de red y algoritmos de aprendizaje automático (Kara y Aydos, 2020; Kotari y Chiplunkar, 2019). Su propósito

es reducir el fraude cibernético, protegiendo contra pérdidas económicas y violaciones de la privacidad. La detección eficaz permite implementar medidas preventivas

Subcategoría Investigación, la investigación de estafa cibernética implica abordar desafíos complejos con métodos tradicionales inadecuados. La evolución tecnológica complica la recopilación y análisis de pruebas en el entorno digital. La lucha contra la estafa cibernética requiere modelos y técnicas de investigación diversos, incluyendo análisis especializados de pruebas y controles (Mayer et al, 2020). La policía y la fiscalía enfrentan desafíos complejos debido a la naturaleza transnacional y evolutiva de los ciberdelitos. La investigación de ciberestafa demanda recursos técnicos y no técnicos especializados, y la efectividad de estos en la persecución de ciberdelincuentes es tema de debate en constante evolución (Defensoría del Pueblo, 2023).

En cuanto a la subcategoría de sanciones o penas en el derecho penal, estas representan castigos impuestos a los infractores, si bien su aplicación se ve obstaculizada por diversos factores, como la complejidad técnica para recopilar pruebas y cuestiones de jurisdicción, especialmente en casos de delitos cibernéticos como la estafa cibernética, según la Ley N° 30096 en Perú, diseñada para abordar los delitos informáticos, pero que aún muestra inefectividades.

El desafío crítico señalado por la Defensoría del Pueblo (2023) es la falta de conocimientos tecnológicos avanzados en el personal judicial, limitando la capacidad de enfrentar fraudes en internet. Por ello, propone como solución global establecer pautas claras y procedimientos para leyes efectivas en este ámbito. La capacitación digital es esencial para que los operadores de justicia comprendan las nuevas formas de delinquir mediante la tecnología y puedan abordarlas eficazmente, protegiendo así a los ciudadanos. Un plan integral con directrices legales y protocolos específicos de actuación se vuelve crucial para combatir con éxito este tipo de criminalidad en expansión.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1. Tipo de investigación

La investigación se clasifico como de tipo básico, ya que su objetivo primordial fue adquirir nuevos conocimientos relativos a los fundamentos del fenómeno delictivo emergente de la cibercriminalidad, en particular, aquellos relacionados con la comisión de estafas cibernéticas (Castro et al., 2023).

En cuanto a su alcance fue temporal, se caracterizó como un estudio transaccional, dado que, como correctamente subraya Vega et al. (2021), se llevó a cabo dentro de un marco temporal específico, concretamente en el año 2022.

En lo que respecta al enfoque metodológico, se adscribe al enfoque cualitativo, debido a que en esta investigación no llevó a cabo una cuantificación de las variables. El propósito fundamental consistió en comprender en profundidad el mencionado fenómeno delictivo, trascendiendo más allá de los datos numéricos, enfocándonos en las percepciones y apreciaciones concretas de especialistas (Sánchez, 2019)

3.1.2. Diseño de investigación

El presente estudio adoptó un sólido enfoque cualitativo no experimental para examinar los efectos de la insuficiente legislación del delito de estafa cibernética de manera integral (Vega et al, 2021).

Si bien otros enfoques se enfocan en variables aisladas, este reconoció la complejidad del tema estudiado como un sistema. De este modo, en lugar de probar hipótesis preestablecidas, este diseño indagó las diversas aristas de la insuficiente legislación desde la perspectiva de distintos actores en el distrito fiscal de Santa. Lo que reveló valiosas perspectivas gracias a su enfoque cualitativo, centrado en la descripción y comprensión.

3.2. Categorías, Subcategorías y matriz de categorización:

Categoría 1: insuficiente legislación

Insuficiente legislación, en la persecución penal, se refiere a la carencia de un marco regulatorio sólido y coherente en el sistema legal (Martín, 2016). Por lo que, la ausencia de una normativa adecuada, facilita la discrecionalidad en el abandono o retiro del ejercicio de la acción penal (Rodríguez, 2013).

Subcategorías:

- Convenio y protocolos sobre la ciberdelincuencia del consejo de Europa (Convenio de Budapest)
- Ley N° 30096
- Articulo N° 196- A del Código penal: Estafa agravada.

Categoría 2: Persecución penal de la estafa cibernética

La persecución penal del delito de estafa cibernética comprende diversas etapas, desde la investigación hasta la imposición de sanciones, y enfrenta retos importantes en el proceso debido a factores como la complejidad tecnológica y los recursos financieros limitados disponibles (Ore y Loza, 2017).

Subcategorías

- Detección
- Investigación
- Sanciones

Matriz de categorización apriorística:

Siguiendo las pautas institucionales pertinentes, se incorporó a la investigación el "Anexo N° 1". En este anexo se incluyó información complementaria y relacionada con la investigación en cuestión. Aunque no se detalla el contenido específico de dicho anexo en esta declaración, es importante destacar que se ajustó a las regulaciones y guías establecidas por esta prestigiosa institución académica.

3.3. Escenario de estudio

El escenario de estudio se refiere al contexto o la situación en la que se lleva a cabo una investigación. En este caso, la presente investigación se desarrolló en el Distrito fiscal del Santa. La elección de este escenario específico aseguró que los resultados son aplicables en un contexto jurídico concreto y refuerza la validez de la investigación.

3.4. Participantes

En esta investigación, se adoptó la recomendación de Hernández y Mendoza (2018) al reconocer la importancia de participantes con características comunes para lograr resultados específicos. Para seleccionar a los 5 jueces y fiscales se tomó en consideración su calificación, experiencia, conocimiento, que tengan la disposición de contribuir y participar en la investigación, fuera de que se establecieron los criterios de inclusión y exclusión.

Con el objetivo de entrevistar a operadores de justicia especializados en estafa cibernética, se seleccionó un grupo de 10 participantes, compuesto equitativamente por 5 jueces y 5 fiscales del distrito fiscal de Santa. Esta elección aseguró la representación de las perspectivas de los magistrados involucrados en la persecución y resolución de casos en este distrito específico, garantizando así la pertinencia y aplicabilidad local de la información recopilada.

Tabla 1

Composición de los participantes

Participantes	Cantidad	Código
Jueces	5	J
Fiscales	5	F
Total	10	

Nota: Del Distrito Fiscal del Santa, 2023.

Criterios de selección

(i) Criterios de inclusión

- Jueces del Distrito del Judicial del Santa.
- Fiscales del Distrito Fiscal del Santa.

(ii) Criterios de exclusión

- Jueces y fiscales que no ejerzan en el Distrito Judicial y Fiscal del Santa respectivamente.
- Jueces y fiscales que se hayan trasladado a otro distrito fiscal.

Asimismo, se ha considerado relevante examinar una muestra de 12 carpetas fiscales para analizar específicamente la categoría 2, que aborda la detección, investigación y sanción de la estafa cibernética. Esta muestra se percibe como representativa dada esta nueva modalidad de la estafa como delito cometido a través de medios digitales, lo que complica su identificación y afecta la presentación de denuncias. La limitación en la disponibilidad de carpetas fiscales sobre este delito justifica la selección de una muestra más pequeña. A pesar de ello, esta muestra de 12 expedientes posibilitó una evaluación cualitativa de los aspectos vinculados con la detección, investigación y sanción del delito en la categoría mencionada.

Tabla 2

Composición de carpetas fiscales

Participantes	Cantidad	Código
Expedientes	12	CF

Fuente: Del Distrito Fiscal del Santa, 2023.

Criterios de selección

(i) Criterios de inclusión

- Investigaciones exclusivamente relacionadas con el delito de estafa cibernética.
- Investigaciones realizadas en el Distrito judicial del Santa.

(ii) Criterios de exclusión

- Investigaciones que aborden delitos distintos a la estafa cibernética.
- Investigaciones que no estén vinculadas al Distrito judicial del Santa.

3.5. Técnicas e instrumentos de recolección de datos

3.5.1. Técnicas

Las técnicas ayudan a encontrar una solución a la problemática detectada y que son escogidas según el tema a investigar, así como criterios de razonabilidad (Rojas, 2011). Considerando lo señalado, se usaron las siguientes

Técnica del análisis documental: Logra representar el contenido de un documento para facilitar su localización posterior (Dulzaides y Molina, 2004). En este caso el análisis documental, no solo recaerá en la literatura, sino que se analizaran 12 carpetas fiscales respecto a las investigaciones de estafa cibernética.

Entrevista: Desde la perspectiva de la entrevista es una técnica de recolección de información y datos que se lleva a cabo a través de una conversación estructurada. En esta conversación, las preguntas se diseñan de manera específica para los propósitos del estudio, a menudo incluyendo preguntas de seguimiento. Las entrevistas se desarrollaran en formato de conversación o debate.

3.5.2. Los Instrumentos

Las técnicas contribuyeron a encontrar una solución a la problemática detectada y fueron seleccionadas según el tema a investigar, así como criterios de razonabilidad (Rojas, 2011). En consideración a lo anterior, se emplearon las siguientes:

Guia de observación documental: Para un mejor análisis de las 12 carpetas fiscales relacionadas con las investigaciones de estafa cibernética, se desarrolló este instrumento, el cual estaba estructurado de acuerdo a la subcategorías detección,

investigación y sanción, ello posibilito una observación de los expedientes más completa.

Guia de entrevista: esta fue una técnica de recolección de información y datos que se llevó a cabo a través de un cuestionario estructurado previamente diseñado antes de la entrevista. Las preguntas fueron diseñadas de manera específica para los propósitos del estudio, incorporando preguntas de seguimiento.

3.6. Procedimientos

La investigación se inició con una descripción de la realidad relacionada con la estafa cibernética a nivel internacional, nacional y local. Se buscaron antecedentes en la literatura académica y documentos oficiales para respaldar la investigación.

A continuación, se formularon claramente el problema de investigación, se plantearon hipótesis y se establecieron objetivos específicos. Se determinó el enfoque, tipo y diseño de la investigación, así como la selección de los participantes.

Se desarrolló una entrevista, que se aplicó a los participantes seleccionados con la debida autorización. Los datos recopilados se procesaron y analizaron de manera descriptiva e inferencial.

Finalmente, se presentaron conclusiones y recomendaciones basadas en los resultados de la investigación, con el objetivo de abordar la problemática de la estafa cibernética y mejorar la comprensión y gestión de este fenómeno.

3.7. Rigor científico

El rigor científico es esencial para garantizar la calidad y validez de la investigación. Se basa en la aplicación meticulosa del método científico, la revisión por la comunidad científica y una planificación, desarrollo, análisis y comunicación precisos. Además, implica la evaluación de la pertinencia, relevancia y consideraciones éticas y sociales de la investigación. (Hernández y Mendoza, 2018). La validez se asegurara a través de la validación de cuestionarios por expertos, y la confiabilidad se logra mediante una validación por triangulación, con ello, se asegura la coherencia y fiabilidad de los resultados.

3.8. Método de análisis de datos

- Se elaboró una matriz de datos de cada una de las categorías que se estudió.
- Se realizaron matrices de triangulación para así lograr la observación de las subdimensiones de cada categoría.

3.9. Aspectos éticos

Se basaron en los siguientes principios: *(a) Fue anónimo,* en razón a que la entrevista se aplicó teniendo el consentimiento de los sujetos participantes, pero sus datos personales no fueron consignados. *(b) Fue confidencial*, en razón a que los datos que se obtuvieron se emplearon para fines netamente académicos y fueron manejados solamente por la persona que está investigando. *(c) La beneficencia*, en razón a que quien investigo es abogado y posee tanto la experiencia como el perfil requerido para llevar a cabo el estudio satisfactoriamente, y, (d) *Es original*, en razón a que se respetó los derechos de autor, evitándose el plagio, en razón a que el tema que se investigo es original y se desarrolló en un contexto específico.

IV. RESULTADOS

La presente investigación arrojó una serie de hallazgos importantes con respecto al delito de estafa cibernética en el Distrito Fiscal de Santa. Estos resultados se desprendieron de un análisis exhaustivo de la normativa legal vigente, así como de entrevistas realizadas a 10 magistrados que ven este tipo de casos con frecuencia. También incluyó la recopilación y evaluación 12 carpetas de distintas sedes fiscales del distrito del Santa, donde se investigó casos de estafa cibernética ocurridos en este distrito.

Las entrevistas se llevaron a cabo con actores clave, concretamente cinco jueces y cinco fiscales. Sus perspectivas brindaron información valiosa sobre la percepción actual de la legislación y las áreas específicas que requieren atención prioritaria con respecto al delito de estafa cibernética. Los magistrados entrevistados, que tienen una amplia experiencia en estos casos, pudieron exponer cuáles son las deficiencias detectadas en la normativa vigente a la hora de perseguir este tipo de delitos, y los resultados fueron:

Resultados según el objetivo general: Determinar los efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022.

Tabla 3

Efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa.

Nº de objetivo	Objetivo específico	Resultado obtenido
1	OE1. Determinar la aplicación de la normativa internacional en la legislación nacional persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	Se determinó que el Convenio de Budapest, representa una normativa internacional orientada a estandarizar legislaciones y mejorar la colaboración transnacional en la lucha contra los ciberdelitos. Este enfoque apunta a optimizar la respuesta legal a la estafa cibernética mediante la armonización de leyes entre los países. Sin embargo, entre los magistrados, existen opiniones divergentes sobre la influencia del Convenio de Budapest en la legislación peruana contra la estafa cibernética. Mientras algunos reconocen su impacto positivo al fomentar la cooperación internacional y la armonización legal, otros expresan reservas. Se señala que, a pesar de que el Perú es firmante del convenio, la normativa nacional aún presenta vacíos en la tipificación del delito y carece de tratados específicos de cooperación internacional en materia de ciberdelitos.
2	OE2. Determinar las principales deficiencias de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	Se determinó que la Ley de Delitos Cibernéticos presenta fortalezas, como su amplitud en la tipificación, pero también limitaciones que incluyen la necesidad de precisiones y recursos. En cuanto a la estafa cibernética, la ley se percibe como favorable, definición clara de elementos y penas proporcionales. El Artículo 196-A reconoce y penaliza la estafa cibernética con medidas más severas. No obstante, persisten desafíos, como la falta de regulación específica, la necesidad de actualización y limitaciones en la presentación de pruebas digitales
3	OE3. Determinar los efectos de la insuficiente legislación	De acuerdo al objetivo específico planteado, los resultados obtenidos a través de las entrevistas realizadas a especialistas y el análisis de carpetas fiscales se determinó que la insuficiente legislación persecutoria ha afectado negativamente la

	persecutoria en la detección del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	detección de casos de estafa cibernética en el Distrito Fiscal de Santa, generando una serie de limitaciones como: - Normas que no contemplan adecuadamente las particularidades del delito cibernético de estafa. - Vacíos legales que dejan espacios de impunidad y dificultan el procesamiento de los infractores. - Deficiente cooperación internacional por falta de adopción de convenios. - Limitadas capacidades de investigación digital, recolección de pruebas electrónicas y recursos especializados. - Escasa formación de operadores de justicia en materia cibernética. - Vulnerabilidad de la población por baja cultura de seguridad digital. - Falta de agilidad procesal e incluso archivo de causas. - A nivel de carpetas fiscales, si bien se describen adecuadamente los hechos y pruebas, en la mayoría no se especifican actores ni roles involucrados, y en ninguna la colaboración interinstitucional. Por lo expuesto, se evidencia la necesidad de actualizar la legislación para enfrentar los desafíos del delito cibernético y mejorar la detección de estas estafas.
4	OE4. Determinar los efectos de la insuficiente legislación persecutoria en la investigación del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	A partir de los resultados obtenidos, se determinó que la insuficiente legislación persecutoria ha dificultado las investigaciones de estafa cibernética en el Distrito Fiscal de Santa de la siguiente manera: - La rápida evolución tecnológica excede la capacidad de actualización de las leyes, generando vacíos legales. - Falta especificidad normativa que aborde adecuadamente nuevos delitos digitales. - Definiciones legales ambiguas de ciberdelitos obstaculizan el procesamiento penal. - Dificultad en la recopilación y preservación de pruebas digitales. - Limitada cooperación transfronteriza por falta de acuerdos legales armonizados. - Escasez de recursos, capacitación y experticia de los investigadores. - Problemas para cooperar con proveedores online debido a ausencia de normas claras. - Asimismo, del análisis de carpetas fiscales pone se en evidencia vacíos

		como la falta de sustento legal de métodos y la indefinición sobre legalidad de algunas actuaciones, lo que evidencia la necesidad de fortalecer las directrices normativas para uniformar criterios de investigación sobre este delito complejo. Por lo expuesto, se concluye que la insuficiente legislación ha dificultado de manera sustancial las labores de investigación de estafas cibernéticas.
5	OE5. Determinar los efectos de la insuficiente legislación persecutoria en la sanción del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	De acuerdo los hallazgos, se determinó que la insuficiente legislación ha afectado negativamente la sanción de la estafa cibernética en el Distrito Fiscal de Santa de la siguiente manera: - Se ha generado un mayor riesgo de impunidad, al no enfrentar adecuadamente los ciberdelitos con sanciones proporcionales a la gravedad de los hechos. Esto debilita los efectos disuasivos. - Se ha otorgado menor protección a las víctimas y provisto escasa justicia frente a estas conductas ilícitas. - Se evidenciaron obstaculización en las investigaciones y condenas efectivas mediante la creación de vacíos normativos. - Se ha limitado las capacidades de las autoridades para combatir de manera coordinada la ciberdelincuencia. - Se ha generado incertidumbre sobre las conductas punibles en el ámbito digital. - Se dificulta la prevención y concientización sobre estafas cibernéticas. - Se ha visto entorpecida la cooperación transfronteriza necesaria dada la dimensión transnacional de estos delitos. - El análisis de las carpetas fiscales corrobora estos hallazgos al evidenciar deficiencias en la documentación de procesos judiciales y omisión de circunstancias atenuantes/agravantes al sancionar. Por lo expuesto, se concluye que esta problemática legislativa ha debilitado de forma importante los fines de la política criminal frente a la ciberdelincuencia.
Resultados por objetivo general		De acuerdo a los hallazgos obtenidos en cada uno de los objetivos específicos, se determinó que la insuficiente legislación persecutoria ha tenido un efecto negativo en el abordaje del delito de estafa cibernética por parte del Distrito Fiscal de Santa en 2022.

	- Específicamente, la normativa deficitaria ha dificultado las tareas de detección al generar vacíos legales que limitan la persecución penal. - Asimismo, ha entorpecido las labores investigativas al no proveer herramientas claras ante aspectos probatorios digitales. - De la misma forma, la insuficiente legislación ha afectado la sanción de este ilícito al no prever medidas disuasivas acordes a la gravedad de los hechos, generando un riesgo mayor de impunidad. - Finalmente, los hallazgos evidencian deficiencias normativas que implican menor tutela de víctimas y limitación en la cooperación transfronteriza necesaria para estos delitos. En conclusión, la investigación permite validar que la insuficiente legislación penal ha debilitado de manera sustancial la capacidad del Distrito Fiscal de Santa de enfrentar adecuadamente el fenómeno de la estafa cibernética durante el período analizado, en detrimento de los objetivos de prevención y sanción eficaz de este tipo de conductas delictivas.

Nota: Entrevista a especialistas.

Interpretación y discusión:

En base a los hallazgos, se pudo determinar que los efectos de la insuficiente legislación persecutoria del delito de estafa cibernética presentan serias limitaciones para combatir eficazmente la estafa cibernética en el Perú y sobre todo en el distrito fiscal del Santa.

La investigación realizada confirma que, en el ámbito del Distrito Fiscal de Santa durante 2022, la insuficiente legislación generó consecuencias negativas en la prevención, detección e investigación de este ilícito cada vez más frecuente. Tales hallazgos concuerdan con posturas como la de Vilca (2022), que enfatizan la urgencia de capacitar a operadores legales en ciberseguridad.

También se corroboran los hallazgos de informes como el de la Defensoría del Pueblo (2023), que señalan carencias en aspectos clave de la División de Investigación de Delitos de Alta Tecnología, tales como software y personal idóneo. Del mismo modo, estudios como los de Avalos (2021) resaltan la importancia de entrenar a funcionarios del sistema de justicia en tecnología digital.

Los entrevistados afirmaron que, producto de esta normativa débil, se afrontaron limitaciones en prevención, acusación con pruebas sólidas e imposición de penas proporcionales, por lo que se concuerda con las investigaciones previas que subrayan la necesidad de conocimientos tecnológicos especializados.

Asimismo, la legislación difusa generó un riesgo elevado de impunidad e indefensión de víctimas. Ello puede mitigarse, según Usaqui (2022), mediante capacitación constante al Ministerio Público.

En suma, la actualización legal, mayor equipamiento técnico-financiero de instituciones y desarrollo de habilidades digitales entre los operadores de justicia, permitiría subsanar las falencias detectadas y optimizar el tratamiento de esta problemática emergente, en aras de lograr una efectiva protección de las víctimas y prevención social.

Resultados según el objetivo específico 1): Determinar la aplicación de la normativa internacional en la legislación nacional persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022.

Tabla 4

Normativa internacional: Convenio de Budapest

	Interrogantes	Nº	Entrevistado/Código	Respuesta
Pregunta Nº 01	Como experto en derecho penal, ¿Qué conoce del Convenio del Consejo de Europa (Convenio de Budapest)?	1	J-1	El Convenio de Budapest es un tratado internacional que tiene como objetivo enfrentar el ciberdelito, incluida la estafa cibernética, a través de la cooperación entre países. Sin embargo, es importante destacar que cada país tiene su propia legislación nacional para abordar este tipo de delitos.
		2	J-2	Un convenio conformado por países como; Argentina, Brasil, Chile, Colombia, Costa Rica, Paraguay, República Dominicana, e incluido Perú. Estos países han ratificado y adoptado este convenio, lo que implica que deben adaptar su legislación nacional para cumplir con las disposiciones del convenio; esto implica la creación o modificación de leyes y regulaciones que sean consistentes con los principios y estándares del convenio en lo que respecta a la persecución de la estafa cibernética.
		3	J-3	El Convenio de Budapest tiene por objetivo de que las legislaciones de cada país perteneciente al convenio incorporen en su legislación nacional los elementos definidos en este; como, tipificar los delitos cibernéticos, establecer penas y sanciones adecuadas, y establecer medidas de investigación y cooperación internacional. Al hacerlo, se crea un marco legal coherente y armonizado que permite a los países colaborar de manera más efectiva en la persecución de la estafa cibernética, tanto a nivel nacional como internacional.
		4	J-4	Este convenio establece una serie de medidas y principios fundamentales para la prevención,

			investigación y persecución de delitos informáticos. También fomenta la cooperación internacional, facilitando la asistencia legal mutua, el intercambio de información entre las autoridades y la capacitación de profesionales en el ámbito de la ciberseguridad.
		5	J-5	Hablamos del primer tratado internacional que fue creado para poder proteger a la sociedad de cada nación perteneciente a este tratado de los delitos cibernéticos, adhiriéndose a su legislación de cada país perteneciente a este convenio.
		6	F-1	El Convenio de Budapest es un tratado internacional que busca armonizar la legislación y mejorar la cooperación entre los países en la lucha contra el ciberdelito. Define una lista de delitos cibernéticos, establece medidas de protección para las víctimas y promueve la cooperación internacional en la investigación y persecución de estos delitos.
		7	F-2	El Convenio de Budapest sobre Ciberdelincuencia, es un acuerdo internacional que establece medidas para combatir la ciberdelincuencia y prevenir, investigar y castigar dichos delitos. El acuerdo cubre una amplia gama de actividades delictivas en la esfera digital, incluido el acceso no autorizado a sistemas, el robo y la piratería de datos, el fraude informático y el uso indebido de dispositivos electrónicos. Establece disposiciones sobre cooperación internacional, extradición e intercambio de información entre los Estados miembros. En conclusión, el Convenio de Budapest busca armonizar las leyes nacionales y fortalecer la cooperación internacional para combatir eficazmente el ciberdelito en todas sus formas.
		8	F-3	Es un tratado internacional que tiene como objetivo combatir los delitos informáticos y proteger a las sociedades contra las amenazas cibernéticas.
		9	F-4	Este convenio es un tratado internacional que tiene como objetivo combatir el ciberdelito y promover la cooperación entre los países en la lucha contra este fenómeno, el Convenio de Budapest fue adoptado en 2001 y entró en vigor en 2004. Está vigente en los Estados miembros

			del Consejo de Europa y también es abierto para la adhesión de otros países no europeos.
	10	F-5	Es un tratado internacional que busca combatir los delitos informáticos y promover la cooperación internacional en este ámbito. Fue adoptado en el año 2001 y ha sido ratificado por numerosos países, incluyendo aquellos que pertenecen al Consejo de Europa. Este convenio establece normas y principios para la prevención, investigación y persecución de delitos informáticos, como el acceso no autorizado a sistemas y datos, interferencia en sistemas informáticos, fraude informático y pornografía infantil en línea, entre otros. También promueve la protección de datos y la seguridad de la información.

Resultados: Para los entrevistados, el Convenio de Budapest constituye un tratado internacional diseñado para abordar de manera coordinada el fenómeno creciente del ciberdelito. Particularmente busca combatir las estafas cibernéticas mediante la cooperación entre los Estados.

Si bien promueve la colaboración a nivel global, cada nación conserva autonomía respecto a su legislación interna sobre este tipo de ilícitos. En este marco, diversos países latinoamericanos como Argentina, Brasil, Chile, Colombia y otros han ratificado el convenio.

Al hacerlo, se comprometen a adecuar sus normativas nacionales conforme a los lineamientos establecidos. El objetivo principal es que incorporen elementos clave, tales como la tipificación de delitos informáticos, penas aplicables y mecanismos de investigación transfronteriza.

De esta forma, se busca generar un andamiaje legal armónico que facilite el intercambio de información para una persecución más eficaz de las estafas tanto a nivel local como a escala global.

Para los entrevistados, el convenio, asimismo, establece pautas fundamentales para la prevención, indagación y sanción de ilícitos digitales. La cooperación jurídica internacional mediante asistencia mutua y capacitación especializada adquiere relevancia.

En definitiva, desde la mirada de los operadores de justicia, el Convenio de Budapest representa un esfuerzo significativo para estandarizar legislaciones y optimizar la colaboración transnacional en la lucha contra el ciberdelito, focalizándose de manera particular en el delito de estafa cibernética.

Nota: Entrevista a especialistas.

Tabla 5

Influencia en la normativa internacional

	Interrogante	Nº	Entrevistado/Código	Respuesta
Pregunta Nº 02	¿Podría identificar de qué manera el Convenio de Budapest sobre Ciberdelincuencia ha influido en la legislación y regulación relacionada con la estafa cibernética en el Perú?	1	J-1	El Convenio de Budapest y las leyes nacionales se vinculan en el tratamiento de la estafa cibernética. Aunque cada país tiene su marco legal, es crucial que colaboren para armonizarlo, asegurando así una cooperación efectiva. Esta colaboración abarca el intercambio de información, asistencia mutua en investigaciones y la adopción de medidas preventivas y sancionatorias contra la estafa cibernética.
		2	J-2	El Convenio de Budapest sobre Ciberdelincuencia no ha influido en la legislación y regulación relacionada con la estafa cibernética propiamente; encontrando vacíos, en la tipificación del delito, medidas de investigación y cooperación internacional.
		3	J-3	El Convenio de Budapest ha influido en la legislación y regulación peruana relacionada con la estafa cibernética al establecer estándares, definir delitos específicos, recomendar penas y sanciones, promover la cooperación internacional y fortalecer la protección de datos personales. Esto ha permitido que el Perú cuente con un marco legal más sólido y coherente en la lucha contra la estafa cibernética.
		4	J-4	Respecto a su influencia en la legislación peruana sobre la estafa cibernética, podríamos decir que ha tenido cierto impacto en la regulación de esta actividad delictiva en nuestro país. Las autoridades peruanas han tomado en cuenta las recomendaciones y lineamientos establecidos en este convenio para actualizar sus leyes y sanciones relacionadas con la ciberdelincuencia; no obstante, debemos recordar que la ley por sí sola no es suficiente para combatir la delincuencia en línea. Es necesario que la

				ciudadanía también tenga conciencia y conocimiento sobre las medidas de seguridad digital para prevenir ser víctima de estafas o fraudes cibernéticos
		5	J-5	Ha servido para poder contextualizar los términos de Sistema Informático y Datos Informáticos.
		6	F-1	Por este convenio contamos con; definición de ciberdelitos y medidas de protección, cooperación internacional. Además, los países que ratifican el convenio deben adoptar las medidas legislativas necesarias para implementar sus disposiciones, es decir, su legislación nacional para tipificar los diferentes delitos cibernéticos y garantizar que los delincuentes sean llevados ante la justicia
		7	F-2	El Convenio de Budapest sobre Ciberdelincuencia ha tenido un impacto significativo en la legislación y regulación de la ciberdelincuencia en el Perú; como resultado del cumplimiento del acuerdo, el país ha fortalecido el marco legal para enfrentar este tipo de delitos, implementando medidas preventivas, investigativas y punitivas más graves. También se han aprobado leyes especiales, como la Ley de Delitos Informáticos, que define claramente los delitos cibernéticos e impone penas más severas a los responsables. Asimismo, la cooperación internacional ha mejorado en la lucha contra la ciberdelincuencia, facilitando el intercambio de información y la cooperación con otros países para perseguir a los delincuentes.
		8	F-3	La ratificación del Convenio de Budapest en Perú frente al fraude cibernético ha generado cambios significativos. Se estableció un marco legal específico, influyendo en la legislación local y promoviendo reformas que fortalecieron la capacidad de investigación y persecución. La creación de unidades especializadas y la implementación de mecanismos de cooperación internacional mejoraron la capacidad de respuesta y

				colaboración, consolidando eficazmente la lucha contra la delincuencia cibernética en el país.
		9	F-4	La adopción del Convenio de Budapest ha permitido al Perú mejorar la cooperación internacional para investigar y perseguir a los delincuentes involucrados en la estafa cibernética. De esta manera, se facilita el intercambio de información y la colaboración entre las autoridades peruanas y de otros países en la lucha contra este delito.
		10	F-5	El Convenio de Budapest también ha contribuido a la concienciación y educación sobre la estafa cibernética en el Perú.; esto a través de su implementación y promoción, se impulsan programas de formación y capacitación dirigidos a profesionales del derecho, fuerzas de seguridad y otros actores clave involucrados en la lucha contra la ciberdelincuencia. Esto ayuda a mejorar la preparación y respuesta del país frente a las estafas cibernéticas.
	Resultados: Las respuestas de los magistrados entrevistados demuestran diversas perspectivas sobre la influencia del Convenio de Budapest en la legislación peruana contra la estafa cibernética. Mientras algunos resaltan su impacto positivo al promover la cooperación internacional y armonización legal, otros expresan dudas señalando que si bien el Perú es firmante, la normativa nacional aún presenta vacíos en la tipificación del delito y falta de tratados de cooperación internacional en materia de ciberdelitos. Asimismo, un enfoque recurrente es la importancia de la concienciación ciudadana sobre seguridad digital, destacando que la ley por sí sola no es suficiente para combatir eficazmente la estafa cibernética. En conjunto, las respuestas sugieren una evaluación diversa respecto al papel del Convenio de Budapest en la legislación y regulación peruana contra este tipo de delitos, dado que existen opiniones tanto favorables como escépticas sobre su impacto real en la armonización legal y cooperativa para enfrentar este problema.			

Nota: Entrevista a especialistas.

Tabla 6

Interconexión entre la normativa internacional y la nacional en el delito de estafa cibernética.

	Interrogante	Nº	Entrevistado/Código	Respuesta
Pregunta Nº 03	¿Considera que existe una interconexión entre el Convenio de Budapest y la legislación nacional para abordar la persecución de la estafa cibernética?	1	J-1	Si, ya que el Convenio de Budapest establece estándares mínimos para la legislación nacional, pero los países pueden tener leyes adicionales o diferentes en relación a la persecución de la estafa cibernética. Por lo tanto, aunque existe una interconexión entre el Convenio y la legislación nacional, cada país puede tener sus propios mecanismos y enfoques para abordar este problema.
		2	J-2	Si, la interconexión entre el Convenio de Budapest y la legislación nacional permite la cooperación entre los países para compartir información, pruebas y conocimientos sobre la estafa cibernética, esto fortalece los mecanismos de persecución y permite una respuesta más eficiente y coordinada frente a este tipo de delito.
		3	J-3	Si, el Convenio de Budapest y la legislación nacional están interconectados y se complementan mutuamente en la persecución de la estafa cibernética. Obteniendo una adaptación de la legislación nacional a los principios y estándares del convenio, que permite una respuesta más efectiva y coordinada a nivel nacional e internacional.
		4	J-4	La legislación nacional puede complementar y fortalecer los principios y medidas establecidos en el Convenio de Budapest, permitiendo una mejor implementación y aplicación de sus disposiciones dentro de cada país. Además, la legislación nacional también puede abordar aspectos específicos que pueden no estar cubiertos por el convenio, como las sanciones y penas establecidas en el ámbito nacional Ambos son necesarios y se complementan mutuamente para lograr una respuesta integral y eficaz en la lucha contra estos delitos.

	5	J-5	Si, ya que complementa nuestra legislación para así tener un plano legal más claro de a que nos enfrentamos cuando tratamos estos delitos cibernéticos.
	6	F-1	Si, el Convenio de Budapest juega un papel importante en la influencia de la legislación nacional relacionada con la estafa cibernética; al proporcionar un marco internacional y lineamientos generales, el convenio alienta a los países signatarios a adoptar medidas similares y promover la cooperación internacional en la lucha contra el cibercrimen.
	7	F-2	El Convenio de Budapest y la legislación nacional están interconectados para abordar el fraude cibernético. El convenio establece estándares internacionales, sirviendo como marco para que los países elaboren sus leyes nacionales y se comprometan a armonizar su legislación, definir delitos cibernéticos, imponer sanciones y facilitar la cooperación internacional. Esta conexión asegura una armonización global en la lucha contra la ciberdelincuencia.
	8	F-3	Sí, el Convenio de Budapest sirve como un guía para los países vinculados, incluido el Perú, al proporcionar recomendaciones y estándares internacionales para la prevención, investigación y persecución de los delitos cibernéticos. Estos estándares internacionales pueden influir en la legislación nacional, ya que los países pueden tomar como referencia las disposiciones del convenio al diseñar y actualizar su propia legislación interna relacionada con la estafa cibernética.
	9	F-4	Si, el Convenio de Budapest y la legislación nacional para abordar la persecución de la estafa cibernética, el convenio de Budapest establece un marco internacional para la cooperación en la lucha contra el ciberdelito, y muchos países, incluido Perú, han adoptado medidas legislativas para alinear su legislación con los estándares establecidos en el convenio. En Perú, se promulgó la Ley de Delitos Informáticos en el año 2013, la cual incorpora muchas de las disposiciones del Convenio de Budapest, esta ley establece penas para diversos delitos

				informáticos, incluida la estafa cibernética, y brinda herramientas legales.
		10	F-5	Si, el Convenio de Budapest y la legislación nacional son herramientas complementarias para abordar la persecución de la estafa cibernética; tal Convenio de Budapest es un tratado internacional que establece normas y directrices para la lucha contra el delito cibernético, mientras que la legislación nacional permite a los países adaptar estas normas a sus sistemas legales internos. Juntos, proporcionan un marco legal sólido para combatir la estafa cibernética de manera efectiva.
	Resultados: Según las perspectivas expresadas por los entrevistados, existe una clara interconexión entre el Convenio de Budapest y la legislación nacional para abordar la persecución de la estafa cibernética. El convenio establece estándares internacionales y proporciona un marco que influye en la elaboración y actualización de las leyes nacionales. Los entrevistados destacan que este proceso permite a los países adoptar medidas legislativas alineadas con los principios y estándares del convenio, promoviendo así la cooperación internacional en la lucha contra el ciberdelito. En resumen, la interconexión entre el Convenio de Budapest y la legislación nacional es considerada fundamental para establecer un marco legal robusto y coordinado en la persecución de la estafa cibernética.			

Nota: Entrevista a especialistas.

Tabla 7

Interpretación de resultados del objetivo específico Nº 1

Objetivo Especifico	Nº	Interpretación	Resultado
1) Determinar la aplicación de la normativa internacional en la legislación nacional persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	**1**	Los operadores de justicia, sostienen que el Convenio de Budapest representa es una normativa internacional que tiene como propósito estandarizar legislaciones y optimizar la colaboración transnacional en la lucha contra los ciberdelito.	Se determinó que la aplicación de la normativa internacional, especialmente el Convenio de Budapest, representa una normativa internacional destinada a estandarizar legislaciones y mejorar la colaboración transnacional en la lucha contra los ciberdelitos. Este enfoque apunta a optimizar la respuesta legal a la estafa cibernética mediante la armonización de leyes entre los países. Sin embargo, entre los magistrados, existen opiniones divergentes sobre la influencia del Convenio de Budapest en la legislación peruana contra la estafa cibernética. Mientras algunos reconocen su impacto positivo al fomentar la cooperación internacional y la armonización legal, otros expresan reservas. Se señala que, a pesar de que el Perú es firmante del convenio, la normativa nacional aún presenta vacíos en la tipificación del delito y carece de tratados
	2	Los magistrados entrevistados demuestran diversas perspectivas sobre la influencia del Convenio de Budapest en la legislación peruana contra la estafa cibernética. Mientras algunos resaltan su impacto positivo al promover la cooperación internacional y armonización legal, otros expresan dudas señalando que si bien el Perú es firmante, la normativa nacional aún presenta vacíos en la tipificación del delito y falta de tratados de cooperación internacional en materia de ciberdelitos. Asimismo, un enfoque recurrente es la importancia de la concienciación ciudadana sobre seguridad digital, destacando que la ley por sí sola no es suficiente para combatir eficazmente la estafa cibernética.	
	3	Según las perspectivas expresadas por los entrevistados, existe una clara interconexión entre el Convenio de Budapest y la legislación nacional para abordar la persecución de la estafa cibernética. El convenio al establecer estándares internacionales y proporcionar un	

	marco que influye en la elaboración y actualización de las leyes nacionales. Los entrevistados destacan que este proceso permite a los países adoptar medidas legislativas alineadas con los principios y estándares internacionales de lucha contra os ciberdelitos.	específicos de cooperación internacional en materia de ciberdelitos.

Nota: Resultados de las tablas 4,5 y 6.

Interpretación y discusión de resultados del objetivo específico 1:

El primer objetivo específico se centró en determinar la aplicación de la normativa internacional en la legislación nacional. Los hallazgos mostraron que los magistrados conocen respecto al Convenio de Budapest, el cual representa una normativa internacional destinada a estandarizar legislaciones y mejorar la colaboración transnacional en la lucha contra los ciberdelitos. Sin embargo, a pesar de este reconocimiento positivo, coinciden con la postura de Alonso y Esparza (2017) que aunque diferentes países incluidos el Perú han establecido leyes basadas en acuerdos internacionales para hacer frente a los crímenes cibernéticos, basados en dicho convenio, la realidad es que la delincuencia cibernética sigue siendo un problema a nivel mundial.

Los hallazgos revelan la existencia de áreas específicas en la legislación nacional respecto a los ciberdelitos que demandan atención y mejora, especialmente en lo concerniente a la estafa cibernética. Aunque se reconoce la conexión entre el convenio internacional y la legislación nacional, se destaca la necesidad de perfeccionar los mecanismos de comunicación y coordinación para lograr una aplicación más efectiva. Este punto de vista coincide con la postura expresada por López (2018), quien subraya que, a pesar de que el Perú es signatario del Convenio de Budapest, el cual define claramente la estafa cibernética como actos ilícitos que ocasionan daños patrimoniales mediante la manipulación de datos o sistemas con el fin de obtener ganancias ilícitas, aún no se ha incorporado una tipificación precisa de este delito en la legislación peruana. Este análisis subraya la importancia de fortalecer la armonización entre la normativa internacional y la legislación nacional para abordar de manera más eficiente la estafa cibernética.

Resultados según el objetivo específico 2*):* Determinar las principales deficiencias de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022***.***

Tabla 8

Fortalezas y limitaciones de la Ley N° 30096.

	Interrogante	Nº	Entrevistado/Código	Respuesta
Pregunta Nº 04	¿Cuáles son las fortalezas y limitaciones que identifica en la Ley N° 30096, ley de delitos cibernéticos en el Perú?	1	J-1	La Ley N° 30096 en Perú sobre delitos cibernéticos destaca por su actualización constante, definiciones claras, sanciones adecuadas y disposiciones para la cooperación internacional en la persecución de estos delitos. Sin embargo, señala desafíos en la Ley: Falta de precisión: Necesidad de mayor claridad en la tipificación de delitos. Recursos de investigación: Limitaciones en capacidad y recursos para investigaciones de delitos cibernéticos, y, Concientización: Requiere inversión en programas educativos sobre riesgos cibernéticos y medidas de protección.
		2	J-2	La ley contra delitos cibernéticos en Perú tiene un amplio alcance, abordando diversas infracciones como acceso indebido, fraude y más, con penas proporcionales y la opción de confiscar bienes ilícitos. Sin embargo, enfrenta desafíos en su aplicación debido a limitaciones de recursos y conciencia pública, lo que dificulta la detección y denuncia de estos delitos.
		3	J-3	La ley se promulgó en 2013, lo que permitió llenar un vacío legal al regular específicamente los delitos cibernéticos, demostrando la voluntad del gobierno por adaptarse a los cambios tecnológicos y brindar una mejor protección jurídica. Si bien la norma fue un paso importante, la rápida evolución tecnológica plantea desafíos para su constante revisión y adecuación, de forma que pueda mantenerse a la vanguardia abordando nuevas modalidades delictivas. Se requiere actualizar periódicamente la ley para afrontar las amenazas emergentes.
		4	J-4	La ley de delitos cibernéticos en el Perú, desde mi perspectiva; en cuanto a las fortalezas de esta ley, busca proteger a las personas de los delitos

				cometidos en el mundo digital, como el robo de identidad, el acoso cibernético y la difusión no autorizada de información privada. La ley establece penas y sanciones para aquellos que cometen estos delitos, lo cual envía un mensaje claro de que estas acciones no serán toleradas; sin embargo, también hay algunas limitaciones en esta ley, ya que es evidente que la tecnología avanza rápidamente, lo que dificulta mantener una ley actualizada y efectiva frente a las nuevas formas de delitos cibernéticos que puedan surgir.
		5	J-5	Entre las fortalezas y debilidades de la legislación peruana contra los delitos informáticos: Fortalezas: i) Previsibilidad: Al tipificar conductas y establecer penas, permite conocer las consecuencias legales de los delitos cibernéticos y aplicarlas oportunamente; y, ii) Conceptualización: Ayuda a comprender correctamente los términos referidos a este tipo de crímenes mediante definiciones claras. En cuanto a las Debilidades: i) Escasa integración del Convenio de Budapest: Si bien lo menciona, se podría profundizar más en adoptar sus disposiciones y artículos, y, ii) Falta de articulación: No especifica cómo aplicar lo establecido ni remite a otra normativa que lo guíe, dificultando su implementación efectiva.
		6	F-1	Las fortalezas son las siguientes: Cooperación internacional, fortalecimiento institucional y prescripción de ciberdelitos. Las limitaciones son las siguientes: Aplicación y recursos, concientización y educación, cooperación entre sectores y capacidad de respuesta rápida.
		7	F-2	Fortalezas: Definición amplia y actualizada de ciberdelito, incluyendo modalidades como hace, suplantación, robo de datos y grooming, lo que permite mayor protección frente a nuevas formas de criminalidad digital. Se establecen sanciones proporcionales y se responsabiliza a proveedores de cooperar en investigaciones. Limitaciones: Falta de claridad en algunos aspectos que dificulta la interpretación y aplicación uniforme de la norma. Es necesario fortalecer mecanismos de cooperación internacional para investigar y procesar estos delitos transfronterizos. Se requiere mejorar la capacidad para investigar y

			procesar efectivamente estos crímenes digitales.
	8	F-3	La ley presenta aciertos como prever la cooperación internacional. No obstante, se deben superar debilidades como no mantenerse a la vanguardia con modificaciones legislativas que incorporen nuevos ilícitos digitales y brindar definiciones más precisas para una adecuada comprensión y uso normativo.
	9	F-4	La ley demuestra voluntad estatal de abordar este tema. No obstante, es menester concientizar e instruir más a usuarios y autoridades, a fin de prevenir ilícitos cibernéticos de manera efectiva aprovechando todo el potencial normativo.
	10	F-5	La ley presenta aciertos pero es necesario superar limitaciones como agilizar procesos y asegurar la actualización permanente de capacidades forenses y legales ante los rápidos cambios tecnológicos.

Resultados: De acuerdo al análisis de las respuestas de los entrevistados, se pueden resumir las siguientes fortalezas y limitaciones más recurrentes en la Ley de Delitos Cibernéticos en el Perú:

Fortalezas:

- Tipificación amplia de conductas y establecimiento de penas proporcionales.
- Disposiciones para cooperación internacional.
- Demuestra voluntad del Estado de abordar los delitos cibernéticos.

Limitaciones:

- Necesidad de mayor precisión y claridad en algunos aspectos de la ley.
- Limitaciones en recursos, capacidades y concientización para investigar estos delitos.
- Riesgo de desactualización ante la rápida evolución tecnológica.
- Hace faltan fortalecer mecanismos de cooperación transfronteriza.
- Se requiere agilizar procesos legales y judiciales relacionados.

Hay consenso en que la Ley N° 30096 muestra importantes avances en la regulación de delitos cibernéticos en el Perú, pero aún enfrenta desafíos, especialmente en términos de precisión, recursos de investigación, concienciación y adaptación a los cambios tecnológicos. La cooperación internacional y la actualización constante son aspectos destacados, pero se subraya la importancia de superar las limitaciones identificadas para fortalecer la eficacia de la legislación.

Nota: Entrevista a especialistas.

Tabla 9

Ley N° 30096 y su limitaciones para la persecución penal.

	Interrogante	Nº	Entrevistado	Respuesta
Pregunta Nº 05	¿Considera que la Ley N° 30096, favorece la persecución penal del delito de estafa cibernética?	1	J-1	Si, ya que, esta ley define los elementos necesarios para la configuración del delito de estafa cibernética, como la utilización de medios electrónicos, el engaño, y la obtención de beneficios económicos ilícitos.
		2	J-2	Sí, la Ley N° 30096 favorece la persecución penal del delito de estafa cibernética. Esta ley establece específicamente como delito el uso ilegítimo de dispositivos o sistemas informáticos para obtener beneficios económicos de forma fraudulenta. Además, contempla penas y sanciones proporcionales a este tipo de delitos.
		3	J-3	Si, puesto que sirve de complemento para resolver tal delito y saber si cumple con lo necesario para ser tipificado bajo este delito.
		4	J-4	Sí, porque esta ley establece medidas de investigación y cooperación en casos de delitos cibernéticos, lo que facilita la recolección de pruebas y la colaboración con otras jurisdicciones en el caso de estafas cibernéticas que involucren a personas o empresas en otros países.
		5	J-5	Si, sin esta ley no podríamos enfrentar los delitos cibernéticos que son muy comunes hoy en día; y es que un vació legal ante uno o varios hechos delictivos podría causar un gran estancamiento para la vía penal del derecho.
		6	F-1	La Ley N° 30096 favorece la persecución penal del delito de estafa cibernética; porque esta normativa define claramente y de manera precisa los distintos tipos de delitos cibernéticos, incluyendo la estafa en línea y esto facilita a las autoridades identificar y procesar a los responsables de estos actos ilícitos.
		7	F-2	Sí, porque la Ley N° 30096 establece una definición amplia de ciberdelitos, que incluyen la estafa cibernética como una forma de engaño o fraude realizado por medios electrónicos; además, la ley determina sanciones proporcionales para este tipo de delitos y considera la responsabilidad de los proveedores de servicios en línea de cooperar en

			las investigaciones.
	8	F-3	Si, La Ley N° 30096, también conocida como la Ley de Delitos Informáticos, es una normativa que tiene como objetivo principal fortalecer la persecución penal de los delitos cibernéticos en Perú, y esta ley es favorable, puesto que establece disposiciones específicas para combatir el fraude electrónico y la estafa cibernética, entre otros delitos relacionados con las tecnologías de la información y comunicación.
	9	F-4	Si, ya que por ejemplo esta ley contempla disposiciones relacionadas con la investigación y recolección de evidencias digitales, lo cual es fundamental para poder llevar a cabo un proceso judicial eficaz.
	10	F-5	Sí, porque la Ley N° 30096 brinda un marco legal sólido que favorece la persecución penal del delito de estafa cibernética al definir claramente los delitos informáticos, establecer sanciones adecuadas y regular los procedimientos de investigación.

Resultados : Todos los magistrados entrevistados coinciden que la Ley N° 30096 favorece la persecución penal de los ciberdelitos, destacando los siguientes puntos:

- Define los ciberdelitos, como el uso de medios electrónicos, el engaño y la obtención de beneficios económicos de forma fraudulenta.
- Establece penas y sanciones proporcionales para este tipo de ilícitos.
- Sirve de complemento legal para tipificar correctamente la conducta como estafa cibernética.
- Regula medidas de investigación como recolección de pruebas digitales y cooperación internacional, lo cual es clave para perseguir este delito.
- Provee un marco normativo que permite enfrentar este problema tan común en la actualidad.
- Define de manera amplia los ciberdelitos, incluyendo específicamente la estafa digital.

Sin embargo, los magistrados expresan la opinión de que, a pesar de estas fortalezas, el delito de estafa cibernética no está tipificado como tal en la normativa. Consideran que debería ser explícitamente incluido y tratado como una modalidad específica de delito cibernético, y sugieren su incorporación para fortalecer la efectividad de la legislación en este ámbito.

Nota: Entrevista a especialistas.

Tabla 10

Artículo N° 196-A del Código Penal y la tipificación de la estafa agravada.

	Interrogantes	Nº	Entrevistado	Respuesta
Pregunta Nª 06	¿Podría explicar en detalle la aplicación del Artículo N° 196-A del Código Penal, respecto a la tipificación de la estafa agravada, en el contexto de la persecución de la estafa cibernética?	1	J-1	El Artículo N° 196-A del Código Penal peruano aborda la estafa cibernética, tipificando la estafa agravada en casos electrónicos. Sus elementos son: a. Engaño: Requiere que el autor use engaño para inducir a error a la víctima. b. Ánimo de lucro: La estafa cibernética busca beneficio económico o material a expensas de la víctima. c. Agravantes: Establece circunstancias que agravan el delito cuando se utiliza medios electrónicos
		2	J-2	La pena será mayor cuando se trate de una estafa q se realice con medios cibernéticos. Es decir que, en cuanto a las penas, el Artículo N° 196-A establece que la pena para la estafa agravada cometida a través de medios electrónicos o cibernéticos puede ser mayor que la pena para la estafa simple. La pena varía según la gravedad del delito y puede incluir privación de libertad, multa u otras sanciones establecidas por el juez.
		3	J-3	La pena será mayor cuando se trate de una estafa que se realice con medios cibernéticos. Es decir que, en cuanto a las penas, el Artículo N° 196-A establece que la pena para la estafa agravada cometida a través de medios electrónicos o cibernéticos puede ser mayor que la pena para la estafa simple. La pena varía según la gravedad del delito y puede incluir privación de libertad, multa u otras sanciones establecidas por el juez.
		4	J-4	Es importante destacar que, debido a la rápida evolución de la tecnología y las formas de cometer estafas cibernéticas, los fiscales y jueces deben adaptar su interpretación y aplicación de la ley para abordar los nuevos métodos y desafíos que surgen constantemente en este ámbito. El Artículo N° 196-A del Código Penal peruano tipifica la estafa agravada, incluyendo aquellas cometidas a través de medios electrónicos o cibernéticos; lo cual es lo más característico de este delito el uso de tales herramientas cibernéticas para cometer el engaño y obtener algún provecho lucrativo de este.

		5	J-5	Este articulo tipifica como agravada la defraudación cuando se comete mediante el uso de tecnologías de la información y las comunicaciones; esto quiere decir, que esta se aplica a los casos de fraude cibernético e impone sanciones más severas a los infractores, reconociendo la naturaleza única del delito cibernético. En el contexto del enjuiciamiento por fraude cibernético, esta disposición se aplicaría cuando un individuo utiliza un sistema informático o Internet para engañar a otra persona o entidad para obtener ganancias financieras. Por ejemplo, si alguien utiliza sitios web falsos para obtener información financiera confidencial de víctimas desprevenidas, podría ser acusado de fraude agravado según la Sección 196-A.
		6	F-1	Si bien este articulo habla sobre la estafa agravada, los supuestos dictados que se dictan en este no abarcan la estafa cibernética; así que con aplicación que un delito puede agravarse con la utilización de medios tecnológicos para fines lucrativos; tal concepto que acabo de dictar podría recaer en el inciso 5 de este código penal peruano, aun así bajo mi criterio, este inciso es prueba de la carente regulación de los ciberdelitos en la norma.
		7	F-2	El artículo 196-A del Código Penal peruano tipifica la estafa agravada, incluyendo en uno de sus incisos la utilización de medios informáticos o redes electrónicas para cometer el delito. Esto reconoce que la estafa cibernética es una forma moderna de estafa que aprovecha las TIC para engañar a las víctimas. Incluye supuestos como la suplantación de entidades bancarias para obtener datos personales y financieros de forma fraudulenta. Este artículo establece penas más severas para la estafa agravada cometida a través de medios digitales. Esto demuestra la voluntad del legislador de proteger mejor a las víctimas de este tipo de estafa y perseguir a sus responsables
		8	F-3	El artículo 196-A del Código Penal peruano reconoce y tipifica la estafa cibernética como una variante moderna de la estafa tradicional, haciendo hincapié en el uso de medios informáticos o redes electrónicas para cometer el delito. Este enfoque refleja la adaptación de la legislación a los avances tecnológicos. La normativa aborda casos como la

			suplantación de entidades bancarias para obtener datos personales y financieros de manera fraudulenta, estableciendo penas más severas para la estafa agravada perpetrada a través de medios digitales.
	9	F-4	Esta disposición legal busca proteger a las personas de los delitos relacionados con la estafa, garantizando una sanción adecuada para aquellos que cometan este tipo de actos. Nos dicta un catálogo de supuestos que son de implicancia a los casos de estafa agravados por características ya sea por número, o herramienta usada para cometer el acto, los lleva a ser de mayor de gravedad y por ende de mayor sanción.
	10	F-5	El artículo 196-A del Código Penal se refiere a la tipificación de la estafa agravada en el ámbito cibernético. Básicamente, esto significa que se considerarán más graves los casos de estafa que involucren tecnología o medios electrónicos. La idea detrás de esta ley es proteger a las personas de aquellos individuos sin escrúpulos que utilizan la tecnología para engañar y robar información personal o dinero. Es importante tener en cuenta que cada país puede tener su propio conjunto de leyes y regulaciones relacionadas con la estafa cibernética.
	Resultados: Los entrevistados manifestaron que el artículo 196-A del Código Penal peruano reconoce y tipifica la estafa cibernética como una variante moderna de la estafa, utilizando medios digitales. Esta disposición aborda el uso de sistemas informáticos, redes e Internet para cometer el delito, incluyendo casos como la suplantación de entidades en línea para robar datos. Asimismo, establece penas más severas para la estafa agravada cometida electrónicamente, con el objetivo de proteger a las víctimas de este fraude digital. Se aplica cuando individuos emplean tecnología para engañar y obtener ganancias económicas, reconociendo el agravante por el uso de herramientas tecnológicas con fines lucrativos.		

Nota: Entrevista a especialistas.

Tabla 11

Desafíos de la interpretación y aplicación del artículo N° 196-A del Código Penal

	Interrogantes	Nº	Entrevistado/Código	Respuesta
Pregunta Nº 07	¿Cuáles considera son los desafíos específicos asociados con la interpretación y aplicación de este artículo en casos de estafa cibernética?	1	J-1	Desafíos en aplicar el Artículo N° 196-A en estafas cibernéticas: Evolución tecnológica: Adaptación constante ante métodos sofisticados de estafadores; y, Cooperación entre sectores: Colaboración esencial entre organismos, proveedores y empresas para prevenir estos delitos.
		2	J-2	Poder interpretar cuales son todos los medios electrónicos por lo que se tipificarían en este tipo, lograr identificar al autor del delito y establecer medidas efectivas para proteger a la víctima de los delitos cibernéticos.
		3	J-3	La falta de regulación otros diversos hechos delictivos cibernéticos, que bajo li opinión deberían tener su propio articulo dentro del Código penal peruano actual; ya que, la generación actual va de mano más con la tecnología que con cualquier otra cosa en el mundo.
		4	J-4	La naturaleza transfronteriza y anónima de la ciberdelincuencia, junto a limitaciones presupuestarias, plantean importantes desafíos en esta labor.
		5	J-5	Que la palabra tecnología, virtual o medios no se menciona, y si bien el más cercano a una estafa cibernética, sería la sustracción de datos de tarjetas; esta solo abarca un supuesto de los variados que hay.
		6	F-1	Considero que los desafíos específicos en este caso, son la falta de una prescripción más clara, que contenga más supuestos que puedan abarcar todos los hechos delictivos que se cometen en el plano de la realidad.
		7	F-2	La interpretación y aplicación del artículo 196-A del Código Penal en casos de fraude cibernético presenta varios desafíos específicos. Algunos de ellos son: I. Prueba digital: En los casos de estafa cibernética, la prueba es principalmente digital,

				lo que puede presentar problemas en términos de autenticidad, integridad y admisibilidad de la prueba digital en los tribunales. II.Capacidad técnica: La complejidad técnica de algunas ciberestafas puede requerir conocimientos informáticos y de ciberseguridad especializados por parte de los jueces y fiscales que llevan estos casos. III.Falta de denuncia: Muchas víctimas de estafas cibernéticas no denuncian el delito por vergüenza, desconocimiento de los procedimientos legales o por creer que no se puede hacer nada, esto dificulta identificar a los perpetradores e investigar los casos.
		8	F-3	El Artículo N° 196-A del Código Penal peruano tipifica la estafa agravada, la estafa agravada se produce cuando una persona engaña a otra para que realice un acto jurídico que perjudique su patrimonio, obteniendo un provecho ilícito a cambio, pero no se encuentra regularizado las estafas cibernéticas en sí; por ende, es notoria la falta de regular los ciberdelitos en nuestro código penal.
		9	F-4	Ausencia de regulaciones en la publicidad engañosa: La falta de regulaciones claras en la publicidad engañosa puede permitir que las empresas hagan afirmaciones falsas o engañosas sobre sus productos o servicios. Esto dificulta que los consumidores puedan detectar y evitar ser víctimas de estafas o adquirir productos que no cumplen con lo prometido.
		10	F-5	El artículo 196-A del Código Penal se refiere a la tipificación de la estafa agravada en el ámbito cibernético. Básicamente, esto significa que se considerarán más graves los casos de estafa que involucren tecnología o medios electrónicos. La idea detrás de esta ley es proteger a las personas de aquellos individuos sin escrúpulos que utilizan la tecnología para engañar y robar información personal o dinero. Es importante tener en cuenta que cada país puede tener su propio conjunto de leyes y regulaciones relacionadas con la estafa cibernética.

	Resultados: Según los participantes, los principales desafíos en la aplicación del Art. 196-A en casos de estafa cibernética serian: - Falta de regulación específica para otros delitos cibernéticos. - Necesidad de actualización constante de la ley frente a avances tecnológicos. - Desafíos en la prueba digital (autenticidad y cadena de custodia). - Limitada capacidad técnica de jueces y fiscales para abordar casos complejos. - Falta de denuncias de las víctimas por vergüenza o desconocimiento. - Ausencia de precisiones sobre medios electrónicos. - Necesidad de cooperación entre sectores público, privado y empresas para prevenir delitos. - Interpretación de tipologías no expresamente reguladas.

Nota: Entrevista a especialistas.

Tabla 12

Interpretación de resultados del objetivo específico Nº 2

Objetivo Específico	Nº	Interpretación	Resultado
2. Determinar las principales deficiencias de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	4	De acuerdo al análisis de las respuestas de los entrevistados, se pueden resumir las siguientes fortalezas y limitaciones más recurrentes en la Ley de Delitos Cibernéticos en el Perú: Fortalezas: - Tipificación amplia de conductas y establecimiento de penas proporcionales. - Disposiciones para cooperación internacional. - Demuestra voluntad del Estado de abordar los delitos cibernéticos. Limitaciones: - Necesidad de mayor precisión y claridad en algunos aspectos de la ley. - Limitaciones en recursos, capacidades y concientización para investigar estos delitos. - Riesgo de desactualización ante la rápida evolución tecnológica. - Hace faltan fortalecer mecanismos de cooperación transfronteriza. - Se requiere agilizar procesos legales y judiciales relacionados. Hay consenso en que la ley presenta aciertos pero se deben superar limitaciones como falta de precisión, desactualización, agilización de procesos y fortalecimiento de capacidades.	El análisis destaca que la Ley de Delitos Cibernéticos presenta fortalezas, como su amplitud en la tipificación, pero también limitaciones que incluyen la necesidad de precisiones y recursos. En cuanto a la estafa cibernética, la ley se percibe como favorable, definición clara de elementos y penas proporcionales. El Artículo 196-A reconoce y penaliza la estafa cibernética con medidas más severas. No obstante, persisten desafíos, como la falta de regulación específica, la necesidad de
	5	Todas las respuestas coinciden en que la Ley N° 30096 favorece la persecución penal del delito de estafa cibernética, destacando los siguientes puntos: - Define los ciberdelitos, como el uso de medios electrónicos, el engaño y la obtención de beneficios económicos de forma fraudulenta.	

		- Establece penas y sanciones proporcionales para este tipo de ilícitos. - Sirve de complemento legal para tipificar correctamente la conducta como estafa cibernética. - Regula medidas de investigación como recolección de pruebas digitales y cooperación internacional, lo cual es clave para perseguir este delito. - Provee un marco normativo que permite enfrentar este problema tan común en la actualidad. - Define de manera amplia los ciberdelitos, incluyendo específicamente la estafa digital.	actualización y limitaciones en la presentación de pruebas digitales
	6	El artículo 196-A del Código Penal peruano reconoce y tipifica la estafa cibernética como una variante moderna de la estafa, utilizando medios digitales. Esta disposición aborda el uso de sistemas informáticos, redes e Internet para cometer el delito, incluyendo casos como la suplantación de entidades en línea para robar datos. Asimismo, establece penas más severas para la estafa agravada cometida electrónicamente, con el objetivo de proteger a las víctimas de este fraude digital. Se aplica cuando individuos emplean tecnología para engañar y obtener ganancias económicas, reconociendo el agravante por el uso de herramientas tecnológicas con fines lucrativos.	
	7	Los Principales desafíos en la aplicación del Art. 196-A en casos de estafa cibernética: - Falta de regulación específica para otros delitos cibernéticos. - Necesidad de actualización constante de la ley frente a avances tecnológicos. - Desafíos en la prueba digital (autenticidad y cadena de custodia). - Limitada capacidad técnica de	

	jueces y fiscales para abordar casos complejos. - Falta de denuncias de las víctimas por vergüenza o desconocimiento. - Ausencia de precisiones sobre medios electrónicos. - Necesidad de cooperación entre sectores público, privado y empresas para prevenir delitos. Interpretación de tipologías no expresamente reguladas.	

Nota: Resultados de las tablas 8, 9,10 y 11.

Interpretación y discusión del objetivo específico 2:

En relación al segundo objetivo específico, que buscaba determinar las principales deficiencias de la legislación persecutoria del delito de estafa cibernética, se identificaron fortalezas y limitaciones en la Ley de Delitos Cibernéticos (Ley N° 30096). Según los entrevistados, la Ley de Delitos Cibernéticos presenta aciertos notables, como la amplitud en la tipificación de delitos y la imposición de penas proporcionales. Sin embargo, a pesar de estos avances legislativos, según señala Mayer et al. (2020) se observa un continuo aumento de ciberdelitos y cibercrimen. Sumado a que la globalización y la sofisticación de los sistemas de tecnología de la información dificultan la captura de ciberdelincuentes, algunos argumentan que las sanciones actuales carecen de la severidad necesaria para disuadir eficazmente (Smith-Ditizio y Smith, 2017).

En relación con la estafa cibernética, los entrevistados señalaron la existencia de limitaciones, especialmente en la necesidad de una mayor precisión en la norma para su tipificación. Actualmente, este delito es tratado como estafa con agravantes. El Informe situacional de cibercriminalidad de la Defensoría del Pueblo (2023) refleja esta distinción al clasificar la estafa como un ciberdelito contra el patrimonio, específicamente en su forma agravada, regulada por el artículo 196-A, numeral 5. Esta variante se materializa cuando el autor utiliza el engaño para acceder a información de tarjetas de ahorro o crédito con el objetivo de obtener ganancias ilegítimas a expensas de terceros.

Los entrevistados también expresaron preocupaciones sobre otros desafíos, como los problemas en materia probatoria digital, como también limitaciones técnicas por parte de jueces y fiscales, así como la escasa presentación de denuncias. Esta postura concuerda con el informe de la Defensoría del Pueblo (2023), que destaca que las licencias de equipos y software de la DIVINDAT-PNP para la recopilación, análisis y procesamiento de evidencia digital no se renuevan adecuadamente. Además, los trámites para levantar el secreto bancario y de comunicaciones llevan más de dos meses. También se resalta que la DIVINDAT–PNP carece de personal capacitado y en cantidad suficiente para abordar la cibercriminalidad, y no cuenta

con un presupuesto específico para mantener e implementar herramientas tecnológicas.

En síntesis si bien la normativa presenta avances reconociendo conductas como la estafa cibernética, todavía persisten deficiencias que dificultan su aplicación efectiva en un contexto de constante cambio tecnológico. Se requiere mejorar la precisión y actualización permanente de la ley, así como fortalecer capacidades investigativas para garantizar una adecuada persecución de este ilícito.

Resultados según el objetivo específico 3*):* Determinar los efectos de la insuficiente legislación persecutoria en la detección del delito de estafa cibernética en el distrito fiscal del Santa, 2022.

Tabla 13

Detección del delito.

	Interrogante	Nº	Entrevistado	Respuesta
Pregunta Nº 08	Como especialista en derecho procesal penal, ¿cómo considera que la insuficiente legislación ha afectado la detección de casos de estafa cibernética en el Distrito Fiscal del Santa?	1	J-1	Los procesos son más tediosos de lo común y algunos otros solo crean carga procesal por falta de fundamentos de derecho que apoyen normativamente su denuncia interpuesta.
		2	J-2	La falta de más intervención del convenio de Budapest en nuestra ley 30096 nos mantiene en un límite y sin avanzar, lo cual al ser carentes de tantos hechos, términos y penas no permite que varios hechos delictivos reciban castigo alguno.
		3	J-3	La detección del fraude cibernético y otros delitos cibernéticos se ven afectados debido a la impunidad que puede aparecer en favor del delincuente. Por lo tanto, es importante que el nuestro país cuente con leyes claras y actualizadas que aborden los desafíos de la era digital y permitan la detección y sanción de los delitos cibernéticos.
		4	J-4	En ausencia de normas claras sobre la obligación de denunciar el fraude cibernético, muchas víctimas optan por no denunciar el delito, por temor a represalias o porque no saben a quién acudir si están siendo estafadas en línea.
		5	J-5	Considero que con la insuficiente legislación no somos capaces de lograr avanzar junto con la necesidad actual que se debe de cumplir para poder castigar los delitos cibernéticos.
		6	F-1	La falta de regulación adecuada en diferentes ámbitos de la tecnología dificulta la detección oportuna de delitos y actividades ilícitas que se desarrollar en el mundo cibernético.
		7	F-2	La falta de normativa específica y actualizada sobre delitos cibernéticos dificulta perseguir y

				sancionar eficazmente este tipo de delitos. En primer lugar, es posible que la legislación existente no aborde adecuadamente las particularidades del delito cibernético, lo que dificulta su identificación y procesamiento; los ciberdelincuentes utilizan técnicas sofisticadas y herramientas digitales para ocultar su identidad y cometer estafas, lo que requiere un marco legal sólido y actualizado. En segundo lugar, la falta de formación adecuada en estos temas por parte de los operadores de justicia, como fiscales y jueces, también afecta la detección de casos de fraude cibernético, una investigación eficaz requiere conocimientos especializados en tecnologías de la información, informática forense y técnicas de investigación digital; además, la falta de recursos específicamente dedicados a combatir el cibercrimen es otro obstáculo; y es que la adquisición de herramientas tecnológicas y la capacitación del personal puede resultar costosa, pero son esenciales para abordar la complejidad de los casos de fraude cibernético.
			8	F-3	Como especialista en derecho procesal penal, considero que la insuficiente legislación se afecta la detección de casos de la siguiente manera: No permite la celeridad en los procesos a llevar, provoca estancamiento y los únicos finales para algunos casos solo parece la nulidad o archivamiento.
			9	F-4	Las leyes no se adaptan a los avances tecnológicos y no contemplan adecuadamente los delitos informáticos, y esto provoca lagunas legales que permitan a los delincuentes evadir la justicia. Además, la falta de educación o de conciencia sobre los riesgos y medidas de seguridad, por parte de los habitantes del Santa, en el uso de tecnologías de la información expone a las personas.
			10	F-5	Una legislación insuficiente en materia de estafa cibernética puede dificultar la detección de estos casos de varias formas. Por ejemplo, si las leyes no definen claramente los delitos

				cibernéticos y no establecen las penas correspondientes, puede ser difícil para los investigadores y fiscales procesar a los infractores de manera efectiva. Además, una legislación débil puede no proporcionar las herramientas necesarias para llevar a cabo investigaciones y recopilar pruebas adecuadas en casos de estafa cibernética. Esto puede limitar las capacidades de las autoridades para rastrear a los perpetradores, identificar sus métodos y asegurar las pruebas necesarias para llevarlos ante la justicia.

Resultados: De acuerdo a las respuestas brindadas por los especialistas entrevistados, la insuficiente legislación ha afectado negativamente la detección de casos de estafa cibernética en el Distrito Fiscal de Santa de la siguiente manera:

En primer lugar, señalaron que la legislación vigente no contempla adecuadamente las particularidades de los delitos cibernéticos, como sus diversas técnicas sofisticadas y el uso de herramientas digitales.

Asimismo, la ausencia de normas claras que definan taxativamente los delitos cibernéticos y establezcan las penas correspondientes deriva, según los expertos, en vacíos legales que dejan espacios de impunidad. Lo que dificulta el procesamiento efectivo de los infractores por parte de fiscales y jueces.

Otro punto es la deficiente cooperación internacional ante la no adopción de convenios relevantes como el de Budapest, lo que limita el intercambio de información necesario para investigar delitos transfronterizos.

También mencionan las limitaciones en capacidades de investigación digital forense, recolección de pruebas electrónicas y falta de recursos especializados. Así como la escasa formación de operadores de justicia en materia cibernética.

Por otro lado, la población adolece de cultura de seguridad digital y concientización sobre riesgos, lo que expone su vulnerabilidad.

En definitiva, la insuficiente legislación genera falta de agilidad procesal, estancamiento y hasta archivo de casos por falta de sustento legal, según los especialistas consultados. Lo que evidencia la necesidad de actualizar la legislación ante los nuevos desafíos del delito cibernético.

Nota: Entrevistas aplicadas a los especialistas.

Tabla 14

Falta de regulación para la detección del delito de estafa cibernética

	Interrogante	Nº	Entrevistado	Respuesta
Pregunta Nª 09	Podría proporcionar ejemplos de situaciones donde se evidencie que la falta de regulación adecuada dificultó la detección oportuna de este delito	1	J-1	Poca colaboración entre jurisdicciones: Falta de cooperación puede dejar delitos sin detección o investigación. Falta de regulación en video vigilancia: Normativas vagas dificultan obtener evidencia visual para autoridades.
		2	J-2	Un señor estafado con una IA que se hacía pasar su madre que vive en otro país, pero como identificar al autor del delito si está bajo otra jurisdicción. Por otro lado, un término no precisado en la legislación causa confusión que solo hace más tedioso el proceso y causa la dificultad de tener que recién interpretar un término que muy posiblemente se evitaría con una correcta legislación.
		3	J-3	Ejemplo 1, el querer manipular la página para descubrir pistas dentro del software o base de datos, pero a falta de personal capacitado, no se podrá ingresar y se tendrá que optar por otras opciones más tediosas. Ejemplo 2, a una señora le siguen llegando mensajes de estafadores por más que ya bloqueo varias cuentas estas siguen apareciendo y no hay medida alguna para protegerla de esto.
		4	J-4	-Falta de regulación en la protección de datos: Si no existen leyes claras y rigurosas que regulen la protección de datos personales en línea, los delincuentes pueden acceder a información confidencial sin ser detectados fácilmente. Esto puede incluir robos de identidad, fraudes financieros y estafas en línea. -Falta de regulación en la seguridad de las transacciones electrónicas: Si no hay reglas claras para garantizar la seguridad de las transacciones en línea, como el uso de certificados de seguridad y protocolos de encriptación, los delincuentes pueden aprovecharse de las vulnerabilidades de seguridad para llevar a cabo fraudes y robo de

			información financiera.
		5	J-5	-El caso de personas comunicándose con individuos que se hacen pasar por otras personas a través de la página “Facebook” y atrayéndolos con mentiras: a falta de una ley o artículo que logre inhabilitar la cuenta de estas personas para que no puedan ingresar a redes y sigan cometiendo sus atrocidades, parece imposible. -Las Estafas realizadas en las actuales redes más concurridas por la actual sociedad; como en “Tik tok” o “Instagram"; ya sea por ventas u ofertas laborales que son los temas de estafa más conocidos en redes.
		6	F-1	-A. Falla en la regulación de las redes sociales: Sin una regulación adecuada, las redes sociales pueden convertirse en un paraíso para los delincuentes que buscan cometer fraudes o acosar a otros usuarios. En ausencia de reglas claras y mecanismos de denuncia efectivos, puede resultar difícil detectar y abordar estas actividades delictivas de manera oportuna. -Falta de regulación en la protección de datos personales: La falta de regulaciones efectivas en la protección de datos personales puede facilitar el robo de información y la realización de actividades ilícitas como el phishing o el fraude de identidad. Sin una regulación adecuada que exija a las empresas salvaguardar la privacidad de los datos de los usuarios, se dificulta la detección y prevención de estos delitos.
		7	F-2	Ejemplo 1: La señora Martínez cayó en una estafa cibernética al proporcionar datos bancarios en respuesta a un falso mensaje del banco. La falta de regulación adecuada dificultó que la policía persiguiera a los estafadores que operaban desde otro país. Ejemplo 2: Buscando empleo, el señor Rodríguez fue estafado al invertir dinero para asegurar un supuesto puesto laboral. Aunque denunció el caso, la falta de rastros de los estafadores y la ausencia de normativas efectivas llevaron al archivo del caso por parte

				de las autoridades.
		8	F-3	Primero, el phishing, táctica cibernética que engaña a las personas para obtener datos confidenciales, carece de regulación efectiva, ya que las víctimas pueden no ser conscientes de cómo sus datos están en riesgo, dificultando la identificación y denuncia de estas actividades fraudulentas. Segundo, la falta de regulación clara en el uso de criptomonedas complica la detección de delitos de lavado de dinero. La anonimidad que ofrecen estas monedas facilita a los ciberdelincuentes realizar transacciones ilegales sin rastreo. La ausencia de directrices claras dificulta los esfuerzos de las autoridades para investigar y prevenir estos delitos.
		9	F-4	-Ausencia de regulaciones en la publicidad engañosa: La falta de regulaciones claras en la publicidad engañosa puede permitir que las empresas hagan afirmaciones falsas o engañosas sobre sus productos o servicios. Esto dificulta que los consumidores puedan detectar y evitar ser víctimas de estafas o adquirir productos que no cumplen con lo prometido.
		10	F-5	- En algunos casos, las empresas no tienen la obligación legal de informar a sus clientes sobre violaciones de seguridad o brechas de datos. Esto significa que, aunque puedan detectar estas violaciones internamente, no están obligados a tomar medidas para remediar el problema e informar a las autoridades relevantes y a los clientes que se han visto afectados. -Las autoridades pueden tener dificultades para investigar y procesar casos de estafas en línea. Por ejemplo, pueden enfrentar desafíos para obtener pruebas forenses digitales necesarias para llevar a cabo una investigación efectiva o para cooperar con otras agencias encargadas de hacer cumplir la ley en otros países.

	Resultados : Los operadores judiciales entrevistados refieren que la falta de regulación adecuada dificultó la detección oportuna de este delito de estafa cibernética, por: Falta de cooperación e intercambio de información entre distintas jurisdicciones dificulta la detección y persecución de delitos cibernéticos que involucran más de un país. Normativas vagas o falta de regulación específica en áreas como protección de datos, seguridad en transacciones, redes sociales, publicidad, uso de criptomonedas, permite que delincuentes operen con mayor facilidad y escapen de la detección. Ausencia de obligaciones claras de parte de empresas para reportar brechas de seguridad o violaciones y cooperar con autoridades. Dificultades para las autoridades en obtener pruebas digitales forenses necesarias cuando existe anonimato o falta de regulación en tecnologías/plataformas involucradas. Términos imprecisos en legislación generan confusión e interpretaciones que dilatan procesos. Falta de capacitación o recursos para que autoridades puedan investigar de manera efectiva en entornos digitales.

Nota: Entrevistas aplicadas a los especialistas.

Tabla 15

Resultados de las carpetas fiscales revisadas mediante la guía de análisis documental, enfocado en la 'detección' del delito de estafa cibernética.

Objetivo específico 3)	Nº de carpeta	Código de carpeta fiscal	Ítems	Calificación		Interpretación
				Si	No	
Determinar los efectos de la insuficiente legislación persecutoria en la ***detección*** del delito de estafa cibernética en el distrito fiscal del Santa, 2022**.**	1	**CF-1**	1)	X		
			2)	X		
			3)		X	
			4)		X	
	2	**CF-2**	1)	X		
			2)	X		
			3)		X	
			4)		X	
	3	**CF-3**	1)	X		
			2)	X		
			3)		X	
			4)		X	
	4	**CF-4**	1)	X		
			2)	X		
			3)		X	
			4)		X	
	5	**CF-5**	1)	X		
			2)	X		
			3)	X		
			4)		X	
	6	**CF-6**	1)	X		
			2)	X		
			3)		X	
			4)		X	
	7	**CF-7**	1)	X		
			2)	X		
			3)		X	
			4)		X	
	8	**CF-8**	1)	X		
			2)	X		
			3)		X	
			4)		X	
	9	**CF-9**	1)	X		
			2)	X		
			3)	X		

		4)		X	
10	**CF-10**	1)	X		
		2)	X		
		3)		X	
		4)		X	
11	**CF-11**	1)	X		
		2)	X		
		3)		X	
		4)		X	
12	**CF-12**	1)	X		
		2)	X		
		3)		X	
		4)		X	

Resultados: En cuanto a la descripción de cómo se detectó el delito, se observa que en el 100% de las carpetas fiscales (12 de 12) se detallan los hechos de detección.

Con respecto a si mencionan las fuentes de información y dispositivos tecnológicos utilizados, en el 100% (12 de 12) se evidencia que sí abordan esta información.

En relación con el detalle de los actores clave en la fase de detección, se observa que el 83% (10 de 12) no especifica los actores y sus roles, mientras que solo el 17% (2 de 12) lo aborda.

Finalmente, en lo que respecta a la descripción de la colaboración interinstitucional en la etapa de detección, se observa que en el 100% de las carpetas fiscales (12 de 12) no proporcionan información sobre la colaboración entre instituciones en esta fase

Nota: Guía de análisis documental.

Especificaciones

ítems	**Subcategoría: Detección**
1	El expediente describe cómo se detectó el delito (hechos)
2	Menciona las fuentes de información y dispositivos tecnológicos utilizados para la detección.
3	Se detallan los actores clave en la fase de detección, indicando su papel.
4	Describe la colaboración interinstitucional en la etapa de detección

Tabla 16

Interpretación de resultados del objetivo específico Nº 3

Objetivo Especifico 3)	Nº	Interpretación	Resultados
Determinar los efectos de la insuficiente legislación persecutoria en la detección del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	8	De acuerdo a las respuestas brindadas por los especialistas entrevistados, la insuficiente legislación ha afectado negativamente la detección de casos de estafa cibernética en el Distrito Fiscal de Santa de la siguiente manera: En primer lugar, señalaron que la legislación vigente no contempla adecuadamente las particularidades de los delitos cibernéticos, como sus diversas técnicas sofisticadas y el uso de herramientas digitales. Asimismo, la ausencia de normas claras que definan taxativamente los delitos cibernéticos y establezcan las penas correspondientes deriva, según los expertos, en vacíos legales que dejan espacios de impunidad. Lo que dificulta el procesamiento efectivo de los infractores por parte de fiscales y jueces. Otro punto es la deficiente cooperación internacional ante la no adopción de convenios relevantes como el de Budapest, lo que limita el intercambio de información necesario para investigar delitos transfronterizos. También mencionan las limitaciones en capacidades de investigación digital forense, recolección de pruebas electrónicas y falta de recursos especializados. Así como la escasa formación de operadores de justicia en materia cibernética. Por otro lado, la población adolece de cultura de seguridad digital y concientización sobre riesgos, lo que expone su vulnerabilidad.	De acuerdo al objetivo específico planteado, los resultados obtenidos a través de las entrevistas realizadas a especialistas y el análisis de carpetas fiscales permiten concluir lo siguiente: La insuficiente legislación persecutoria ha afectado negativamente la detección de casos de estafa cibernética en el Distrito Fiscal de Santa, generando una serie de limitaciones como: - Normas que no contemplan adecuadamente las particularidades del delito cibernético de estafa.

		En definitiva, la insuficiente legislación genera falta de agilidad procesal, estancamiento y hasta archivo de casos por falta de sustento legal, según los especialistas consultados. Lo que evidencia la necesidad de actualizar la legislación ante los nuevos desafíos del delito cibernético.	- Vacíos legales que dejan espacios de impunidad y dificultan el procesamiento de los infractores.
	9	Los operadores judiciales entrevistados refieren que la falta de regulación adecuada dificultó la detección oportuna de este delito de estafa cibernética, por: - Falta de cooperación e intercambio de información entre distintas jurisdicciones dificulta la detección y persecución de delitos cibernéticos que involucran más de un país. - Normativas vagas o falta de regulación específica en áreas como protección de datos, seguridad en transacciones, redes sociales, publicidad, uso de criptomonedas, permite que delincuentes operen con mayor facilidad y escapen de la detección. - Ausencia de obligaciones claras de parte de empresas para reportar brechas de seguridad o violaciones y cooperar con autoridades. - Dificultades para las autoridades en obtener pruebas digitales forenses necesarias cuando existe anonimato o falta de regulación en tecnologías/plataformas involucradas. - Términos imprecisos en legislación generan confusión e interpretaciones que dilatan procesos. Falta de capacitación o recursos para que autoridades puedan investigar de manera efectiva en entornos digitales.	- Deficiente cooperación internacional por falta de adopción de convenios. - Limitadas capacidades de investigación digital, recolección de pruebas electrónicas y recursos especializados. - Escasa formación de operadores de justicia en materia cibernética. - Vulnerabilidad de la población por baja cultura de seguridad

			digital. - Falta de agilidad procesal e incluso archivo de causas.
12 Carpetas	En cuanto a la descripción de cómo se detectó el delito, se observa que en el 100% de las carpetas fiscales (12 de 12) se detallan los hechos de detección. Con respecto a si mencionan las fuentes de información y dispositivos tecnológicos utilizados, en el 100% (12 de 12) se evidencia que sí abordan esta información. En relación con el detalle de los actores clave en la fase de detección, se observa que el 83% (10 de 12) no especifica los actores y sus roles, mientras que solo el 17% (2 de 12) lo aborda. Finalmente, en lo que respecta a la descripción de la colaboración interinstitucional en la etapa de detección, se observa que en el 100% de las carpetas fiscales (12 de 12) no proporcionan información sobre la colaboración entre instituciones en esta fase.	A nivel de carpetas fiscales, si bien se describen adecuadamente los hechos y pruebas, en la mayoría no se especifican actores ni roles involucrados, y en ninguna la colaboración interinstitucional. Por lo expuesto, se evidencia la necesidad de actualizar la legislación para enfrentar los desafíos del delito cibernético y mejorar la detección de estas estafas.

Nota: Resultados de las tablas 13,14 y 15.

Interpretación y discusión del objetivo específico 3:

El tercer objetivo específico abordó los efectos de la insuficiente legislación persecutoria en la detección del delito de estafa cibernética, los resultados obtenidos a través de entrevistas a especialistas y el análisis de carpetas fiscales arrojaron conclusiones reveladoras.

Según los especialistas consultados, la insuficiente legislación ha impactado negativamente la detección de casos de estafa cibernética en varias dimensiones. En primer lugar, los entrevistados destacaron que la legislación vigente no aborda adecuadamente las particularidades de los delitos cibernéticos, incluyendo sus técnicas sofisticadas y el uso de herramientas digitales. Este hallazgo coincide con el estudio de Quevedo (2017), quien concluyó que la persecución de estos delitos requiere un profundo entendimiento de las técnicas fundamentales relacionadas con la tecnología de la información, sumado a la ausencia de normas claras y taxativas en la definición de delitos cibernéticos crea vacíos legales, dificultando el procesamiento efectivo de infractores.

En esa línea, los especialistas destacaron las limitaciones en las capacidades de investigación digital, la recolección de pruebas electrónicas y la falta de recursos especializados. Se identificó la escasa formación de operadores de justicia en materia cibernética y la baja cultura de seguridad digital en la población como factores que contribuyen a la vulnerabilidad ante la estafa cibernética. Por lo tanto, según Alonso y Esparza (2017), es fundamental contar con personal experto y las herramientas tecnológicas adecuadas para la efectiva persecución de estos delitos.

En términos procesales, la falta de agilidad procesal, estancamiento y archivo de casos debido a la falta de sustento legal fueron subrayados como problemas recurrentes. La ausencia de especificaciones en actores y roles involucrados en las carpetas fiscales, así como la falta de colaboración interinstitucional, evidencian la necesidad de mejorar la cooperación y coordinación en la detección y persecución de casos de estafa cibernética.

También sostuvieron que la falta de cooperación e intercambio de información entre jurisdicciones, normativas vagas o la ausencia de regulación específica en diversas áreas, junto con la falta de obligaciones claras por parte de las empresas, fueron resaltadas como obstáculos clave. En respuesta a esta problemática, Avalos (2021) propuso establecer acuerdos estratégicos con empresas proveedoras de servicios tecnológicos y entidades bancarias y financieras para mejorar la investigación fiscal. Asimismo, consideró importante adecuar la legislación peruana al Convenio de Budapest en este campo en específico.

En el análisis de carpetas fiscales, se destaca una consistencia en la descripción de los hechos, las fuentes de información y los dispositivos tecnológicos utilizados. Sin embargo, se identificaron deficiencias significativas, como la falta de especificación de actores clave y la ausencia de detalles sobre la colaboración interinstitucional, aspectos que podrían tener un impacto negativo en los esfuerzos de detección y persecución. La falta de identificación completa de los actores se atribuye a la naturaleza virtual de muchos delitos cibernéticos, según señala Sain (2018), donde la simulación o suplantación en el entorno digital dificulta la atribución de responsabilidades.

Resultados según el objetivo específico 4): Determinar los efectos de la insuficiente legislación persecutoria en la investigación del delito de estafa cibernética en el distrito fiscal del Santa, 2022

Tabla 17

Sanción del delito de estafa cibernética

	Interrogante	Nº	Entrevistado	Respuesta
Pregunta Nª 10	¿Cuáles considera que son los retos específicos que ha enfrentado en la investigación de estos delitos debido a la insuficiente legislación?	1	J-1	Los desafíos en el ámbito legal y de capacitación: Cambios tecnológicos rápidos: Desafían la efectividad del marco legal actual. Falta de capacitación: Sin personal preparado, las investigaciones se retrasan o frustran.
		2	J-2	Uno el fraude cibernético, la falta de una regulación adecuada ha dificultado la identificación a tiempo de este delito, que las autoridades de diferentes países cooperen en la investigación y el procesamiento de delincuentes. Y la falta de acuerdos y marcos legales claros puede obstaculizar la capacidad de las autoridades para obtener o entregar pruebas. Dos, falta de expertos capacitados, la investigación de delitos cibernéticos requiere expertos con conocimientos técnicos y capacidad para monitorear la actividad en línea y analizar datos digitales.
		3	J-3	Ejemplo 1, el querer manipular la página para descubrir pistas dentro del software o base de datos, pero a falta de personal capacitado, no se podrá ingresar y se tendrá que optar por otras opciones más tediosas. Ejemplo 2, a una señora le siguen llegando mensajes de estafadores por más que ya bloqueo varias cuentas estas siguen apareciendo y no hay medida alguna para protegerla de esto.
		4	J-4	La falta de medidas realmente efectivas para evitar que la víctima sufra las consecuencias de un delito cibernético. Y falta de capacitación en las herramientas tecnológicas, haciendo referencia a los saberes además de los más básicos.
		5	J-5	La falta de regulación respecto a la sanción para quienes cometieron delitos cibernéticos podría abordarse con la prohibición permanente de su acceso a estas redes. Además, la identificación de

			la prueba del delito enfrenta desafíos debido a la falta de una definición clara, lo que podría generar confusión en el proceso.
		6	F-1	La naturaleza internacional de los delitos cibernéticos representa un desafío importante, los ciberdelincuentes pueden operar desde cualquier parte del mundo y aprovechar las diferencias jurisdiccionales para evadir la responsabilidad, y la falta de un marco legal armonizado entre países dificulta la cooperación internacional y ralentiza el proceso de investigación y enjuiciamiento.
		7	F-2	Uno de ellos es la falta de legislación específica y actualizada que aborde adecuadamente el ciberdelito; en muchos casos, las leyes existentes no tienen en cuenta los avances tecnológicos y las nuevas formas de delinquir en el entorno digital, lo que dificulta procesar y sancionar a los responsables. También, la falta de recursos y capacitación especializada en materia de investigación de delitos cibernéticos también representa un desafío, la tecnología avanza rápidamente y los delincuentes se adaptan constantemente, por lo que es necesario contar con personal y equipos capacitados para hacer frente a estas amenazas; sin embargo, en muchos casos, la capacitación y los recursos son limitados, lo que dificulta la recopilación de pruebas y la identificación de los responsables.
		8	F-3	En primer lugar considero la velocidad a la que evoluciona la tecnología y los métodos utilizados por los ciberdelincuentes superan con creces la capacidad de las leyes existentes para mantenerse actualizadas. La falta de legislación específica y adecuada para abordar los nuevos tipos de delitos cibernéticos dificulta la investigación y el enjuiciamiento de los responsables. Los investigadores se enfrentan a un terreno legal incierto y a menudo deben adaptar interpretaciones legales existentes para aplicarlas a situaciones nuevas y complejas.
		9	F-4	La recopilación y preservación de pruebas digitales es un reto significativo, puesto que los datos electrónicos pueden ser fácilmente modificados o eliminados, lo que dificulta la obtención de pruebas sólidas. Además, la insuficiente legislación en cuanto a los estándares y procedimientos para la recopilación y

			adquisición de pruebas digitales puede poner en peligro la integridad de la evidencia y debilitar los casos contra los ciberdelincuentes.
	10	F-5	Primero, la ambigüedad en la definición de delitos cibernéticos dificulta la investigación y procesamiento al carecer de una base legal sólida, lo que complica establecer qué acciones son ilegales y cómo abordarlas. Segundo, la jurisdicción cruzada en delitos cibernéticos, con actores ubicados en diferentes jurisdicciones, presenta obstáculos para la investigación. La falta de acuerdos internacionales sólidos y marcos legales claros complica la coordinación entre investigadores y agencias en otros países. Tercero, la cooperación con proveedores de servicios en línea se ve obstaculizada por la falta de regulaciones claras sobre cómo deben colaborar con las autoridades y preservar la privacidad de los usuarios.
Resultados: Los operadores judiciales señalan como principal reto la rápida evolución tecnológica y cambios en las modalidades delictivas, que exceden la capacidad de las leyes de actualizarse a dichos avances. Otro desafío radica en la falta de legislación específica que aborde adecuadamente nuevos delitos digitales, generando vacíos legales. También presenta dificultades la ambigüedad en la definición legal de ciberdelitos, obstaculizando el procesamiento penal por carecer de base legal clara. Un problema relevante lo constituye la recopilación y preservación de pruebas digitales, que pueden ser fácilmente alteradas u borradas. La jurisdicción transfronteriza dificulta la cooperación internacional, ante la falta de acuerdos legales armonizados. Los investigadores enfrentan limitaciones por la escasez de recursos, capacitación y experticia especializada para estos casos. La cooperación con proveedores online también se ve entorpecida por ausencia de normas claras sobre colaboración con justicia respetando privacidad.			

Fuente: Entrevistas aplicadas a los especialistas.

Tabla 18

Obstáculos en la" investigación" del delito de estafa cibernética

	Interrogante	Nº	Entrevistado	Respuesta
Pregunta Nº 11	Proporcione ejemplos de obstáculos que ha encontrado en la recopilación de pruebas o en la identificación de los autores de estafas cibernéticas en su jurisdicción.	1	J-1	Desafíos en ciberseguridad: Tecnologías avanzadas de hacking: Ciberdelincuentes emplean tácticas avanzadas para ocultar sus actividades, complicando la obtención de pruebas forenses digitales. Comunicaciones encriptados: El uso de encriptación en transacciones y comunicaciones dificulta el acceso a información relevante, permitiendo a los delincuentes evadir fácilmente rastros digitales identificables.
		2	J-2	Falta de conciencia y capacitación: La falta de conocimiento y capacitación adecuada en las fuerzas encargadas de hacer cumplir la ley puede ser un obstáculo importante, los investigadores enfrentan dificultades para comprender y seguir las pistas digitales, lo que retrasa la recopilación de pruebas y la identificación de los responsables.
		3	J-3	-Falta de tecnología necesaria para lograr localizar al sujeto que cometió el acto delictivo. -Falta de personal especializado en la cibernética, la materia por no decir todos apenas podemos manejar sistemas simples.
		4	J-4	-Anonimato en línea: Los delincuentes cibernéticos pueden ocultar su identidad utilizando técnicas como el uso de redes privadas virtuales (VPN), servidores proxy u otras herramientas para enmascarar su dirección IP. Esto dificulta la tarea de rastrear la ubicación real del autor de la estafa. -Jurisdicción y cooperación internacional limitada: Las estafas cibernéticas pueden cruzar fronteras, lo que puede complicar la jurisdicción y la cooperación entre países, siendo posible que la jurisdicción de un país no cubra a los delincuentes que operan desde otro país, lo que dificulta la persecución legal efectiva.
		5	J-5	El anonimato representa un obstáculo al permitir a individuos participar en actividades sin revelar su identidad, facilitado por técnicas como servidores

			proxy utilizadas por ciberdelincuentes para ocultarse. La atribución, otro desafío, busca identificar al responsable del delito cibernético. El uso de herramientas que mejoran el anonimato complica la identificación de dispositivos y personas involucradas en el ciberdelito. Además, desafíos técnicos como sistemas operativos y software propietarios requieren herramientas especializadas para la identificación y preservación de evidencia digital. La falta de equipo y herramientas forenses digitales adecuadas limita la capacidad de los investigadores para llevar a cabo investigaciones de delitos cibernéticos en dispositivos digitales.
		6	F-1	Tenemos, la identificación de los autores de estafas cibernéticas y la recopilación de pruebas, la dificultad para rastrear a través de fronteras, la eliminación de pruebas digitales y los desafíos relacionados con la jurisdicción y la atribución. Estos obstáculos requieren una mayor cooperación internacional y marcos legales actualizados que aborden específicamente estos problemas en el ámbito de los delitos cibernéticos.
		7	F-2	-La dificultad para rastrear las transacciones financieras realizadas a través de medios electrónicos, los estafadores suelen utilizar métodos sofisticados para ocultar su identidad y el origen del dinero, lo que dificulta seguir el rastro del flujo de fondos. -La falta de colaboración de proveedores de servicios en línea y plataformas tecnológicas, para obtener pruebas sólidas, necesitamos acceder a información almacenada en servidores o cuentas de usuarios, pero nos encontramos con trabas legales y burocráticas que limitan nuestro acceso a esta información; además, algunas plataformas se muestran reticentes a colaborar o no tienen los mecanismos adecuados para compartir información de manera eficiente.
		8	F-3	-Uso de tecnologías ocultas; es decir, los perpetradores de estafas cibernéticas suelen utilizar tecnologías como la red oscura (dark web) y servicios para ocultar sus identidades y ubicaciones, esto crea dificultades en la labor de

			rastreo e identificación de los responsables, ya que sus actividades ilegales están protegidas por capas de anonimato. - Rastreo a través de fronteras; las estafas cibernéticas son a menudo realizadas desde diferentes partes del mundo, aprovechando las lagunas en la cooperación internacional.
	9	F-4	-Tenemos lo que son la: tecnología avanzada, los estafadores cibernéticos a menudo utilizan herramientas y técnicas sofisticadas; falta de cooperación, la falta de cooperación entre los proveedores de servicios en línea, y cambio de identidad, algunos estafadores cibernéticos pueden utilizar identidades falsas.
	10	F-5	Jurisdicciones Múltiples: Las estafas cibernéticas pueden abarcar diversas jurisdicciones, dificultando la identificación y persecución de los responsables. Tecnologías de Cifrado: Estafas cibernéticas que involucran comunicaciones cifradas complican la interceptación y seguimiento por parte de investigadores. Métodos criptográficos sólidos obstaculizan el acceso a información esencial para identificar a los responsables. Transacciones Financieras Complejas: Estafadores recurren a sistemas de pago alternativos o criptomonedas, dificultando el seguimiento del flujo de dinero y la identificación de destinatarios finales.
Resultados: Los principales obstáculos que los operadores judiciales han encontrado en la recopilación de pruebas y la identificación de autores de estafas cibernéticas en su jurisdicción, según lo expuesto, incluyen el uso de tecnologías de ocultamiento por parte de los delincuentes como VPNs, proxy y dark web, lo que dificulta el rastreo de IPs y ubicaciones. Asimismo, se presenta el anonimato online a través de diversas herramientas, así como la falta de cooperación entre proveedores para acceder a información almacenada y limitaciones en el rastreo transfronterizo. También el uso de cifrado y métodos criptográficos sofisticados que obstaculizan la interceptación de comunicaciones, así como transacciones financieras complejas mediante sistemas de pago alternativos. Otros factores son la eliminación o modificación de evidencias digitales, limitaciones tecnológicas y escasez de personal especializado, sumado a las dificultades derivadas de la jurisdicción multifacética de estos delitos que abarcan varias regiones.		

Nota: Entrevistas aplicadas a los especialistas.

Tabla 19

Resultados de carpetas fiscales revisadas mediante la guía de análisis documental enfocado en la 'investigación' del delito de estafa cibernética.

Objetivo específico 4)	Nº de carpeta	Código de carpeta fiscal	Ítems	Calificación		Observaciones
				Si	No	
Determinar los efectos de la insuficiente legislación persecutoria en la ***investigación*** del delito de estafa cibernética en el distrito fiscal del Santa, 2022	1	**CF-1**	5)		X	
			6)		X	
			7)		X	
			8)		X	
	2	**CF-2**	5)	X		
			6)		X	
			7)	X		
			8)		X	
	3	**CF-3**	5)	X		
			6)		X	
			7)	X		
			8)		X	
	4	**CF-4**	5)		X	
			6)		X	
			7)	X		
			8)		X	
	5	**CF-5**	5)	X		
			6)	X		
			7)	X		
			8)	X		
	6	**CF-6**	5)	X		
			6)	X		
			7)	X		
			8)	X		
	7	**CF-7**	5)		X	
			6)		X	
			7)	X		
			8)		X	
	8	**CF-8**	5)		X	
			6)		X	
			7)	X		
			8)		X	
	9	**CF-9**	5)		X	
			6)		X	

		7)	X		
		8)		X	
10	**CF-10**	5)	X		
		6)		X	
		7)	X		
		8)		X	
11	**CF-11**	5)	X		
		6)		X	
		7)	X		
		8)		X	
12	**CF-12**	5)	X		
		6)	X		
		7)	X		
		8)	X		

Resultados: De la revisión de las 12 carpetas fiscales se revela que, en relación con la mencionada de los métodos de investigación empleados junto con su base legal (ítem 1), solo el 67% lo realiza de manera adecuada.

En cuanto a la inclusión de información sobre órdenes y autorizaciones judiciales requeridas (ítem 2), aunque el 75% lo aborda, aún queda un margen del 25% que no garantiza la legalidad de los procedimientos.

Aunque la gran mayoría, el 92%, detalla adecuadamente la evidencia reunida y su admisibilidad (ítem 3), el 8% que no lo hace podría deberse a precisiones legales pendientes.

En relación con la descripción de la preservación y manejo legal de la prueba (ítem 4), aunque el 75% cumple, el 25% restante deja dudas sobre el apego al marco jurídico durante la recolección.

Estos vacíos en la caracterización de aspectos fundamentales de la pesquisa, que en algunos ítems superan el 25%, evidencian la necesidad de fortalecer las directrices normativas para uniformar los criterios de investigación, especialmente en casos relacionados con el delito de estafa cibernética.

Nota: Guía de análisis documental.

Especificaciones

ítems	Subcategoría: Detección
5	Menciona los métodos y técnicas de investigación empleados, junto con su base legal.
6	Incluye información sobre órdenes judiciales y autorizaciones requeridas en la investigación.
7	Detalla la evidencia reunida durante la investigación, subrayando su admisibilidad (pruebas)
8	Describe la preservación y el manejo de la evidencia, cumpliendo con los requisitos de ley.

Tabla 20

Interpretación de resultados del objetivo específico Nº 4

Objetivo Especifico 4)	Nº De Preguntas	Interpretación	Resultado
Determinar los efectos de la insuficiente legislación persecutoria en la investigación del delito de estafa cibernética en el distrito fiscal del Santa, 2022	10	Los operadores judiciales señalan como principal reto la rápida evolución tecnológica y cambios en las modalidades delictivas, que exceden la capacidad de las leyes de actualizarse a dichos avances. Otro desafío radica en la falta de legislación específica que aborde adecuadamente nuevos delitos digitales, generando vacíos legales. También presenta dificultades la ambigüedad en la definición legal de ciberdelitos, obstaculizando el procesamiento penal por carecer de base legal clara. Un problema relevante lo constituye la recopilación y preservación de pruebas digitales, que pueden ser fácilmente alteradas u borradas. La jurisdicción transfronteriza dificulta la cooperación internacional, ante la falta de acuerdos legales armonizados. Los investigadores enfrentan limitaciones por la escasez de recursos, capacitación y experticia especializada para estos casos. La cooperación con proveedores online también se ve entorpecida por ausencia de normas claras sobre colaboración con justicia respetando privacidad.	A partir de los resultados obtenidos, se puede concluir que la insuficiente legislación persecutoria ha dificultado las investigaciones de estafa cibernética en el Distrito Fiscal de Santa de la siguiente manera: - La rápida evolución tecnológica excede la capacidad de actualización de las leyes, generando vacíos legales. - Falta especificidad normativa que aborde adecuadamente nuevos delitos digitales. - Definiciones legales ambiguas de ciberdelitos obstaculizan el procesamiento penal. - Dificultad en la recopilación y preservación de pruebas digitales.
	11	Los principales obstáculos que los operadores judiciales han encontrado en la recopilación de pruebas y la identificación de autores de estafas cibernéticas en su jurisdicción, según lo expuesto, incluyen el uso de tecnologías de ocultamiento por parte de los delincuentes como VPNs, proxy y dark web, lo que dificulta el rastreo de IPs y ubicaciones. Asimismo, se presenta	

		el anonimato online a través de diversas herramientas, así como la falta de cooperación entre proveedores para acceder a información almacenada y limitaciones en el rastreo transfronterizo. También el uso de cifrado y métodos criptográficos sofisticados que obstaculizan la interceptación de comunicaciones, así como transacciones financieras complejas mediante sistemas de pago alternativos. Otros factores son la eliminación o modificación de evidencias digitales, limitaciones tecnológicas y escasez de personal especializado, sumado a las dificultades derivadas de la jurisdicción multifacética de estos delitos que abarcan varias regiones.	- Limitada cooperación transfronteriza por falta de acuerdos legales armonizados. - Escasez de recursos, capacitación y experticia de los investigadores. - Problemas para cooperar con proveedores online debido a ausencia de normas claras.
	12 Carpetas	De la revisión de las 12 carpetas fiscales se revela que, en relación con la mencionada de los métodos de investigación empleados junto con su base legal (ítem 1), solo el 67% lo realiza de manera adecuada. En cuanto a la inclusión de información sobre órdenes y autorizaciones judiciales requeridas (ítem 2), aunque el 75% lo aborda, aún queda un margen del 25% que no garantiza la legalidad de los procedimientos. Aunque la gran mayoría, el 92%, detalla adecuadamente la evidencia reunida y su admisibilidad (ítem 3), el 8% que no lo hace podría deberse a precisiones legales pendientes. En relación con la descripción de la preservación y manejo legal de la prueba (ítem 4), aunque el 75% cumple, el 25% restante deja dudas sobre el apego al marco jurídico durante la recolección. Estos vacíos en la caracterización de aspectos fundamentales de la pesquisa, que en algunos ítems superan el 25%, evidencian la necesidad de fortalecer las directrices normativas para uniformar los criterios de investigación, especialmente en casos relacionados con el delito de estafa cibernética.	Asimismo, del análisis de carpetas fiscales pone se en evidencia vacíos como la falta de sustento legal de métodos y la indefinición sobre legalidad de algunas actuaciones, lo que evidencia la necesidad de fortalecer las directrices normativas para uniformar criterios de investigación sobre este delito complejo. Por lo expuesto, se concluye que la insuficiente legislación ha dificultado de manera sustancial las labores de investigación de estafas cibernéticas.

Nota: Resultados de las tablas 17,18 y 19.

Interpretación y discusión del objetivo específico 4:

El cuarto objetivo específico abordó los efectos de la insuficiente legislación persecutoria en la investigación de la estafa cibernética, según la percepción de los operadores judiciales. Los profesionales identificaron varios desafíos en la investigación del delito. Mencionaron que la rápida evolución tecnológica supera la capacidad de actualización de las leyes, generando vacíos normativos que obstaculizan la persecución efectiva. La falta de especificidad normativa para abordar nuevos delitos digitales y la ambigüedad en las definiciones legales de ciberdelitos también dificulta el procesamiento penal.

Además, destacaron que la recopilación y preservación de pruebas digitales plantea desafíos, ya que estas pueden ser fácilmente alteradas o borradas, afectando la integridad de la evidencia. La falta de cooperación internacional, especialmente en casos transfronterizos, se ve obstaculizada por la ausencia de acuerdos legales armonizados. También señalaron que la falta de recursos, capacitación y experto.

El análisis de las carpetas fiscales reveló deficiencias en aspectos cruciales de la investigación, como la falta de menciones detalladas de métodos de investigación, órdenes judiciales requeridas y evidencia reunida, así como la ausencia de descripciones claras sobre la preservación y manejo legal de la prueba. Esto evidencia la necesidad de fortalecer las directrices normativas para uniformar los criterios de investigación, especialmente en el ámbito de la estafa cibernética. La Defensoría del Pueblo (2023) subraya la complejidad de la investigación de ciberestafa y la necesidad de recursos especializados tanto técnicos como no técnicos, destacando la evolución constante de los debates sobre la efectividad de los modelos y técnicas de investigación en la persecución éxitos

Resultados según el objetivo específico 5): Determinar los efectos de la insuficiente legislación persecutoria en la sanción del delito de estafa cibernética en el distrito fiscal del Santa, 2022.

Tabla 21

La sanción del delito de estafa cibernética

	Interrogantes	Nº	Entrevistado	Respuesta
Pregunta Nº 12	¿Cuáles son las implicaciones de la insuficiente legislación en la imposición de sanciones o penas por delitos de estafa cibernética?	1	J-1	Dificultad cooperación internacional: La falta de legislación sólida complica la colaboración entre países, dificultando la persecución de los delincuentes cibernéticos. Debilidad en prevención: insuficiente legislación debilita la capacidad para prevenir futuras estafas cibernéticas y disuadir su repetición.
		2	J-2	La insuficiente legislación en la imposición de sanciones o penas por delitos de estafa cibernética puede tener varias implicaciones; como dificultades por la capacidad de los sistemas de justicia para castigar de manera efectiva a los culpables y disuadir a otros de cometer delitos similares. Esto puede llevar a un aumento en la impunidad y a un mayor riesgo para los ciudadanos; ya que, la falta de sanciones proporcionales puede desalentar a las víctimas de denunciar estos delitos, lo que limita aún más la capacidad de las autoridades para investigar y procesar a los responsables.
		3	J-3	Podrían ser; uno, la falta de sanciones graves que hagan entender realmente la gravedad de cometer tal hecho delictivo; dos, la falta de conceptualización de términos como IA o software que son también herramientas que utilizan los ciberdelincuentes.
		4	J-4	Falta de disuasión: La falta de sanciones adecuadas puede hacer que los delincuentes perciban los delitos de estafa cibernética como un riesgo bajo. Sin una penalización significativa, no hay un incentivo lo suficientemente fuerte para disuadir a las personas de cometer este tipo de delitos.

			-Escasa protección para las víctimas: La falta de sanciones adecuadas puede resultar en una falta de justicia para las víctimas de estafa cibernéticos, si los delincuentes no enfrentan consecuencias proporcionales a sus acciones, las víctimas pueden sentir que no se les ha hecho justicia y que el sistema legal no está protegiéndolas adecuadamente.
		5	J-5	La falta de leyes nacionales armonizadas contra los delitos cibernéticos, no permite que los esfuerzos para prevenir la recurrencia del fraude en línea y combatir su propagación. Las víctimas de delitos cibernéticos se encuentran completamente vulnerables no solo en el mundo virtual, sino en su día a día en la sociedad sin una medida que les brinde la protección necesaria según su caso.
		6	F-1	La insuficiente legislación causa dificultades en la capacidad de las autoridades para que puedan investigar y perseguir eficazmente a los autores de estafas cibernéticas. Además, los encargados de hacer cumplir la ley pueden encontrarse con obstáculos legales y barreras para llevar a cabo investigaciones exhaustivas, recolectar pruebas sólidas y presentar cargos adecuados, limitando su capacidad para proteger a los ciudadanos y brindar justicia a las víctimas de estafas cibernéticas.
		7	F-2	La insuficiente legislación, dificulta la persecución efectiva de los delitos cibernéticos; ya que las leyes existentes no cubren todas las formas de estafa cibernética y también dificulta la colaboración y cooperación internacional, dado que los delitos cibernéticos trascienden fronteras.
		8	F-3	La insuficiente legislación provoca que los esfuerzos por detener esta clase de delitos sean en vano; puesto que es importante contar con leyes claras y efectivas que establezcan sanciones apropiadas y sin estas además, no se podrá garantizar la protección de los ciudadanos, ni promover un entorno en línea seguro y confiable.
		9	F-4	La insuficiente legislación en la imposición de sanciones o penas por delitos de estafa cibernética puede tener varias implicaciones. En

			resumen, la insuficiente legislación en la imposición de sanciones o penas por delitos de estafa cibernética puede llevar a la impunidad de los delincuentes; conllevan desafíos en la cooperación internacional, falta de disuasión y protección insuficiente para las víctimas.
	10	F-5	La insuficiente legislación en la imposición de sanciones o penas por delitos de estafa cibernética puede tener varias implicaciones negativas; como, la impunidad, baja disuasión, falta de protección para las víctimas y dificultad en la cooperación internacional.
	Resultados: Las principales implicaciones de la insuficiente legislación en la imposición de sanciones por delitos de estafa cibernética, según los entrevistados, son que puede generar impunidad entre los delincuentes al no enfrentar consecuencias acordes a sus acciones, debilidad en los efectos disuasivos al no percibirse estos delitos como de alto riesgo, escasa protección y falta de justicia para las víctimas de estos ilícitos, dificultades en la cooperación internacional ante la falta de legislación armonizada, obstáculos en las capacidades investigativas y procesales de las autoridades, barreras para llevar a cabo indagaciones exhaustivas y obtener pruebas sólidas, y limitaciones para prevenir la reiteración de estas conductas a futuro. En resumen, la insuficiente legislación en este campo puede derivar en resultados contraproducentes como la impunidad, baja disuasión, escasa protección de víctimas y dificultades en la cooperación transfronteriza, entorpeciendo los esfuerzos por combatir adecuadamente estos delitos.		

Nota: Entrevistas aplicadas a los especialistas.

Tabla 22

Influencia en la sanción de la deficiencia de regulación.

	Interrogantes	Nº	Entrevistado	Respuesta
Pregunta Nº 13	¿Cómo influye la carestía de regulación adecuada en la disuasión y prevención de la estafa cibernética en su distrito fiscal?	1	J-1	Se requiere legislación sólida contra el ciberdelito, dotando de recursos a las autoridades para que investiguen y sancionen eficazmente. También es clave la cooperación internacional mediante el intercambio de información y la coordinación de acciones, a fin de combatir estas conductas de forma armonizada.
		2	J-2	-La carestía de regulación adecuada puede tener un impacto significativo en la disuasión y prevención de la estafa cibernética en cualquier distrito fiscal; ya que al no contar con una regulación clara y efectiva, las autoridades pueden enfrentar dificultades para identificar y perseguir a los responsables de estos delitos. Además, quiero agregar que desde mi punto de vista, es importante destacar que la prevención de la estafa cibernética también depende de la educación y concientización de la población. Una regulación adecuada puede ayudar a promover campañas informativas y programas de capacitación que enseñen a las personas cómo protegerse y cómo reconocer los posibles riesgos en línea.
		3	J-3	Desde mi perspectiva, la falta de una regulación adecuada debilita los esfuerzos para disuadir y prevenir el fraude cibernético, lo que conduce a un aumento en el número de casos y en la vulnerabilidad de los ciudadanos a esta forma de delito. Por lo tanto, es importante que se implementen leyes y regulaciones claras y efectivas para abordar este problema y proteger a la comunidad en línea.
		4	J-4	Es crucial contar con regulaciones sólidas que aborden específicamente el delito cibernético y brinden a las autoridades la capacidad de actuar de manera efectiva; ya que o sino por lo contrario, se carecerá de recursos suficientes para capacitar y equipar a las fuerzas del orden, así como la colaboración entre las diferentes

			entidades involucradas para compartir información y coordinar esfuerzos.
		5	J-5	La falta de una regulación adecuada puede tener un impacto significativo en la disuasión y prevención del fraude cibernético en su distrito fiscal. La insuficiente legislación puede crear lagunas jurídicas que los delincuentes pueden aprovechar para llevar a cabo sus actividades fraudulentas sin afrontar consecuencias, esto puede debilitar la capacidad de las autoridades para investigar y procesar eficazmente los delitos cibernéticos. Además, la falta de regulación puede generar una falta de claridad sobre qué acciones son ilegales en el ámbito digital y qué medidas deben tomar las empresas y los individuos para protegerse, y esto puede dejar a las personas vulnerables a estafas y fraudes en línea, ya que es posible que no conozcan las mejores prácticas de seguridad o las señales de advertencia de un intento de estafa.
		6	F-1	-La carestía de regulaciones es una problemática por la cual los gobiernos y las instituciones pertinentes deben establecer marcos regulatorios sólidos para abordar estos delitos cibernéticos; es decir, creación de leyes y políticas que aborden los diferentes aspectos de estos delitos, así como el fortalecimiento de las capacidades de aplicación de la ley y la cooperación internacional en la lucha contra la ciberdelincuencia.
		7	F-2	-La carestía de regulación adecuada tiene un impacto; ya que, la falta de regulación adecuada disminuye la disuasión para cometer delitos cibernéticos. Y la carestía de regulación adecuada también dificulta la prevención de la estafa cibernética; puesto que la carencia de leyes y normativas claras, vuelve más complicado el establecer estándares de seguridad cibernética y promover buenas prácticas en el manejo de datos personales y financieros, lo cual deja a las personas y las organizaciones vulnerables a ataques cibernéticos y estafas.
		8	F-3	La carencia de una adecuada regulación contra la lucha contra la estafa cibernética debilita los mecanismos de disuasión, ya que la carencia de estas leyes que sancionen estos actos delictivos

				de manera apropiada, puede causar que estos delitos sigan afectando a la sociedad.
		9	F-4	La carestía de regulación adecuada tiene un impacto significativo en la disuasión y prevención de la estafa cibernética en mi distrito fiscal de la siguiente manera: Ausencia de normas claras, dificultad en el camino a desarrollar las investigaciones y recaudaciones, falta de una aplicación efectiva.
		10	F-5	La falta de regulación adecuada en diferentes aspectos relacionados con los delitos cibernéticos puede dificultar la detección oportuna de estos delitos y la protección efectiva de los ciudadanos. Es fundamental contar con leyes y regulaciones claras y actualizadas que aborden las nuevas formas de ciberdelincuencia y proporcionen un marco legal sólido para prevenir y combatir estos delitos.
	Resultados: La carestía de regulación adecuada, según los entrevistados, influye negativamente en la disuasión y prevención de la estafa cibernética en los distritos fiscales debido a que debilita los esfuerzos punitivos al crear vacíos normativos que obstaculizan investigaciones y condenas efectivas, reduce la capacidad de las autoridades para combatir estos delitos de manera coordinada, genera falta de certeza sobre cuáles conductas son ilegales en el ámbito digital, dificulta establecer estándares claros de ciberseguridad y promover buenas prácticas, aumenta la vulnerabilidad de las personas y empresas ante amenazas cibernéticas, complica las campañas de prevención y concientización sobre estafas digitales, y entorpece la cooperación transfronteriza necesaria para estas indagaciones. En suma, la falta de marcos legales sólidos, actualizados y acordes a la evolución tecnológica debilita sustancialmente los esfuerzos encaminados a disuadir y proteger de ciberdelitos.			

Nota: Entrevistas aplicadas a los especialistas.

Tabla 23

Analisis de las carpetas fiscales revisadas mediante la guia de análisis documental, enfocado en la "sanción" del delito de estafa cibernética.

Objetivo específico 5)	Nº de carpeta	Código de carpeta fiscal	Ítems	Calificación		Observación
				Si	No	
Determinar los efectos de la insuficiente legislación persecutoria en la ***sanción*** del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	1	**CF-1**	9)		X	
			10)	X		
			11)	X		
			12)	X		
			13)		X	
	2	**CF-2**	9)		X	
			10)	X		
			11)	X		
			12)	X		
			13)		X	
	3	**CF-3**	9)		X	
			10)	X		
			11)	X		
			12)	X		
			13)		X	
	4	**CF-4**	9)		X	
			10)	X		
			11)	X		
			12)	X		
			13)		X	
	5	**CF-5**	9)	X		
			10)	X		
			11)	X		
			12)	X		
			13)		X	
	6	**CF-6**	9)		X	
			10)	X		
			11)	X		
			12)	X		
			13)		X	
	7	**CF-7**	9)		X	
			10)	X		
			11)	X		
			12)	X		
			13)		X	
	8	**CF-8**	9)		X	
			10)	X		
			11)	X		

		12)	X		
		13)		X	
9	**CF-9**	9)		X	
		10)	X		
		11)	X		
		12)	X		
		13)		X	
10	**CF-10**	9)	X		
		10)	X		
		11)	X		
		12)	X		
		13)		X	
11	**CF-11**	9)		X	
		10)	X		
		11)	X		
		12)	X		
		13)		X	
12	**CF-12**	9)	X		
		10)	X		
		11)	X		
		12)	X		
		13)		X	

Resultados: Respecto a lo encontrado, el Ítem 9, que evalúa la inclusión de información sobre audiencias judiciales y decisiones en las carpetas, se destaca que solo el 75% de estas (equivalente a 9 de las 12 carpetas) proporcionaron dicha información, dejando un margen del 25% (3 carpetas) que carece de documentación en este aspecto.

Por otro lado, los Ítems 10, 11 y 12 revelaron un rendimiento perfecto, con un 100% de respuestas afirmativas. Esto confirma que en la totalidad de las carpetas (12 de 12) se desarrollaron de manera integral las partes de la sentencia, se motivaron los hechos y derechos aplicados, y se detallaron las penas impuestas.

Sin embargo, el Ítem 13, que busca la descripción de circunstancias atenuantes o agravantes al imponer las penas, arrojó respuestas negativas en el 100% de los casos (0 de 12 carpetas las mencionaron).

En resumen, aunque se logra una fundamentación correcta de las sentencias, persiste un margen del 25% que no documenta adecuadamente las audiencias y decisiones. Además, ninguna carpeta especifica factores modificatorios de la pena, sugiriendo posibles limitaciones normativas para abordar de manera integral estos delitos digitales adaptados a su contexto.

Nota: Guía de análisis documental.

Especificaciones

ítems	Subcategoría: Detección
9	En el desarrollo del proceso se incluyó información sobre audiencias judiciales y decisiones tomadas.
10	En el expediente, se han independizado y están debidamente desarrolladas las tres partes básicas de la sentencia: parte expositiva, motivación de hechos y derecho, y decisión.
11	Propiamente en la sentencia, el juzgador desarrolla claramente la motivación de hechos y derechos que llevaron a la decisión, justificando la pena impuesta.
12	Se detallan las penalidades impuestas a los culpables, incluyendo sanciones monetarias, penas de prisión, restricciones de acceso a la tecnología.
13	Se describe si se aplicaron circunstancias agravantes o atenuantes en la imposición de las penas.

Tabla 24

Interpretación de resultados del objetivo específico Nº 5

Objetivo Especifico 5)	Nº de preguntas	Interpretación	Resultado
Determinar los efectos de la insuficiente legislación persecutoria en la sanción del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	12	Las principales implicaciones de la insuficiente legislación en la imposición de sanciones por delitos de estafa cibernética, según los entrevistados, son que puede generar impunidad entre los delincuentes al no enfrentar consecuencias acordes a sus acciones, debilidad en los efectos disuasivos al no percibirse estos delitos como de alto riesgo, escasa protección y falta de justicia para las víctimas de estos ilícitos, dificultades en la cooperación internacional ante la falta de legislación armonizada, obstáculos en las capacidades investigativas y procesales de las autoridades, barreras para llevar a cabo indagaciones exhaustivas y obtener pruebas sólidas, y limitaciones para prevenir la reiteración de estas conductas a futuro. En resumen, la insuficiente legislación en este campo puede derivar en resultados contraproducentes como la impunidad, baja disuasión, escasa protección de víctimas y dificultades en la cooperación transfronteriza, entorpeciendo los esfuerzos por combatir adecuadamente estos delitos.	De acuerdo a la perspectiva de los entrevistados, puede concluirse que la insuficiente legislación ha afectado negativamente la sanción de la estafa cibernética en el Distrito Fiscal de Santa de la siguiente manera: - Se ha generado un mayor riesgo de impunidad, al no enfrentar adecuadamente los ciberdelitos con sanciones proporcionales a la gravedad de los hechos. Esto debilita los efectos disuasivos. - Se ha otorgado menor protección a las víctimas y provisto escasa justicia frente a estas conductas ilícitas. - Se evidenciaron obstaculización en las investigaciones y condenas

	13	La carestía de regulación adecuada, según los entrevistados, influye negativamente en la disuasión y prevención de la estafa cibernética en los distritos fiscales debido a que debilita los esfuerzos punitivos al crear vacíos normativos que obstaculizan investigaciones y condenas efectivas, reduce la capacidad de las autoridades para combatir estos delitos de manera coordinada, genera falta de certeza sobre cuáles conductas son ilegales en el ámbito digital, dificulta establecer estándares claros de ciberseguridad y promover buenas prácticas, aumenta la vulnerabilidad de las personas y empresas ante amenazas cibernéticas, complica las campañas de prevención y concientización sobre estafas digitales, y entorpece la cooperación transfronteriza necesaria para estas indagaciones. En suma, la falta de marcos legales sólidos, actualizados y acordes a la evolución tecnológica debilita sustancialmente los esfuerzos encaminados a disuadir y proteger de ciberdelitos.	efectivas mediante la creación de vacíos normativos. - Se ha limitado las capacidades de las autoridades para combatir de manera coordinada la ciberdelincuencia. - Se ha generado incertidumbre sobre las conductas punibles en el ámbito digital. - Se dificulta la prevención y concientización sobre estafas cibernéticas. Se ha visto entorpecida la cooperación transfronteriza necesaria dada la dimensión transnacional de estos delitos. El análisis de las carpetas fiscales corrobora estos hallazgos al evidenciar deficiencias en la documentación de procesos judiciales y omisión de

	12 Carpetas	Respecto a lo encontrado, el Ítem 9, que evalúa la inclusión de información sobre audiencias judiciales y decisiones en las carpetas, se destaca que solo el 75% de estas (equivalente a 9 de las 12 carpetas) proporcionaron dicha información, dejando un margen del 25% (3 carpetas) que carece de documentación en este aspecto. Por otro lado, los Ítems 10, 11 y 12 revelaron un rendimiento perfecto, con un 100% de respuestas afirmativas. Esto confirma que en la totalidad de las carpetas (12 de 12) se desarrollaron de manera integral las partes de la sentencia, se motivaron los hechos y derechos aplicados, y se detallaron las penas impuestas. Sin embargo, el Ítem 13, que busca la descripción de circunstancias atenuantes o agravantes al imponer las penas, arrojó respuestas negativas en el 100% de los casos (0 de 12 carpetas las mencionaron). En resumen, aunque se logra una fundamentación correcta de las sentencias, persiste un margen del 25% que no documenta adecuadamente las audiencias y decisiones. Además, ninguna carpeta especifica factores modificatorios de la pena, sugiriendo posibles limitaciones normativas para abordar de manera integral estos delitos digitales adaptados a su contexto.	circunstancias atenuantes/agravantes al sancionar. Por lo expuesto, se concluye que esta problemática legislativa ha debilitado de forma importante los fines de la política criminal frente a la ciberdelincuencia.

Nota: Resultados de las tablas 21, 22 y 23.

Interpretación y discusión del objetivo específico 5:

El quinto objetivo específico abordó los efectos de la insuficiente legislación persecutoria en la sanción del delito de estafa cibernética. Los entrevistados señalaron que, según su experiencia, los resultados obtenidos en cuanto a sanciones evidenciaron un mayor riesgo de impunidad, menor protección a las víctimas, obstaculización en las investigaciones y limitación en las capacidades de las autoridades para combatir la ciberdelincuencia de manera coordinada.

Como señala Micos (2012), las penas son castigos impuestos a quienes cometen delitos, aunque su aplicación puede verse dificultada por varios factores, como penas muy bajas o no lograr identificar al perpetrador a pesar de denunciarse el delito. La falta de sanciones proporcionales a la gravedad de los hechos genera incertidumbre sobre las conductas punibles en el ámbito digital.

Esta mención se valida con el análisis de las 12 carpetas fiscales, el cual revela deficiencias en la documentación de procesos judiciales. En particular, un 55% de las carpetas no proporciona información sobre audiencias judiciales y decisiones, debido a que no se logró acusar por falta de elementos de convicción o por no identificar a los sujetos activos.

En los procesos donde sí hubo acusación, la falta de mención de circunstancias atenuantes o agravantes al imponer las penas evidencia la necesidad de una mayor claridad normativa para juzgar de manera integral los delitos digitales.

En síntesis, el análisis validó la necesidad de fortalecer la documentación de procesos judiciales, dado que en muchos casos no se logró acusar por falta de pruebas, y cuando sí hubo condena no se consideraron adecuadamente las circunstancias del delito al imponer la sanción. Esto demanda mayor precisión legal.

La postura de la Defensoría del Pueblo (2023) se valida aquí, al señalar que la falta de conocimientos informáticos sofisticados entre el personal judicial dificulta la lucha contra delitos como la estafa en línea.

Por tanto, se la investigación demostró que la premisa de que la insuficiente legislación penal ha debilitado sustancialmente la capacidad del Distrito Fiscal de Santa para enfrentar adecuadamente el fenómeno de la estafa cibernética. La discusión de estos resultados proporciona una base sólida para la formulación de recomendaciones y propuestas de mejora, orientadas a fortalecer la legislación y las capacidades institucionales para prevenir, detectar, investigar y sancionar la estafa cibernética de manera más efectiva.

V. CONCLUSIONES

Con el objetivo general, se determinó que la insuficiente legislación persecutoria del delito de estafa cibernética ha tenido un impacto negativo en el abordaje de este ilícito en el Distrito Fiscal. Aunque los magistrados reconocen la influencia de la normativa internacional, enfatizan la necesidad de mejorar la tipificación del delito para una implementación más efectiva. La Ley de Delitos Cibernéticos muestra avances, pero enfrenta desafíos en precisión normativa, recopilación de pruebas y capacitación de investigadores. La insuficiente legislación dificulta la detección e investigación, genera impunidad, limita la sanción efectiva y restringe la cooperación internacional, debilitando la capacidad para perseguir eficazmente el delito de estafa cibernética como tal.

Con el primer objetivo específico, se determinó que los magistrados entrevistados reconocen la aplicación de la normativa internacional en la legislación nacional, siendo el Perú signatario del convenio de Budapest. Sin embargo, destacan la necesidad de perfeccionar se implementación efectiva, haciendo énfasis en la tipificación precisa del delito de estafa cibernética. Sugieren incorporar esta tipificación legal en la Ley Nº 30096 para mejorar los mecanismos de comunicación y cooperación entre países en la lucha contra este ilícito. Los consultados creen que esta medida fortalecería la articulación de la normativa internacional con las leyes locales, elevando la eficacia en la lucha contra la ciberdelincuencia a nivel nacional.

Con el segundo objetivo específico se logró la identificación tanto de las fortalezas como las limitaciones de la Ley de Delitos Cibernéticos en relación con la estafa cibernética. Aunque se han logrado avances notables, como la amplitud en tipificaciones y penas de los ciberdelitos, aún persisten deficiencias que obstaculizan su aplicación efectiva. Estas incluyen la necesidad de mayor precisión normativa para abordar el delito de estafa cibernética, así como desafíos en materia probatoria, recursos y capacitación de autoridades. A pesar de los esfuerzos de persecución penal, la estafa cibernética continúa siendo tratada como agravante del delito de

estafa mediante su comisión por medios digitales. Estas deficiencias, agravadas por el dinámico contexto tecnológico, subrayan la imperiosa necesidad de mejoras continuas tanto en la legislación como en las capacidades investigativas, asegurando así una persecución adecuada de este delito emergente.

Con el tercer objetivo específico se determinó que la insuficiente legislación persecutoria ha impactado negativamente la detección de casos de estafa cibernética, dado que no aborda adecuadamente las particularidades técnicas de estos delitos, ni fortalece las capacidades de investigación digital, recolección de pruebas electrónicas y cooperación interinstitucional requerida. Asimismo, se evidenciaron vacíos normativos que obstaculizan la agilidad procesal y generan déficit en la especificación de actores involucrados en carpetas fiscales. Por lo tanto, se requiere actualizar la legislación para incorporar un enfoque digital en la detección e incorporar lineamientos que uniformicen criterios de investigación y mejoren la colaboración entre autoridades, a fin de contrarrestar los efectos negativos identificados.

Con el cuarto objetivo específico se determinó que la insuficiente legislación impacta en la investigación de estafas cibernéticas en el Distrito Fiscal del Santa. La rápida adaptación de la legislación a la evolución tecnológica, la clarificación de definiciones legales y el fortalecimiento de recursos y capacitación para los investigadores son elementos esenciales para superar estos desafíos. La colaboración internacional y con proveedores online también requiere de marcos normativos claros. La mejora en la documentación y cumplimiento de procedimientos legales en las carpetas fiscales es vital para garantizar la efectividad de las investigaciones.

Con el quinto objetivo específico se logró determinar que la insuficiente legislación tiene impacto en la sanción de la estafa cibernética en el Distrito Fiscal del Santa. Desde un mayor riesgo de impunidad hasta la vulnerabilidad de las víctimas y la dificultad en la cooperación internacional, los resultados apuntan a la urgente necesidad de fortalecer la legislación en este ámbito. La creación de normativas

claras, proporcionales y adaptadas a la evolución tecnológica es esencial para lograr una efectiva disuasión, protección de las víctimas y cooperación transfronteriza en la persecución de delitos cibernéticos.

VI. RECOMENDACIONES

Primero: al poder legislativo se le recomienda, armonizar la legislación nacional con el Convenio de Budapest para ciberdelincuencia, especialmente enfocándose en la tipificación precisa del delito de estafa cibernética.

Segundo: al poder legislativo se le recomienda, mejorar la Ley de Delitos Cibernéticos incorporando definiciones más precisas, fortaleciendo las capacidades investigativas y normando específicamente la estafa cibernética.

Tercero: al poder legislativo se le recomienda, establecer mecanismos para la rápida adaptación de la legislación a los cambios tecnológicos, clarificando definiciones legales y asegurando recursos y capacitación adecuados para los investigadores.

Cuarto: al ministerio público se le recomienda, solicitar y asignar un mayor presupuesto que permita reforzar recursos tecnológicos y proporcionar capacitación actualizada a los investigadores.

Quinto: al ministerio público, se le recomienda fortalecer la capacitación y recursos del personal del Ministerio Público, especialmente en áreas de ciberdelincuencia, para mejorar la efectividad en la persecución de casos de estafa cibernética.

Sexto: a la policía, se le recomienda, proporcionar capacitación especializada en investigación digital para todos los cuerpos policiales, asegurando una respuesta más efectiva a la estafa cibernética en todos los distritos del Perú.

Sétimo: a la policía, se les recomienda, garantizar el acceso a recursos tecnológicos actualizados para las unidades especializadas en delitos cibernéticos como la Divindat, ello facilitará la investigación y recolección de pruebas, fortaleciendo así la capacidad de respuesta ante la estafa cibernética

REFERENCIAS

Acuario, S. M. (2007). *Delitos informáticos: generalidades.* Organización de los Estados Americanos. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Alonso, L.A. y Esparza, I. (2017). Los retos procesales de la criminalidad informática desde una perspectiva española. *Novum Jus, 11(1)*, 39–72. https://doi.org/10.14718/NovumJus.2017.11.1.2

Aranguren, Y.U. (2022). *Estafa e imputación de la víctima*. IUS Latin, Revista Latinoamericana de Derecho. https://iuslatin.pe/estafa-e-imputacion-de-la-victima/

Arias, L.A. (2021). *Limitaciones del sistema penal para investigar y probar la comisión del Ciberdelito en El Salvador.* [Tesis de maestría, Universidad de El Salvador]. Sistema Bibliotecario. https://ri.ues.edu.sv/id/eprint/26913/.

Ashworth. A. (2009). Fiscalía, policía y público: ¿una guía para una buena vigilancia? *Howard: Revista de Justicia Penal, 23(2),* 65-87. https://doi.org/10.1111/J.1468-2311.1984.TB00495.X

Ávalos, Z. (2021). Necesidad de especialización para combatir la ciberdelincuencia. *Revista Institucional de la Academia de la Magistratura, 15 (1),* 43-62. https://revistainstitucional.amag.edu.pe/index.php/amag/article/view/85

Bradley, L., Noble, N., & Hendricks, B. (2020). El Manual de Publicaciones APA: Cambios en la séptima edición. *The Family Journal, 28(2),* 126-130. https://doi.org/10.1177/1066480720911625

Buompadre, J. E. (2012). *Manual de derecho penal*. Parte especial. Astrea.

Carhuancho, B. y Núñez, F.V. (2020). *Ciberdelincuencia en tiempos de covid-19: ¿La vulneración a derechos constitucionales?* Lumen, 16(1), 93-100. https://doi.org/10.33539/lumen.2020.v16n1.2287

Casado, I (2017). *Estafas cometidas a través de compras online*. Universidad del País Vasco. https://addi.ehu.es/handle/10810/29866.

Castro, G., Huanca, A., Rojas, M.C. y Reyes, M.A. (2023). Compendio Estadístico-2022: Sector Interior. Ministerio del Interior.

Castro, J.J., Camargo, E. y Gómez, L.K. (2023). La investigación aplicada y el desarrollo experimental en el fortalecimiento de las competencias de la sociedad del siglo XXI. Tecnura, 27(75), 140-174. https://dialnet.unirioja.es/servlet/articulo?codigo=8728928

Cisneros, C.P. y Jiménez, R.C. (2021). El delito de estafa: naturaleza, elementos y consumación. *Dilemas contemporáneos 41(1), 1-18*. https://doi.org/10.46377/dilemas.v8i.2794

Clough, J. (2019). Un mundo de diferencias: el Convenio de Budapest sobre ciberdelincuencia y los desafíos de la armonización. *Revista de Derecho de la Universidad de Monash*. https://doi.org/10.26180/5DB8050CA2B5B

Consejo Nacional de Política Criminal. (2020). *Diagnóstico situacional multisectorial sobre la ciberdelincuencia en el Perú.* Ministerio de Justicia y Derechos Humanos.https://www.gob.pe/institucion/minjus/informes-publicaciones/1604516-diagnostico-situacional-multisectorial-sobre-la-ciberdelincuencia-en-el-peru.

Defensoría del pueblo. (2023). *Informe Defensorial N° 001-2023-DP/ADHPD: la ciberdelincuencia en el Perú: estrategias y retos del estado.* Defensoría del pueblo.

Diccionario panhispánico del español jurídico. (2023). *Persecución de delitos.* Panhispánico. https://dpej.rae.es/lema/persecuci%C3%B3n-de-delitos#:~:text=Acci%C3%B3n%20orientada%20a%20la%20comprobaci%C3%B3n,autoridad%20o%20el%20funcionario%20p%C3%BAblico.

Domínguez, R.A. y Vera, R (2022). Análisis espacial del ciberfraude al comercio electrónico. *PODIUM, Nº. 41(1)*, 21-40. https://dialnet.unirioja.es/servlet/articulo?codigo=8621006

DPL News. (2022). *El aumento de la ciberdelincuencia a escala de economía mundial.* DPL News. https://dplnews.com/el-aumento-de-la-ciberdelincuencia-a-escala-de-economia-mundial/.

Dulzaides, M.E. y Molina, A.M. (2004). Análisis documental y de información: dos componentes de un mismo proceso. *Scielo*. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352004000200011

Durán, C (2023). *El comercio electrónico en el contexto de las redes sociales en colombia: principales problemáticas y desafíos actuales.* Universidad Autónoma De Bucaramanga. https://repository.unab.edu.co/bitstream/handle/20.500.12749/19574/2023_Tesis_Maria_Camila_Duran.pdf?sequence=5&isAllowed=y.

El peruano. (2022). *Denuncias por delitos informáticos se incrementaron en más del 90% en el Perú*. Diario Oficial. Página Oficial. https://www.elperuano.pe/noticia/188048-denuncias-por-delitos-informaticos-se-incrementaron-en-mas-del-90-en-el-peru

Golman, T. y Le Nguyen, C. (2021). Difusión del Convenio de Budapest sobre ciberdelincuencia y desarrollo de legislación sobre ciberdelincuencia en los países insulares del Pacífico: 'ley en los libros' versus 'ley en acción'. *Revisión de seguridad y derecho informático, 40 (1)*. https://doi.org/10.1016/J.CLSR.2020.105521

González, J. (2020). *Comercio electrónico en China y México: surgimiento, evolución y perspectivas.* México y la Cuenca del Pacífico, 9 (27), 53-84.

Hernández, R., y Mendoza, C (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta.* Editorial Mc Graw Hill Education.

Ibáñez, I. (2022). *Alerta por incremento de fraudes y estafas online en el Perú: Estas son las más comunes*. Infobae. https://www.infobae.com/america/peru/2022/11/04/ciberseguridad-que-modalidades-de-fraudes-y-estafas-online-son-mas-comunes-en-el-peru/

Infobae. (2022). Delitos informáticos se han incrementado en el Perú. Delitos informáticos se han incrementado en el Perú. Infobae. https://www.infobae.com/america/peru/2022/09/05/delitos-informaticos-se-han-incrementado-en-el-peru/#:~:text=De%20enero%20a%20abril%202022,ser%20v%C3%ADctima%20de%20los%20ciberdelincuentes.

Interpol. (2020). *Un informe de Interpol muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19.* Página web de la Interpol. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

Kara, I. y Aydos, M. (2020). *Fraude cibernético: detección y análisis del criptoransomware.* IEEE Explore. https://doi.org/10.1109/UEMCON51285.2020.9298128

Kotari, M. y Chiplunkar, N.N. (2020). *Una encuesta sobre detección y análisis de amenazas a la seguridad cibernética mediante herramientas de monitoreo.* En B. Gupta y S. Srinivasagopalan (Eds.). *Manual de investigación sobre sistemas de detección de intrusiones* (págs. 77-104). IGI Global. https://doi.org/10.4018/978-1-7998-2242-4.ch005

López, B. (2018). El delito de estafa cometido a través de las redes sociales: problemas de investigación y enjuiciamiento. *IDP: derecho y política, 27(1),* 42-51. https://dialnet.unirioja.es/servlet/articulo?codigo=7329022

Loza, G. y Ore, A. (2017). *La Estructura del Proceso Común en el Nuevo Código Procesal Penal Peruano.* Derecho y Sociedad, 25(1), 163-177.

https://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/17025

Martín, A. (2016). *Un triángulo necesario: la ciencia de la legislación, el control constitucional de las leyes penales y la legislación experimental*. Springer.

Martínez, J.J. (2022). *Propuestas de variables de gestión pública para una productividad eficaz en el poder judicial.* Fondo Editorial del Poder Judicial del Perú.

Mateo, I. (2013). *Ciberdelincuencia, desarrollo y persecución tecnológica*. Universidad Politécnica de Madrid. http://oa.upm.es/22176/1/PFC_IVAN_MATEOS_PASCUAL.pdf

Mayer, L. y Oliver, G. (2020). El delito de fraude informático: concepto y delimitación. Revista chilena de derecho y tecnología, 9(1), 151-184. https://www.scielo.cl/scielo.php?pid=S071958420200001001 51&script=sci_abstract.

Mayer, L., y Oliver, G. (2020). El delito de fraude informático: concepto y delimitación. *Revista Chilena De Derecho Y Tecnología, 9(1)*, 151–184. https://doi.org/10.5354/0719-2584.2020.57149

Ministerio de Justicia y Derechos Humanos. (2022). *Fraudes informáticos y suplantación de identidad son los ciberdelitos más frecuentes en el país. Fraudes informáticos y suplantación de identidad son los ciberdelitos más frecuentes en el país.* Plataforma Única del Estado Peruano. https://www.gob.pe/institucion/minjus/noticias/588261-fraudes-informaticos-y-suplantacion-de-identidad-son-los-ciberdelitos-mas-frecuentes-en-el-pais

Ministerio del Interior. (2016). *Ciberpolicías contra delitos informáticos*. Portal del Ministerio del interior del Perú. https://www.mininter.gob.pe/content/ciberpolic%C3%AD-contra-delitos-inform%C3%A1ticos

Montes, S. (2022). *El panorama del cibercrimen a nivel mundial en estadísticas.* Escudo Digital. https://www.escudodigital.com/ciberseguridad/panorama-cibercrimen-nivel-mundial-en-cinco-estadisticas_51740_102.html

Plataforma única del estado peruano. (2023) *¿Cuáles son los casos de ciberdelincuencia más comunes en el Perú? ¿Cuáles son los casos de ciberdelincuencia más comunes en el Perú?* Plataforma Única del Estado Peruano. https://www.gob.pe/25710-cuales-son-los-casos-de-ciberdelincuencia-mas-comunes-en-el-peru

Quevedo, J.M. (2017). *Investigación y prueba del ciberdelito*. [Tesis doctoral, Universidad de Barcelona]. Dialnet. https://dialnet.unirioja.es/servlet/tesis?codigo=230669

Ríos, A.A. (2014). Análisis y perspectivas del comercio electrónico en México. *Enl@ce: Revista Venezolana de Información, Tecnología y Conocimiento, 11(3),* 97-121.

Rodríguez, M. (2013). Principios de obligatoriedad y discrecionalidad en el ejercicio de la acción penal. *Rev. Derecho Valdivia, 26 (1),* 181-208. http://dx.doi.org/10.4067/S0718-09502013000100009

Rojas, I.R. (2011). Elementos para el diseño de técnicas de investigación: una propuesta de definiciones y procedimientos en la investigación científica. *Tiempo de Educar, 12(24),* 277-297. https://www.redalyc.org/pdf/311/31121089006.pdf

Romeo, C.M. (1996). *Delitos informáticos de carácter patrimonial*. Informática y Derecho, 9 (1), 413-441.

Sain, G.R. (2018). *La estrategia gubernamental frente al cibercrimen: la importancia de las políticas preventivas más allá de la solución penal*. Erreius.

Sánchez, F.A. (2019). Fundamentos epistémicos de la investigación cualitativa y cuantitativa: Consensos y disensos. *Revista Digital Investigación Docencia Universitaria, 13(1),* 102-122. http://dx.doi.org/10.19083/ridu.2019.644.

Smith, R, Grabosky, P. y Urbas, G. (2003). *Ciberdelincuentes en juicio*. Instituto Australiano de Criminología.

Smith-Ditizio, A.A. & Smith, A.D. (2017). *Desafíos del fraude informático y sus implicaciones legales* (4ª Ed.). Enciclopedia de ciencia y tecnología de la información.

Téllez, J.A. (1996). Los Delitos informáticos. Revista iberoamericana de derecho informático, 1(1), 461-474. https://dialnet.unirioja.es/servlet/articulo?codigo=248768

Usaqui, K. (2021). *Los actos de investigación en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, distrito fiscal de Lima, 2021.* [Tesis maestría, Universidad Cesar Vallejo]. Repositorio. https://hdl.handle.net/20.500.12692/89325

Vega, A, Maguiña, J.L., Soto, A., Lama, J. y Correa, L.E. (2021). Estudios transversales. *Revista de la Facultad de Medicina Humana, 21(1),* 179-185. https://dx.doi.org/10.25176/rfmh.v21i1.3069

Vilchez, R.C. (2020). La ciberdelincuencia en el contexto de la pandemia del coronavirus. Una aproximación desde el marco convencional. *Ars Iuris Salmanticensis, 8(1),* 21-25. https://gredos.usal.es/bitstream/handle/10366/146139/La_ciberdelincuencia_en_el_contexto_de_l.pdf?sequence=1&isAllowed=y

Zevallos, O (2020). Delitos informáticos: ¿Cuáles son los principales fraudes informáticos que se pueden cometer a través del E-Commerce? *El portal jurídico de IUS ET VERITAS.* https://ius360.com/delitos-informaticos-cuales-son-los-principales-fraudes-informaticos-que-se-pueden-cometer-a-traves-del-e-commerce-oscar-zevallos-prado/

ANEXO N° 1: MATRIZ DE CATEGORIZACIÓN

TÍTULO: "Efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022".							
Problema general	Objetivo General	Objetivo Específico	Categoría de estudio	Definición conceptual	Subcategorías	Nº	Interrogante
¿Cuáles son los efectos de la insuficiente legislación persecutoria del delito de estafa cibernética del distrito fiscal del Santa, 2022?	Determinar los efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	1. Determinar la aplicación de la normativa internacional en la legislación nacional en la persecución del delito de estafa cibernética en el distrito fiscal del Santa, 2022	Categoría 1: insuficiente legislación	La insuficiente legislación, que en la persecución penal, se refiere a la carencia de un marco regulatorio sólido y coherente en el sistema legal (Martín, 2016). La ausencia de una normativa adecuada en este contexto facilita la discrecionalidad en el abandono o retiro del ejercicio de la acción penal (Bachmaier y Demleitner, 2018).	Convenio y protocolos sobre la ciberdelincuencia del consejo de Europa (Convenio de Budapest).	1	Como experto en derecho penal, ¿Qué conoce del Convenio del Consejo de Europa (Convenio de Budapest)?
						2	¿Podría identificar de qué manera el Convenio de Budapest sobre Ciberdelincuencia ha influido en la legislación y regulación relacionada con la estafa cibernética en el Perú?
						3	¿Considera que existe una interconexión entre el Convenio de Budapest y la legislación nacional para abordar la persecución de la estafa cibernética?
¿Cuáles son los efectos de la insuficiente legislación persecutoria	Determinar los efectos de la i insuficiente legislación persecutoria del delito de estafa cibernética en	. 2. Determinar las principales deficiencias de la insuficiente legislación persecutoria del delito de estafa			Ley N° 30096	4	¿Cuáles son las fortalezas y limitaciones que identifica en la Ley N° 30096, ley de delitos cibernéticos en el Perú?
						5	¿Considera que la Ley N° 30096, favorece la

del delito de estafa cibernética del distrito fiscal del Santa, 2022?	el distrito fiscal del Santa, 2022	cibernética en el distrito fiscal del Santa, 2022.					persecución penal del delito de estafa cibernética?
					-Articulo N° 196- A del Código penal: Estafa agravada.	6	¿Podría explicar en detalle la aplicación del Artículo N° 196-A del Código Penal, respecto a la tipificación de la estafa agravada, en el contexto de la persecución de la estafa cibernética?
						7	¿Cuáles considera son los desafíos específicos asociados con la interpretación y aplicación de este artículo en casos de estafa cibernética?
		3. Determinar los efectos de la insuficiente legislación persecutoria en la detección del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	Categoría 2: Persecución penal de la estafa cibernética	La persecución penal del delito de estafa cibernética comprende diversas etapas, desde la investigación hasta la imposición de sanciones, y enfrenta retos importantes en el proceso debido a factores como la complejidad tecnológica y los recursos	Detección	8	Como especialista en derecho procesal penal, ¿cómo considera que la insuficiente legislación ha afectado la detección de casos de estafa cibernética en el Distrito Fiscal del Santa?
						9	Podría proporcionar ejemplos de situaciones donde se evidencie que la falta de regulación adecuada dificultó la detección oportuna de este delito
		4. Determinar los efectos de la insuficiente legislación persecutoria en			Investigación	10	¿Cuáles considera que son los retos específicos que ha enfrentado en la investigación de estos delitos debido a la insuficiente

	la investigación del delito de estafa cibernética en el distrito fiscal del Santa, 2022	financieros limitados disponibles (Ore y Loza, 2017).			legislación legislativa?
				11	Proporcione ejemplos de obstáculos que ha encontrado en la recopilación de pruebas o en la identificación de los autores de estafas cibernéticas en su jurisdicción.
	5. Determinar los efectos de la insuficiente legislación persecutoria en la sanción del delito de estafa cibernética en el distrito fiscal del Santa, 2022.		Sanción	12	¿Cuáles son las implicaciones de la insuficiente legislación en la imposición de sanciones o penas por delitos de estafa cibernética?
				13	¿Cómo influye la carestía de regulación adecuada en la disuasión y prevención de la estafa cibernética en su distrito fiscal?

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 02

Consentimiento Informado

Título de la investigación: “Efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa - 2022”
Investigador (a): Jean Carlos Acosta Zavaleta.

Propósito del estudio

Le invitamos a participar en la investigación titulada “Efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa - 2022”, cuyo objetivo es determinar los efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022

Esta investigación es desarrollada por el estudiante de posgrado del programa académico de maestría en derecho penal y procesal penal de la Universidad César Vallejo del campus Chimbote, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la institución.

Este estudio, pretende analizar el como la tecnología trajo consigo los ciberdelitos, donde la figura delictiva de la estafa cibernética tiene una alta incidencia; sin embargo son pocos quienes presentan denuncias, pues factores como la cuantía, la novedad del delito, la desinformación la vergüenza influyen en la baja tasa de denuncias, sumado a la baja tasa de sentencias por este tipo de delitos, por la insuficiente legislación, se dificulta su percusión penal efectiva. En este tenor, se consideró como el problema de investigación, ¿Cuáles son los efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa – 2022?

Procedimiento

Si usted decide participar en la investigación se realizará lo siguiente

1. Se realizará una entrevista donde se recogerán datos personales y algunas preguntas.
2. Dicha entrevista, tendrá una duración aproximada de 25 minutos y se realizará en su ambiente de labores.
3. Las respuestas al cuestionario o guía de entrevista serán codificadas usando un número de identificación y, por lo tanto, serán anónimas.

* Obligatorio a partir de los 18 años

INVESTIGA UCV

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

Confidencialidad (principio de justicia):

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 (a) Jean Carlos Acosta Zavaleta, email: jean.acosta.33@gmail.com y Docente asesora Mg. Patricia Janet Moreno Núñez, email: Pmorenon@ucvvirtual.edu.pe

Consentimiento

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

Nombre y apellidos: ……..……..
Fecha y hora: ……..…….

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

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 03: EVALUACIÓN DE CARPETAS FISCALES

GUÍA DE ANÁLISIS DOCUMENTAL

TITULO DE LA INVESTIGACIÓN: "Efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa – 2022"

MAESTRANDO: Acosta Zavaleta, Jean Carlos

CODIFICACIÓN DE LA CARPETA FISCAL: _____

INICIO DE LA INVESTIGACIÓN:_____

FECHA DE CONCLUSIÓN DE LA INVESTIGACIÓN:_____

Ítems	**Subcategoría: Detección**	**Escala de Cumplimiento**	
		Si	No
1	El expediente se describe cómo se detectó el delito (hechos)		
2	Menciona las fuentes de información y dispositivos tecnológicos utilizados para la detección.		
3	Se individualizó y detalló el papel de cada actor que posibilitó la detección del delito.		
4	Describe la colaboración interinstitucional en la etapa de detección		
Ítems	**Subcategoría: investigación**		
5	Se menciona los métodos y técnicas de investigación empleados, junto con su base legal.		
6	Incluye información sobre órdenes judiciales y autorizaciones requeridas en la investigación.		
7	Se detalla la evidencia reunida durante la investigación, subrayando su admisibilidad (pruebas)		
8	Describe la preservación y el manejo de la evidencia, cumpliendo con los requisitos de ley.		
Ítems	**Subcategoría: sanción**		
9	En el desarrollo del proceso se incluyó información sobre audiencias judiciales y decisiones tomadas.		
10	En el expediente, se han independizado y están debidamente desarrolladas las tres partes básicas de la sentencia: parte expositiva, motivación de hechos y derecho, y decisión.		
11	Propiamente en la sentencia, el juzgador desarrolla claramente la motivación de hechos y derechos que llevaron a la decisión, justificando la pena impuesta.		
12	Se detallan las penalidades impuestas a los culpables, incluyendo sanciones monetarias, penas de prisión, restricciones de acceso a la tecnología.		
13	Se describe si se aplicaron circunstancias agravantes o atenuantes en la imposición de las penas.		

Calificación General del Proceso:

Calificación General del Proceso	**Escala de cumplimiento**	**EFECTOS O CONSECUENCIAS DETECTADAS DE LA INSUFICIENTE REGULACIÓN NORMATIVA.**
El expediente demuestra un proceso de persecución penal del delito de estafa cibernética.	Si /no	
Identifica con precisión los actores, métodos y procedimientos utilizados en el proceso, cumpliendo con la legislación peruana.	Si /no	

Observaciones Adicionales:

_____
_____
_____
_____
_____
_____
_____
_____
_____

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 03-A: GUÍA DE ENTREVISTA A PARTICIPANTES

TÍTULO DE LA INVESTIGACIÓN:

"Efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa – 2022"

MAESTRANDO:

Acosta Zavaleta, Jean Carlos

Estimado Magistrado:

Me dirijo a ustedes como investigador en derecho con el propósito de llevar a cabo un estudio sobre insuficiente legislación persecutoria del delito de estafa cibernética, con el fin de mejorar la comprensión de los procesos judiciales y contribuir al desarrollo continuo de nuestra práctica legal.

Su participación es esencial para enriquecer este proyecto. La información recopilada, tratada con la más estricta confidencialidad, proporcionará valiosas percepciones que podrían traducirse en mejoras tangibles en nuestra labor diaria.

ENTREVISTA

CATEGORÍA 1: INSUFICIENTE LEGISLACIÓN

Subcategoría: Convenio y protocolos sobre la ciberdelincuencia del Consejo de Europa (Convenio de Budapest):

1. Como experto en derecho penal, ¿Qué conoce del Convenio del Consejo de Europa (Convenio de Budapest)?
2. ¿Podría identificar de qué manera el Convenio de Budapest sobre Ciberdelincuencia ha influido en la legislación y regulación relacionada con la estafa cibernética en el Perú?
3. ¿Considera que existe una interconexión entre el Convenio de Budapest y la legislación nacional para abordar la persecución de la estafa cibernética?

Subcategoría: Ley N° 30096:

4. ¿Cuáles son las fortalezas y limitaciones que identifica en la Ley N° 30096, ley de delitos cibernéticos en el Perú?
5. ¿Considera que la Ley N° 30096, favorece la persecución penal del delito de estafa cibernética?

Subcategoría: Artículo N° 196-A del Código Penal: Estafa Agravada:

6. ¿Podría explicar en detalle la aplicación del Artículo N° 196-A del Código Penal, respecto a la tipificación de la estafa agravada, en el contexto de la persecución de la estafa cibernética?
7. ¿Cuáles considera son los desafíos específicos asociados con la interpretación y aplicación de este artículo en casos de estafa cibernética?

CATEGORÍA 2: PERSECUCIÓN PENAL DE LA ESTAFA CIBERNÉTICA

Subcategoría: Detección

8. Como especialista en derecho procesal penal, ¿cómo considera que la insuficiente legislación ha afectado la detección de casos de estafa cibernética en el Distrito Fiscal del Santa?
9. Podría proporcionar ejemplos de situaciones donde se evidencie que la falta de regulación adecuada dificultó la detección oportuna de este delito

Subcategoría: Investigación

10. ¿Cuáles considera que son los retos específicos que ha enfrentado en la investigación de estos delitos debido a la insuficiente legislación?
11. Proporcione ejemplos de obstáculos que ha encontrado en la recopilación de pruebas o en la identificación de los autores de estafas cibernéticas en su jurisdicción.

Subcategoría: Sanciones:

12. ¿Cuáles son las implicaciones de la insuficiente legislación en la imposición de sanciones o penas por delitos de estafa cibernética?
13. ¿Cómo influye la carestía de regulación adecuada en la disuasión y prevención de la estafa cibernética en su distrito fiscal?

Agradezco de antemano su colaboración y estoy disponible para abordar cualquier pregunta o inquietud que puedan tener durante este proceso.

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 04: EVALUACIÓN DE EXPERTOS

EVALUACIÓN: JUICIO DE EXPERTO Nº 01

Respetado magistrado: Usted ha sido seleccionado para evaluar los instrumentos "GUÍA DE ENTREVISTA" y "GUÍA DE ANALISIS DOCUMENTAL". Su participación en la evaluación de este instrumento es de suma importancia para garantizar su validez y asegurar que los resultados obtenidos sean utilizados de manera eficaz. Agradezco sinceramente su valiosa colaboración.

1. Datos generales de especialista

Nombre del especialista:	CARMEN NELLY ,MACUADO ARROYO
Grado profesional:	Maestría (X) Doctor ( )
Área de formación académica:	Universidad Cesar Vallejo
Áreas de experiencia profesional:	Penal
Institución donde labora:	Ministerio Público
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)

2. Propósito de la evaluación:

Validar el contenido de los instrumentos de recojo de datos, por juicio de expertos.

3. Datos del investigador

Nombre de las Pruebas:	"GUÍA DE ENTREVISTA" "GUÍA DE ANÁLISIS DOCUMENTAL"
Autor:	Jean Carlos Acosta Zavaleta
Procedencia:	Programa académico de Maestría en derecho penal y procesal penal
Administración:	Presencial
Tiempo de aplicación:	20 minutos.
Ámbito de aplicación:	Distrito judicial del Santa y Distrito fiscal del Santa.
Objetivo de la investigación:	Determinar los efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022

4. Presentación de instrucciones para el especialista:

La calificación deberá ser de acuerdo a lo siguiente:

CATEGORÍA	CALIFICACIÓN	INDICADOR
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la categoría o indicador que está midiendo**.**	1. No cumple con el criterio	El ítem no tiene relación lógica con la categoría
	2. Bajo Nivel	El ítem tiene una relación tangencial /lejana con la categoría.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Alto nivel	El ítem se encuentra está relacionado con la categoría que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la categoría.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

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

A continuación a usted le presento el cuestionario "GUÍA DE ENTREVISTA" para la investigación titulada: "EFECTOS DE LA INSUFICIENTE LEGISLACIÓN PERSECUTORIA DEL DELITO DE ESTAFA CIBERNÉTICA EN EL DISTRITO FISCAL DEL SANTA, 2022". Elaborado por el Abog. Jean Carlos Acosta Zavaleta en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

UNIVERSIDAD CÉSAR VALLEJO

Objetivos		Ítem	Claridad				Coherencia				Relevancia				Observaciones
			1	2	3	4	1	2	3	4	1	2	3	4	
1. Determinar la aplicación de la normativa internacional en la legislación nacional persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022	1	Como experto en derecho penal, ¿Qué conoce del Convenio del Consejo de Europa (Convenio de Budapest)?				X				X				X	
	2	¿Podría identificar de qué manera el Convenio de Budapest sobre Ciberdelincuencia ha influido en la legislación y regulación relacionada con la estafa cibernética en el Perú?				X				X				X	
	3	¿Considera que existe una interconexión entre el Convenio de Budapest y la legislación nacional para abordar la persecución de la estafa cibernética?				X				X				X	
2. Determinar las principales deficiencias de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	4	¿Cuáles son las fortalezas y limitaciones que identifica en la Ley N° 30096, ley de delitos cibernéticos en el Perú?				X				X				X	
	5	¿Considera que la Ley N° 30096, favorece la persecución penal del delito de estafa cibernética?				X				X				X	
	6	¿Podría explicar en detalle la aplicación del Artículo N° 196-A del Código Penal, respecto a la tipificación de la estafa agravada, en el contexto de la persecución de la estafa cibernética?				X				X				X	
	7	¿Cuáles considera son los desafíos específicos asociados con la interpretación y aplicación de este artículo en casos de estafa cibernética?				X				X				X	
3. Determinar los efectos de la insuficiente legislación persecutoria en la detección del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	8	Como especialista en derecho procesal penal, ¿cómo considera que la insuficiente legislación ha afectado la detección de casos de estafa cibernética en el Distrito Fiscal del Santa?				X				X				X	
	9	Podría proporcionar ejemplos de situaciones donde se evidencie que la falta de regulación adecuada dificultó la detección oportuna de este delito				X				X				X	
4. Determinar los efectos de la insuficiente legislación persecutoria en la investigación del delito de estafa cibernética en el distrito fiscal del Santa, 2022	10	¿Cuáles considera que son los retos específicos que ha enfrentado en la investigación de estos delitos debido a la insuficiente legislación?				X				X				X	
	11	Proporcione ejemplos de obstáculos que ha encontrado en la recopilación de pruebas o en la identificación de los autores de estafas cibernéticas en su jurisdicción.				X				X				X	
5. Determinar los efectos de la insuficiente legislación persecutoria en la sanción del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	12	¿Cuáles son las implicaciones de la insuficiente legislación en la imposición de sanciones o penas por Delitos de estafa cibernética?				X				X				X	
	13	¿Cómo influye la carestía de regulación adecuada en la disuasión y prevención de la estafa cibernética en su distrito fiscal?				X				X				X	

Asimismo, a usted le presento la "GUÍA DE ANÁLISIS DOCUMENTAL" para la investigación titulada: "EFECTOS DE LA INSUFICIENTE LEGISLACIÓN PERSECUTORIA DEL DELITO DE ESTAFA CIBERNÉTICA EN EL DISTRITO FISCAL DEL SANTA, 2022". Elaborado por el Abog. Jean Carlos Acosta Zavaleta en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

Objetivos	Ítem		Claridad				Coherencia				Relevancia				Observaciones
			1	2	3	4	1	2	3	4	1	2	3	4	
3. Determinar los efectos de la insuficiente legislación persecutoria en la detección del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	1	El expediente describe cómo se detectó el delito (hechos)				X				X				X	
	2	Menciona las fuentes de información y dispositivos tecnológicos utilizados para la detección.				X				X				X	
	3	Se individualizó y detalló el papel de cada actor que posibilitó la detección del delito.				X				X				X	
	4	Describe la colaboración interinstitucional en la etapa de detección				X				X				X	
4. Determinar los efectos de la insuficiente legislación persecutoria en la investigación del delito de estafa cibernética en el distrito fiscal del Santa, 2022	5	Menciona los métodos y técnicas de investigación empleados, junto con su base legal.				X				X				X	
	6	Incluye información sobre órdenes judiciales y autorizaciones requeridas en la investigación.				X				X				X	
	7	Detalla la evidencia reunida durante la investigación, subrayando su admisibilidad (pruebas)				X				X				X	
	8	Describe la preservación y el manejo de la evidencia, cumpliendo con los requisitos de ley.				X				X				X	
5. Determinar los efectos de la insuficiente legislación persecutoria en la sanción del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	9	En el desarrollo del proceso se incluyó información sobre audiencias judiciales y decisiones tomadas.				X				X				X	
	10	En el expediente, se han independizado y están debidamente desarrolladas las tres partes básicas de la sentencia: parte expositiva, motivación de hechos y derecho, y decisión.				X				X				X	
	11	Propiamente en la sentencia, el juzgador desarrolla claramente la motivación de hechos y derechos que llevaron a la decisión, justificando la pena impuesta.				X				X				X	
	12	Se detallan las penalidades impuestas a los culpables, incluyendo sanciones monetarias, penas de prisión, restricciones de acceso a la tecnología.				X				X				X	

	13	Se describe si se aplicaron circunstancias agravantes o atenuantes en la imposición de las penas.				X			X				X		

FISCAL PROVINCIAL PENAL
SEGUNDA FISCALIA PENAL - DIST. FISCAL DEL SANTA
Firma del evaluador
DNI: 32966345

UNIVERSIDAD CÉSAR VALLEJO

EVALUACIÓN: JUICIO DE EXPERTO Nº 02

Respetado magistrado: Usted ha sido seleccionado para evaluar los instrumentos "GUÍA DE ENTREVISTA" y "GUÍA DE ANALISIS DOCUMENTAL". Su participación en la evaluación de este instrumento es de suma importancia para garantizar su validez y asegurar que los resultados obtenidos sean utilizados de manera eficaz. Agradezco sinceramente su valiosa colaboración.

1. Datos generales de especialista

Nombre del especialista:	JOSÉ LUIS AVALOS MÉNDEZ
Grado profesional:	Maestría (X) Doctor ( )
Área de formación académica:	Universidad Cesar Vallejo
Áreas de experiencia profesional:	Derecho Penal
Institución donde labora:	Ministerio Público
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)

2. Propósito de la evaluación:

Validar el contenido de los instrumentos de recojo de datos, por juicio de expertos.

3. Datos del investigador

Nombre de las Pruebas:	"GUÍA DE ENTREVISTA" "GUÍA DE ANÁLISIS DOCUMENTAL"
Autor:	Jean Carlos Acosta Zavaleta
Procedencia:	Programa académico de Maestría en derecho penal y procesal penal
Administración:	Presencial
Tiempo de aplicación:	20 minutos.
Ámbito de aplicación:	Distrito judicial del Santa y Distrito fiscal del Santa.
Objetivo de la investigación:	Determinar los efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022

4. Presentación de instrucciones para el especialista:

La calificación deberá ser de acuerdo a lo siguiente:

CATEGORÍA	CALIFICACIÓN	INDICADOR
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la categoría o indicador que está midiendo**.**	1. No cumple con el criterio	El ítem no tiene relación lógica con la categoría
	2. Bajo Nivel	El ítem tiene una relación tangencial /lejana conla categoría.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Alto nivel	El ítem se encuentra está relacionado con la categoría que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la categoría.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

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

A continuación a usted le presento el cuestionario "GUÍA DE ENTREVISTA" para la investigación titulada: "EFECTOS DE LA INSUFICIENTE LEGISLACIÓN PERSECUTORIA DEL DELITO DE ESTAFA CIBERNÉTICA EN EL DISTRITO FISCAL DEL SANTA, 2022". Elaborado por el Abog. Jean Carlos Acosta Zavaleta en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

UNIVERSIDAD CÉSAR VALLEJO

Objetivos	Ítem		Claridad				Coherencia				Relevancia				Observaciones
			1	2	3	4	1	2	3	4	1	2	3	4	
1. Determinar la aplicación de la normativa internacional en la legislación nacional persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022	1	Como experto en derecho penal, ¿Qué conoce del Convenio del Consejo de Europa (Convenio de Budapest)?				X				X				X	
	2	¿Podría identificar de qué manera el Convenio de Budapest sobre Ciberdelincuencia ha influido en la legislación y regulación relacionada con la estafa cibernética en el Perú?				X				X				X	
	3	¿Considera que existe una interconexión entre el Convenio de Budapest y la legislación nacional para abordar la persecución de la estafa cibernética?				X				X				X	
2. Determinar las principales deficiencias de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	4	¿Cuáles son las fortalezas y limitaciones que identifica en la Ley N° 30096, ley de delitos cibernéticos en el Perú?				X				X				X	
	5	¿Considera que la Ley N° 30096, favorece la persecución penal del delito de estafa cibernética?				X				X				X	
	6	¿Podría explicar en detalle la aplicación del Artículo N° 196-A del Código Penal, respecto a la tipificación de la estafa agravada, en el contexto de la persecución de la estafa cibernética?				X				X				X	
	7	¿Cuáles considera son los desafíos específicos asociados con la interpretación y aplicación de este artículo en casos de estafa cibernética?				X				X				X	
3. Determinar los efectos de la insuficiente legislación persecutoria en la detección del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	8	Como especialista en derecho procesal penal, ¿cómo considera que la insuficiente legislación ha afectado la detección de casos de estafa cibernética en el Distrito Fiscal del Santa?				X				X				X	
	9	Podría proporcionar ejemplos de situaciones donde se evidencie que la falta de regulación adecuada dificultó la detección oportuna de este delito				X				X				X	
4. Determinar los efectos de la insuficiente legislación persecutoria en la investigación del delito de estafa cibernética en el distrito fiscal del Santa, 2022	10	¿Cuáles considera que son los retos específicos que ha enfrentado en la investigación de estos delitos debido a la insuficiente legislación?				X				X				X	
	11	Proporcione ejemplos de obstáculos que ha encontrado en la recopilación de pruebas o en la identificación de los autores de estafas cibernéticas en su jurisdicción.				X				X				X	
5. Determinar los efectos de la insuficiente legislación persecutoria en la sanción del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	12	¿Cuáles son las implicaciones de la insuficiente legislación en la imposición de sanciones o penas por Delitos de estafa cibernética?				X				X				X	
	13	¿Cómo influye la carestía de regulación adecuada en la disuasión y prevención de la estafa cibernética en su distrito fiscal?				X				X				X	

Asimismo, a usted le presento la "GUÍA DE ANÁLISIS DOCUMENTAL" para la investigación titulada: "EFECTOS DE LA INSUFICIENTE LEGISLACIÓN PERSECUTORIA DEL DELITO DE ESTAFA CIBERNÉTICA EN EL DISTRITO FISCAL DEL SANTA, 2022". Elaborado por el Abog. Jean Carlos Acosta Zavaleta en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

Objetivos	Ítem		Claridad				Coherencia				Relevancia				Observaciones
			1	2	3	4	1	2	3	4	1	2	3	4	
3. Determinar los efectos de la insuficiente legislación persecutoria en la detección del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	1	El expediente describe cómo se detectó el delito (hechos)				X				X				X	
	2	Menciona las fuentes de información y dispositivos tecnológicos utilizados para la detección.				X				X				X	
	3	Se individualizó y detalló el papel de cada actor que posibilitó la detección del delito.				X				X				X	
	4	Describe la colaboración interinstitucional en la etapa de detección				X				X				X	
4. Determinar los efectos de la insuficiente legislación persecutoria en la investigación del delito de estafa cibernética en el distrito fiscal del Santa, 2022	5	Menciona los métodos y técnicas de investigación empleados, junto con su base legal.				X				X				X	
	6	Incluye información sobre órdenes judiciales y autorizaciones requeridas en la investigación.				X				X				X	
	7	Detalla la evidencia reunida durante la investigación, subrayando su admisibilidad (pruebas)				X				X				X	
	8	Describe la preservación y el manejo de la evidencia, cumpliendo con los requisitos de ley.				X				X				X	
5. Determinar los efectos de la insuficiente legislación persecutoria en la sanción del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	9	En el desarrollo del proceso se incluyó información sobre audiencias judiciales y decisiones tomadas.				X				X				X	
	10	En el expediente, se han independizado y están debidamente desarrolladas las tres partes básicas de la sentencia: parte expositiva, motivación de hechos y derecho, y decisión.				X				X				X	
	11	Propiamente en la sentencia, el juzgador desarrolla claramente la motivación de hechos y derechos que llevaron a la decisión, justificando la pena impuesta.				X				X				X	
	12	Se detallan las penalidades impuestas a los culpables, incluyendo sanciones monetarias, penas de prisión, restricciones de acceso a la tecnología.				X				X				X	

	13	Se describe si se aplicaron circunstancias agravantes o atenuantes en la imposición de las penas.				X				X				X	

Dr. José Luis Avalos Méndez
Fiscal Adjunto Provincial (T)
Fiscalía Provincial Penal de Pallasca
Distrito Fiscal del Santa
Firma del evaluador
DNI: 41.52 90 42

UNIVERSIDAD CÉSAR VALLEJO

EVALUACIÓN: JUICIO DE EXPERTO Nº 03

Respetado magistrado: Usted ha sido seleccionado para evaluar los instrumentos "GUÍA DE ENTREVISTA" y "GUÍA DE ANALISIS DOCUMENTAL". Su participación en la evaluación de este instrumento es de suma importancia para garantizar su validez y asegurar que los resultados obtenidos sean utilizados de manera eficaz. Agradezco sinceramente su valiosa colaboración.

1. Datos generales de especialista

Nombre del especialista:	ELIZABETH MILAGROS OBREGÓN RUIZ
Grado profesional:	Maestría (X) Doctor ( )
Área de formación académica:	Universidad Cesar Vallejo
Áreas de experiencia profesional:	Penal
Institución donde labora:	Ministerio Público
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)

2. Propósito de la evaluación:

Validar el contenido de los instrumentos de recojo de datos, por juicio de expertos.

3. Datos del investigador

Nombre de las Pruebas:	"GUÍA DE ENTREVISTA" "GUÍA DE ANÁLISIS DOCUMENTAL"
Autor:	Jean Carlos Acosta Zavaleta
Procedencia:	Programa académico de Maestría en derecho penal y procesal penal
Administración:	Presencial
Tiempo de aplicación:	20 minutos.
Ámbito de aplicación:	Distrito judicial del Santa y Distrito fiscal del Santa.
Objetivo de la investigación:	Determinar los efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022

4. Presentación de instrucciones para el especialista:

La calificación deberá ser de acuerdo a lo siguiente:

CATEGORÍA	CALIFICACIÓN	INDICADOR
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la categoría o indicador que está midiendo**.**	1. No cumple con el criterio	El ítem no tiene relación lógica con la categoría
	2. Bajo Nivel	El ítem tiene una relación tangencial /lejana con la categoría.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Alto nivel	El ítem se encuentra está relacionado con la categoría que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la categoría.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

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

A continuación a usted le presento el cuestionario "GUÍA DE ENTREVISTA" para la investigación titulada: "EFECTOS DE LA INSUFICIENTE LEGISLACIÓN PERSECUTORIA DEL DELITO DE ESTAFA CIBERNÉTICA EN EL DISTRITO FISCAL DEL SANTA, 2022". Elaborado por el Abog. Jean Carlos Acosta Zavaleta en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

UNIVERSIDAD CÉSAR VALLEJO

Objetivos	Ítem		Claridad				Coherencia				Relevancia				Observaciones
			1	2	3	4	1	2	3	4	1	2	3	4	
1. Determinar la aplicación de la normativa internacional en la legislación nacional persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022	1	Como experto en derecho penal, ¿Qué conoce del Convenio del Consejo de Europa (Convenio de Budapest)?				X				X				X	
	2	¿Podría identificar de qué manera el Convenio de Budapest sobre Ciberdelincuencia ha influido en la legislación y regulación relacionada con la estafa cibernética en el Perú?				X				X				X	
	3	¿Considera que existe una interconexión entre el Convenio de Budapest y la legislación nacional para abordar la persecución de la estafa cibernética?				X				X				X	
2. Determinar las principales deficiencias de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	4	¿Cuáles son las fortalezas y limitaciones que identifica en la Ley N° 30096, ley de delitos cibernéticos en el Perú?				X				X				X	
	5	¿Considera que la Ley N° 30096, favorece la persecución penal del delito de estafa cibernética?				X				X				X	
	6	¿Podría explicar en detalle la aplicación del Artículo N° 196-A del Código Penal, respecto a la tipificación de la estafa agravada, en el contexto de la persecución de la estafa cibernética?				X				X				X	
	7	¿Cuáles considera son los desafíos específicos asociados con la interpretación y aplicación de este artículo en casos de estafa cibernética?				X				X				X	
3. Determinar los efectos de la insuficiente legislación persecutoria en la detección del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	8	Como especialista en derecho procesal penal, ¿cómo considera que la insuficiente legislación ha afectado la detección de casos de estafa cibernética en el Distrito Fiscal del Santa?				X				X				X	
	9	Podría proporcionar ejemplos de situaciones donde se evidencie que la falta de regulación adecuada dificultó la detección oportuna de este delito				X				X				X	
4. Determinar los efectos de la insuficiente legislación persecutoria en la investigación del delito de estafa cibernética en el distrito fiscal del Santa, 2022	10	¿Cuáles considera que son los retos específicos que ha enfrentado en la investigación de estos delitos debido a la insuficiente legislación?				X				X				X	
	11	Proporcione ejemplos de obstáculos que ha encontrado en la recopilación de pruebas o en la identificación de los autores de estafas cibernéticas en su jurisdicción.				X				X				X	
5. Determinar los efectos de la insuficiente legislación persecutoria en la sanción del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	12	¿Cuáles son las implicaciones de la insuficiente legislación en la imposición de sanciones o penas por Delitos de estafa cibernética?				X				X				X	
	13	¿Cómo influye la carestía de regulación adecuada en la disuasión y prevención de la estafa cibernética en su distrito fiscal?				**X**				**X**				**X**	

Asimismo, a usted le presento la "GUÍA DE ANÁLISIS DOCUMENTAL" para la investigación titulada: "EFECTOS DE LA INSUFICIENTE LEGISLACIÓN PERSECUTORIA DEL DELITO DE ESTAFA CIBERNÉTICA EN EL DISTRITO FISCAL DEL SANTA, 2022". Elaborado por el Abog. Jean Carlos Acosta Zavaleta en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

Objetivos	Ítem		Claridad				Coherencia				Relevancia				Observaciones
			1	2	3	4	1	2	3	4	1	2	3	4	
3. Determinar los efectos de la insuficiente legislación persecutoria en la detección del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	1	El expediente describe cómo se detectó el delito (hechos)				X				X				X	
	2	Menciona las fuentes de información y dispositivos tecnológicos utilizados para la detección.				X				X				X	
	3	Se individualizó y detalló el papel de cada actor que posibilitó la detección del delito.				X				X				X	
	4	Describe la colaboración interinstitucional en la etapa de detección				X				X				X	
4. Determinar los efectos de la insuficiente legislación persecutoria en la investigación del delito de estafa cibernética en el distrito fiscal del Santa, 2022	5	Menciona los métodos y técnicas de investigación empleados, junto con su base legal.				X				X				X	
	6	Incluye información sobre órdenes judiciales y autorizaciones requeridas en la investigación.				X				X				X	
	7	Detalla la evidencia reunida durante la investigación, subrayando su admisibilidad (pruebas)				X				X				X	
	8	Describe la preservación y el manejo de la evidencia, cumpliendo con los requisitos de ley.				X				X				X	
5. Determinar los efectos de la insuficiente legislación persecutoria en la sanción del delito de estafa cibernética en el distrito fiscal del Santa, 2022.	9	En el desarrollo del proceso se incluyó información sobre audiencias judiciales y decisiones tomadas.				X				X				X	
	10	En el expediente, se han independizado y están debidamente desarrolladas las tres partes básicas de la sentencia: parte expositiva, motivación de hechos y derecho, y decisión.				X				X				X	
	11	Propiamente en la sentencia, el juzgador desarrolla claramente la motivación de hechos y derechos que llevaron a la decisión, justificando la pena impuesta.				X				X				X	
	12	Se detallan las penalidades impuestas a los culpables, incluyendo sanciones monetarias, penas de prisión, restricciones de acceso a la tecnología.				X				X				X	

	13	Se describe si se aplicaron circunstancias agravantes o atenuantes en la imposición de las penas.				X				X				X	

Firma del evaluador
DNI: 40172725

ANEXO 05: CODIFICACIÓN DE PARTICIPANTES

Tabla 25

Codificación de especialista

N°	CÓDIGO ASIGNADO	FUNCIÓN	DISTRITO JUDICIAL
1	**J-1**	Juez del juzgado penal colegiado permanente	Distrito judicial del Santa
2	**J-2**	Juez del juzgado penal unipersonal y juzgado penal colegiado itinerante	Distrito judicial del Santa
3	**J-3**	Juez del segundo juzgado penal unipersonal	Distrito judicial del Santa
4	**J-4**	Juez del juzgado penal de investigación preparatoria – NCPP	Distrito judicial del Santa
5	**J-5**	Juez superior de la segunda sala penal	Distrito judicial del Santa
6	**F-1**	Fiscal adjunto titular de la fiscalía provincial penal de Pallasca	Distrito Fiscal del santa
7	**F-2**	Fiscal adjunto titular de la fiscalía provincial penal de Pallasca	Distrito Fiscal del santa
8	**F-3**	Fiscal Superior – tercera fiscalía superior del santa	Distrito Fiscal del santa
9	**F-4**	Fiscal Adjunto – Segunda Fiscalía provincial penal del santa	Distrito Fiscal del santa
10	**F-5**	Fiscal Superior – Primera fiscalía superior del santa	Distrito Fiscal del santa

Fuente: Distrito fiscal del Santa, 2023**.**

Tabla 26

Codificación de carpetas fiscales

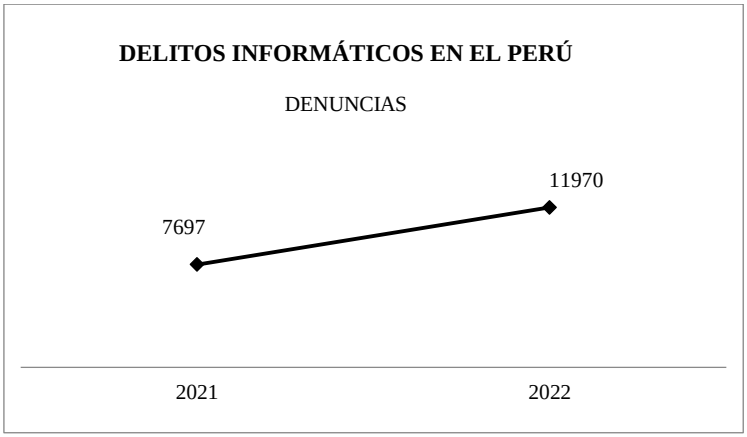
N°	CÓDIGO ASIGNADO	DELITO	DISTRITO FISCAL
1	**CF-1**	Estafa agravada	Distrito Fiscal del Santa
2	**CF-2**	Estafa agravada	Distrito Fiscal del Santa
3	**CF-3**	Estafa agravada	Distrito Fiscal del Santa
4	**CF-4**	Estafa agravada	Distrito Fiscal del Santa
5	**CF-5**	Estafa agravada	Distrito Fiscal del Santa
6	**CF-6**	Estafa agravada	Distrito Fiscal del Santa
7	**CF-7**	Estafa agravada	Distrito Fiscal del Santa
8	**CF-8**	Estafa agravada	Distrito Fiscal del Santa
9	**CF-9**	Estafa agravada	Distrito Fiscal del Santa
10	**CF-10**	Estafa agravada	Distrito Fiscal del Santa
11	**CF-11**	Estafa agravada	Distrito Fiscal del Santa
12	**CF-12**	Estafa agravada	Distrito Fiscal del Santa

Fuente: Distrito fiscal del Santa, 2023

ANEXO 06: FIGURAS DE INCIDENCIA DELICTIVA

Figura 1

Reporte de incidencia de delitos informáticos en el Perú.



Nota: Reporte Oficial de incidencia delictiva relacionada con los crímenes informáticos en el territorio peruano durante el periodo comprendido entre 2021 y 2022. ***Fuente*****:** Ministerio del Interior (2023)

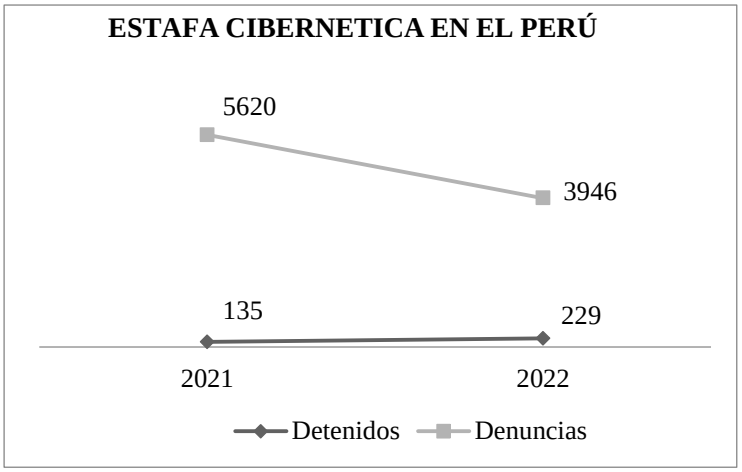
Figura 2

Reporte de incidencia de delitos estafa y otras defraudaciones en el Perú

Nota: Reporte Oficial de incidencia delictiva relacionada con los delitos de estafa y otras defraudaciones en el territorio peruano durante el periodo comprendido entre 2021 y 2022. ***Fuente*****:** Ministerio del Interior (2023)

Figura 3

Reporte de incidencia de estafa cibernética en el Perú, periodo 2021-2022



Nota: Reporte Oficial de incidencia delictiva relacionada con los delitos estafa cibernética en el territorio peruano durante el periodo comprendido entre 2021 y 2022, enfatizando los índices de denuncias y capturas. ***Fuente:*** Divindat (2023)

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 07: AUTORIZACIÓN

MINISTERIO PÚBLICO
REPÚBLICA DEL PERÚ

Decenio de la Igualdad de oportunidades para mujeres y hombres
Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho
PRESIDENCIA DE LA JUNTA DE FISCALES SUPERIORES DEL DISTRITO FISCAL DE SANTA

Señor:
JEAN CARLOS ACOSTA ZAVALETA
Correo electrónico: jean.acosta33@gmail.com
Presente. -

Asunto : Remite solicitud de autorización.

Referencia : Solicitud s/n de fecha 22 de febrero del 2024

Expediente : MUPDFS20240001301

Tengo el agrado de dirigirme a usted, para saludarla cordialmente y, al mismo tiempo, en atención al documento de la referencia, cursado por su persona, en relación a la solicitud de autorización para publicar la identidad en los resultados de su investigación "Efectos de la inadecuada legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa - 2022", **INFORMARLE** que este Despacho Superior, autoriza la publicación de su trabajo de investigación (Tesis), el nombre de "Distrito Fiscal del Santa", toda vez que esta tiene fines académicos; lo que se hace de conocimiento para fines pertinentes.

Sin otro particular, hago propicia la ocasión para expresarle mi mayor consideración.

Atentamente,

MIRIAM LUZMILA LUCERO TAMAYO
PRESIDENCIA DE LA JUNTA DE FISCALES SUPERIORES DEL DISTRITO FISCAL DE SANTA

cc:

MLT/sar
R.3648