



FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

Carrera de **DERECHO Y CIENCIAS POLÍTICAS**

“LA CADENA DE CUSTODIA EN EL FRAUDE
INFORMÁTICO: ANÁLISIS DE LA LEGISLACIÓN
PERUANA DE 2022”

Tesis para optar al título profesional de:

ABOGADO

Autor:

Jean Pierre Luis Firel Rojas

Asesor:

Dr. Michael Lincold Trujillo Pajuelo
<https://orcid.org/0000-0002-0757-2349>

LIMA - PERÚ

2023

JURADO EVALUADOR

Jurado 1 Presidente(a)	Alcides Pelayo Chavarry Correa
	Nombre y Apellidos

Jurado 2	Vanessa Anthuanet Vigil Ruiz
	Nombre y Apellidos

Jurado 3	Michael Trujillo Pajuelo
	Nombre y Apellidos

INFORME DE SIMILITUD

Jean Pierre

ORIGINALITY REPORT

12%

SIMILARITY INDEX

12%

INTERNET SOURCES

3%

PUBLICATIONS

7%

STUDENT PAPERS

PRIMARY SOURCES

1	tesis.ucsm.edu.pe Internet Source	1%
2	qdoc.tips Internet Source	1%
3	repositorio.uladech.edu.pe Internet Source	1%
4	pdfcookie.com Internet Source	1%
5	doku.pub Internet Source	1%
6	Submitted to Universidad Privada del Norte Student Paper	1%
7	vsip.info Internet Source	1%
8	dataonline.gacetajuridica.com.pe Internet Source	1%
9	moam.info Internet Source	1%

DEDICATORIA

Dedico esta investigación a todas las víctimas del delito de fraudes informáticos, con la esperanza de que el análisis de la cadena de custodia ofrezca un camino sólido para hacer frente a esta problemática y brindar justicia a quienes la necesita

AGRADECIMIENTO

Quiero expresar mi profundo agradecimiento, en primer lugar, a Dios por brindarme la invaluable oportunidad de vivir y experimentar este viaje llamado vida.

Agradezco sinceramente a la Universidad Privada del Norte por proporcionarme el entorno académico propicio para mi desarrollo.

A mis respetados docentes, les agradezco por su dedicación y compromiso en mi formación profesional, siendo piezas fundamentales en mi aprendizaje.

A mi asesor, por su guía constante y apoyo durante todo el proceso de investigación, siendo un faro en mi trayecto académico.

A mi familia, en especial a mi amada madre Antonia y a mi querida tía Gloria, les dedico un agradecimiento especial. Mi madre, por darme la vida y sacrificarse incansablemente para asegurarse de que nunca me faltara nada, siempre firme en su deseo de verme convertirme en un profesional de provecho. A mi tía Gloria, por sus acciones y consejos que me motivaron a ser una mejor persona y me recordaron la importancia de no rendirme ante las dificultades.

Finalmente, agradezco a mis amigos, quienes siempre estuvieron ahí, brindándome su apoyo incondicional. Su amistad ha sido un pilar fundamental en este recorrido. A todos, mi más sincero agradecimiento por ser parte esencial de mi camino.

TABLA DE CONTENIDO

JURADO EVALUADOR.....	2
INFORME DE SIMILITUD	3
DEDICATORIA	4
AGRADECIMIENTO.....	5
TABLA DE CONTENIDO	6
INDICE DE TABLAS	7
RESUMEN	8
CAPÍTULO I: INTRODUCCIÓN	9
CAPÍTULO II: METODOLOGÍA	27
CAPÍTULO III. RESULTADOS	32
CAPÍTULO IV. DISCUSIÓN Y CONCLUSIONES	59
REFERENCIAS	67
ANEXOS	74

INDICE DE TABLAS

Tabla 1: Análisis de la Revista Anales	33
Tabla 2: Análisis de la revista Discusiones	34
Tabla 3: Análisis de la revista Ficp	34
Tabla 4: Análisis de la revista Iusta	36
Tabla 5: Análisis de la Revista Teorder	37
Tabla 6: Análisis del Repositorio Dspace	38
Tabla 7: Análisis del Expediente RN N°001607-2021	50
Tabla 8: Análisis de la Revista Ecos Sociales	39
Tabla 9: Análisis de la Revista Semilla Científica	40
Tabla 10: Análisis de Tesis de la Universidad Siglo XXI	41
Tabla 11: Análisis del Diario la Ley N° 8859	42
Tabla 12: Análisis de Tesis de la Universidad de León	43
Tabla 13: Análisis de la Revista Chilena de Derecho y Tecnología	44
Tabla 14: Análisis de Tesis de la Universidad Cesar Vallejo	45
Tabla 15: Análisis de Tesis de la Universidad de Cuenca	46
Tabla 16: Análisis de la Revista de Información Tecnológica y sociedad	47
Tabla 17: Análisis de la Revista Informática Forense	48
Tabla 18: Análisis de la Revista Chilena de Tecnología y Derecho	49
Tabla 19: Análisis del Expediente N° 1607-2021	53

RESUMEN

El objetivo principal del estudio fue determinar cómo la incorrecta implementación de la cadena de custodia afecta el procesamiento de pruebas en el sistema judicial peruano y evaluar el impacto negativo en el tratamiento de pruebas. La metodología empleada fue cualitativa, con diseño de teoría fundamentada, tipo básico, nivel descriptivo. Se evidenció que la cadena de custodia de las pruebas ante la perpetración de delitos informáticos es deficientemente ejecutada, especialmente porque se trata de pruebas no tangibles, como correos electrónicos o mensajes telefónicos utilizados para obtener información bancaria o contraseñas que en milisegundos pueden ser borrados, suprimidos o alterados logrando obstaculizar el funcionamiento normal del sistema, y abordaje legal. Frente a esta índole, el sistema jurídico carece de los mecanismos y herramientas necesarias para afrontar estas situaciones con la debida severidad, lo que conduce a la impunidad. En conclusión, la cadena de custodia en comisiones de hecho por el delito en mención presenta deficiencias críticas, puesto que el sistema jurídico muestra carencias significativas al no contar con los mecanismos y herramientas necesarios para abordar estas situaciones con la severidad requerida, lo que resulta en un riesgo latente de impunidad.

Palabras Clave: cadena de custodia, fraude informático, evidencias digitales

CAPÍTULO I: INTRODUCCIÓN

1.1. Realidad problemática

Desde la década de 1960, de acuerdo con Egocheaga (2016). la tecnología no ha cesado de evolucionar, llevándonos a la era digital actual. En el mundo moderno, es indiscutible que "Internet es un sistema mundial de comunicación entre personas, caracterizado por su capacidad de transmitir información a gran velocidad, incluyendo datos que antes eran privados. No está limitado por el espacio, el tiempo ni fronteras nacionales".

Hoy en día, mantener la privacidad se ha vuelto cada vez más complicado debido a la rapidez con la que las Tecnologías de la Información y las Comunicaciones (TIC) recopilan datos de maneras y lugares inesperados. Esto presenta un desafío para los sistemas legales, que deben asegurar la protección de los derechos humanos, especialmente en lo referente a delitos informáticos.

Además, el avance tecnológico de Internet ha dado lugar a las redes sociales, que se han transformado en una plataforma clave para las relaciones interpersonales en la sociedad, con el objetivo principal de compartir información. En el contexto internacional, hay numerosos casos relevantes, entre ellos El País (2015). Se refiere a la red social AshleyMadison.com, un sitio web donde los usuarios buscaban encuentros extramatrimoniales. Un grupo de hackers conocidos como "The Impact Team" comprometió la base de datos de la compañía propietaria de esta página, resultando en el robo de información de aproximadamente 37 millones de usuarios. Este incidente es un claro ejemplo de cómo se vulneró la privacidad y la vida íntima de los usuarios de AshleyMadison.com, quienes esperaban anonimato y seguridad en la información proporcionada a la plataforma. A pesar de las consideraciones morales sobre los servicios de AshleyMadison.com, el robo de datos y las consecuentes prácticas delictivas, como la extorsión, son injustificables.

Es así como Torres (2018), señala que otro caso relevante ocurrió en 2017 cuando el Departamento de Seguridad Nacional de EE. UU. solicitó a Twitter datos de usuarios que criticaban al entonces presidente Donald J. Trump. Esto incluía nombres, números de teléfono, correos electrónicos y direcciones IP. Twitter respondió demandando al Gobierno, argumentando que esta solicitud violaba la Primera Enmienda de la Constitución de EE. UU. Esta enmienda protege el derecho de los usuarios a expresarse políticamente bajo seudónimo en la plataforma, y la acción del gobierno podría generar un "Chilling Effect", disuadiendo a los usuarios de ejercer su libertad de expresión en redes sociales. Aunque la controversia se disipó cuando el gobierno desistió de su solicitud, este caso planteó serias dudas sobre la expectativa de privacidad en la información que las personas comparten voluntariamente en redes sociales. Este tema ha sido explorado en la jurisprudencia estadounidense. Inicialmente, la Corte Suprema de los Estados Unidos sostenía que las personas no podían esperar privacidad sobre la información que compartían voluntariamente con terceros. Sin embargo, con el advenimiento del mundo virtual, opiniones recientes de jueces de la Corte Suprema y de expertos en la materia sugieren que esta perspectiva necesita ser revisada. Se reconoce ahora que la privacidad no es simplemente el opuesto de lo público y que el secreto no es un requisito para la privacidad. En cambio, su función principal debería ser otorgar a los ciudadanos control sobre ciertos aspectos de sus vidas

Casos como U.S v. Jones (2012) y Packingham v. North Carolina (2017) han tratado la cuestión de la privacidad en la era digital, reconociendo cómo Internet, las nuevas tecnologías y, por extensión, las redes sociales, han afectado la percepción de la intimidad. Estos casos establecen que los usuarios de redes sociales tienen derecho, bajo la Primera Enmienda, a compartir información sin renunciar al control sobre su identidad pública. Sin embargo, aplicar esta doctrina de forma generalizada podría ir en contra de los principios constitucionales estadounidenses, dados los cambios en las relaciones interpersonales

provocados por la tecnología, sugiriendo la necesidad de un análisis individualizado de cada caso de privacidad en el ámbito virtual, como un proceso de custodia de pruebas en un proceso de estos mismos, de tal forma que los delitos informáticos, sea por internet o empleando algún otro método análogo, sea resuelto de la forma más efectiva.

En Perú, la evolución digital también ha tenido un impacto significativo, especialmente en la comunicación masiva. Esto ha llevado a una mayor difusión de información privada o de dominio público, lo que a su vez ha generado tensiones entre el derecho a la privacidad y las libertades comunicativas, así como fraudes informáticos, o el manejo de pruebas en cuanto a cadenas de custodia.

Desde la puesta en vigencia la ley N°30096 Ley de delitos informáticos y su última actualización en el Nuevo Código Procesal Penal, se ha generado una serie de cuestiones acerca de la cadena de custodia y como esta afecta el proceso penal con el uso de las nuevas tecnologías, específicamente en los casos de fraude informático que se encuentra en la cúspide de delitos informáticos en estos últimos años, dicha preocupación es por la falta de conocimiento de la recolección de medios de prueba o indicios, siendo que la recolección de los mismos son incorporados sin las medidas de protección idóneas, dando como resultado un obstáculo al momento de sentenciar por parte de los magistrados, del mismo modo que se coloca en tela de juicio la condena o absolución de un sujeto, debido a que los abogados que se encuentran defendiendo a su patrocinado podrán aprovechar el incorrecto manejo de la cadena de custodia para absolver al acusado.

En cuanto a la cadena de custodia ha tomado relevancia para los operadores de justicia por lo crucial que este es dentro de los procesos penal y más aún cuando se refiere a delitos informáticos, donde las evidencias son el contenido dentro de los sistemas informáticos no pueden ser palpables o tocables, entre la variedad de fraudes podemos encontrar la utilización de correos electrónicos o mensajes telefónicos con el fin de obtener

información bancaria o contraseñas, del mismo modo el borrado, supresión o alteración de datos con el objetivo de impedir el normal funcionamiento del sistema entre otros más tipos de fraude informático. Es deplorable encontrar que la cadena de custodia es contaminada por no entender que estas requieren un cuidado distinto al resto, porque no es un objeto que se pueda tocar o apreciar a simple vista, en tanto la policía no muestra una capacidad para realizar de manera idónea la recolección de indicios, embalaje y el transporte de este.

Por lo mencionado líneas anteriores causo el estudio de este trabajo de investigación, en donde la cadena de custodia resulta un medio de prueba indiscutible frente a los diversos tipos de fraude informático, por ello permitirá otorgar veracidad al momento de crear convicción al juez y por ello pueda dictar responsabilidad penal.

Es así como Paternina (2018), refiere que la cadena de custodia en los delitos informáticos tiene como objetivo prevenir cambios o alteraciones en los materiales relacionados con un crimen para mantener su validez como prueba en la investigación del delito. Por ello, es necesario seguir un estricto protocolo técnico con estos elementos, desde su recolección hasta su almacenamiento. Estos protocolos limitarán el acceso a las pruebas y permitirán identificar a los responsables en caso de manipulaciones indebidas o intentos de acceso sin autorización. Recomendando a través de conocimientos forenses que el momento adecuado para realizar el procedimiento, que busca minimizar la destrucción de equipos o datos, aprovechando que el sospechoso podría estar en línea, y garantizando la seguridad de los investigadores, como también la necesidad de entrar sin previo aviso para evitar que se destruyan o alteren los equipos o la evidencia que contienen. Por otra parte, refiere que se debe llevar a cabo allanamientos e incautaciones en distintos lugares al mismo tiempo, ya que los datos pueden estar distribuidos en varios sitios, incluyendo sistemas de red y conexiones remotas, así como buscar documentos que contengan información sobre acceso, conexiones en redes, entre otros detalles relevantes.

Por otra parte, Peñaloza (2022) refiere que la cadena de custodia es crucial en un proceso judicial para garantizar un juicio imparcial, justo y objetivo. Tras un delito, los agentes que llegan al lugar, ya sea físico o virtual, donde se cometió, inician una serie de procedimientos estandarizados para preservar la integridad y proteger las pruebas y evidencias. Es esencial que estas operaciones se realicen de manera que no dejen lugar a dudas sobre su validez. Así, los análisis o estudios llevados a cabo por peritos cualificados estarán sólidamente fundamentados. Cuando estas pruebas se presenten en el juicio, deben ser consideradas como evidencia fiable, ofreciendo al juez una visión clara y convincente de los hechos ocurridos.

La Cadena de Custodia, en términos propios, se refiere a una serie de procedimientos que son legalmente establecidos por las leyes actuales. Estos procedimientos facilitan la investigación de huellas y pruebas para asegurar su aceptación por la justicia. Es fundamental que no existan dudas sobre su integridad, autenticidad, seguridad y, en caso necesario, que se establezca claramente la conexión entre el delito cibernético, el lugar del suceso y las personas acusadas, asegurando así la existencia de un vínculo causal. El objetivo de la cadena de custodia es asegurar que los indicios y pruebas analizados en el laboratorio y presentados en juicio sean exactamente los mismos que se recolectaron en la escena del crimen, manteniendo así su autenticidad y valor como prueba.

En el ámbito del proceso penal, la cadena de custodia nos informa sobre las acciones llevadas a cabo, los datos obtenidos, y las personas responsables, incluyendo los nombres de los peritos que intervinieron y las investigaciones realizadas a las pruebas. Además de las evidencias, forman parte de la cadena de custodia todos los documentos relacionados, como actas, fichas identificativas y registros legales, asegurando que solo personas autorizadas han tenido acceso a la evidencia y que se ha preservado su estado original. Si este no fuera el caso, los custodios, que incluyen a la Policía Judicial, el custodio, el perito y la Fiscalía,

deben demostrar que no intentaron alterar las pruebas. En caso de negligencia, se tomarán las acciones legales correspondientes. Siendo ello, La cadena de custodia se enfoca en tres metas principales. En primera instancia recolectar huellas y pruebas en la escena del crimen, siguiendo procedimientos que aseguren su originalidad e integridad, lo cual refuerza el debido proceso legal. En segunda instancia, adherirse a protocolos científicos para prevenir alteraciones, degradaciones, contaminaciones y destrucción de las pruebas recopiladas. Esto incluye documentar quiénes han tenido contacto o acceso a las evidencias, el tiempo que estuvieron bajo su custodia, así como las pericias forenses realizadas, asegurando así una custodia efectiva. Y finalmente, presentar en el juicio las evidencias y los informes para que sean evaluados por la autoridad competente, demostrando su autenticidad, integridad, preservación, seguridad, almacenamiento, continuidad y registro detallado.

Asimismo, Rubio (2016), referente a la normativa española, señala que, en varias ocasiones, los Tribunales han rechazado la validez de pruebas informáticas en procesos judiciales debido a la ruptura de la cadena de custodia. La cadena de custodia es crucial en el manejo de pruebas informáticas, ya que determinar si una prueba ha sido alterada es un asunto claro y dicotómico: la prueba está alterada o no lo está. Si la prueba permanece inalterada desde su recolección hasta su análisis forense, se considera que la cadena de custodia se ha mantenido. Cualquier cambio, accidental o intencionado, en la prueba compromete su autenticidad y la invalida. Desde su recolección hasta su análisis, la prueba enfrenta varios procesos. Inicialmente, se identifica, luego se sella, etiqueta, inventaría y almacena, quedando siempre bajo la custodia de un funcionario público como un letrado de la administración de justicia. Este funcionario actúa como fedatario público. Eventualmente, la prueba se analiza ante este funcionario o su sustituto, según lo autorice la Ley y la jurisprudencia. Cualquier cambio en el estatus de la prueba, como su desprecintado para análisis o un cambio en el custodio, debe registrarse en un acta firmada por los funcionarios

relevantes. Cualquier cambio en el estatus de la prueba que no esté debidamente documentado y firmado puede generar sospechas sobre la integridad de la cadena de custodia, especialmente si la prueba es incriminatoria. En España, las leyes procesales civiles y criminales no contienen disposiciones específicas sobre la conservación de la cadena de custodia de las pruebas, ni existen reglamentos que orienten a los funcionarios en este sentido. Las prácticas en este ámbito se basan en el sentido común, la buena fe, la presunción de veracidad de los funcionarios y la jurisprudencia. Un ejemplo de cómo se aborda la cadena de custodia en España se encuentra en la STS 1190/2009, que enfatiza la importancia de mantener la "mismidad de la prueba", asegurando que lo que se traslada y analiza es idéntico a lo recogido en la escena del delito. Es por ello por lo que mantener la cadena de custodia asegura que una prueba es auténtica y no ha sido alterada. Respecto a las evidencias informáticas, la STC 170/2003 establece que la inclusión de soportes informáticos en un proceso penal debe garantizar la identidad completa e integridad del contenido original. Esto implica que los resultados de las pruebas periciales se basen en los mismos soportes recogidos, asegurando que no se haya manipulado su contenido.

Es así como es de suma importancia darle la preponderancia debida a la cadena de custodia, de tal forma que se proyecte un buen trabajo referente a los delitos informáticos.

Es así como, para hacer frente a los crecientes delitos cibernéticos que han alcanzado su punto máximo en 2019 y en el último año 2020, en comparación con años anteriores, y debido a la nueva realidad global a la que se viene adaptando, donde las transacciones humanas (compras, ventas, pagos, operaciones bancarias, etc.) se realizan en línea, y donde la población está siendo afectada por nuevas formas de delitos que ya no ocurren en las calles como antes, sino en internet.

En España, de acuerdo con el Informe sobre el estado de internet en términos de seguridad de Akamai, las estafas en línea aumentaron un 45% en comparación con el año

2019, causando pérdidas de aproximadamente 3,400 millones de dólares. Estas estafas se llevaron a cabo mediante varias técnicas cibernéticas, incluyendo el phishing. En México, la pandemia de Covid-19 ha provocado un aumento en los ataques cibernéticos, la mayoría efectuados a través de correos electrónicos. Diariamente se interceptan 324 mil intentos de fraude, lo que equivale a unos 225 por minuto y 4 cada segundo. Este incremento se atribuye a que los delincuentes cibernéticos han desarrollado nuevas técnicas para cometer delitos.

En Perú, se promulgó una ley penal especial con el objetivo de prevenir y sancionar actos ilegales que afectan a los sistemas y datos informáticos, el secreto de las comunicaciones y otros bienes jurídicos protegidos que se vean perjudicados por esta clase de delitos, como el patrimonio, la fe pública, el orden financiero y monetario, y la independencia sexual.

Fue así que el 22 de octubre de 2013 se publicó la Ley N°30096, Ley de Delitos Informáticos, la cual luego fue modificada por la Ley N°30171 el 10 de marzo de 2014. Esta ley, en lugar de abordar temas no incluidos en el Código Penal de 1991 y la Ley N°30096, presentó varias inconsistencias y lagunas en su regulación de delitos informáticos. Incluso llegó a ser redundante con respecto a lo ya estipulado en el Código Penal vigente, resultando en una sobre-regulación. Considerando que la globalización alcanza niveles sin precedentes, nuestro marco legal debería adaptarse para enfrentar eficazmente amenazas cibernéticas, definiendo claramente y con rigor las diferencias y especificaciones de cada uno de estos delitos.

El Código Penal de Perú incluía el Capítulo X, "Delitos Informáticos", añadido por el artículo único de la Ley N° 27309 el 17 de julio de 2000. Este capítulo, que abarcaba los artículos 207-A a 207-D, definía varios tipos penales para este tipo de infracciones contra bienes jurídicos. Sin embargo, estos artículos fueron derogados por la disposición complementaria derogatoria única de la Ley N°30096, publicada el 22 de octubre de 2013,

que más tarde fue modificada por la Ley N° 30171. Específicamente, el artículo 207-A del Código Penal establecía que aquellos que accedieran o utilizaran indebidamente bases de datos o sistemas de redes de computadoras para diseñar, ejecutar, alterar, interferir, interceptar, acceder o copiar información serían sancionados con hasta dos años de cárcel o con prestación de servicios comunitarios.

En la actualidad, los sistemas informáticos no solo se utilizan como herramientas auxiliares en diversas actividades cotidianas, sino que también facilitan la obtención y manejo de información, funcionando como medios de comunicación. Debido a esto, la informática está presente en casi todas las ocupaciones, reemplazando tareas que anteriormente se realizaban manualmente. Esto ha llevado a la digitalización de la información, almacenada en computadoras, servidores y medios virtuales, lo que la hace vulnerable a accesos no autorizados.

La rápida evolución en la potencia, funcionalidad y variabilidad del software y del hardware informático ha sido tal, que anteriormente se podía estar seguro de que era imposible sustraer cierta información específica. No obstante, con el avance de la globalización y el crecimiento de las industrias de la computación e informática, se ha desarrollado un sistema capaz de almacenar y transmitir grandes cantidades de datos en instantes, facilitando el acceso a esta información a un número creciente de personas, mientras las legislaciones luchan por mantenerse al día.

Los avances tecnológicos globales y la capacidad de almacenamiento de los dispositivos electrónicos actuales hacen más compleja la vigilancia y regulación de estos dispositivos y del comportamiento de sus usuarios. Estos últimos están además influenciados por presiones sociales que promueven nuevas formas de ganar dinero. Es vital monitorear estos avances tecnológicos y su impacto en el entorno de los individuos. Los delitos informáticos, han evolucionado junto con las tecnologías de la información, sumergiendo a

la sociedad en un proceso de desarrollo y mejora en todas sus áreas, incluyendo la delincuencia, que ahora puede cometer ilícitos desde cualquier parte del mundo, con un gran alcance informático y de forma anónima Fuentes (2021).

Del mismo modo es de consideración que la preparación, actualización y capacitación a los órganos que dan apoyo en la investigación como la Policía Nacional del Perú que no comprenden la magnitud de los hechos delictivos, por lo general no saben cuál es el cuidado debido pretendiéndose así realizar un método de recolección de indicios paupérrimo.

Es crucial señalar que la finalidad de este estudio analizar cómo influye el incorrecto uso del procedimiento de la cadena de custodia en casos de fraude informático, por ello Gonzales (2021) hace relación que la prueba en términos forenses, se pueden afirmar que las evidencias digitales obtenidas sean reunidas de manera apropiada y con ninguna probabilidad de alteración, acatando así la cadena de custodia., con el fin de persuadir al tribunal de que la exposición es verdadera y que nadie ha modificado la prueba.

El conocimiento de fraude informático es enlazado con la utilización, modificación de los datos o programas del sistema informático; donde se establecen las conductas que se materializan en la suplantación de la identidad, vulneración al secreto a las comunicaciones, entre otras. Tal es el caso que los autores Mayer y Oliver (2020) plantean una noción similar, dado que ellos señalan que debe existir una manipulación de los sistemas informáticos, donde se debe tener en cuenta que la definición precisa del fraude informático debe basarse en tres factores vinculantes: el comportamiento del agente, el resultado y el ánimo.

El tratamiento en la cadena de custodia digital nos permite establecer en forma correcta la identidad, integridad y autenticidad en aquellos rastros digitales o pruebas relacionadas con un delito desde el momento de su descubrimiento hasta que estén disponibles como prueba en el juicio. La intención es garantizar aquella identidad verdadera

en los datos incautados y analizados. Por lo tanto, la cadena de custodia digital tiene un valor instrumental ya que sirve para garantizar que lo que se analiza y presenta como prueba en el tribunal sea coherente con la evidencia digital recopilada.

Ahora bien, en el contexto nacional señala Divindat (2020) realizó un análisis con respecto a las denuncias y casos denunciados sobre el delito de fraude informático, arrojando los siguientes resultados donde se registra que desde el año 2020 ha crecido a 4168 denuncias, mientras que el año siguiente ascendió a la cifra 5620 denuncias siendo este año la más alta con respecto a los próximos años, estos delincuentes según estadísticas son de origen peruano, que utilizan nombre de ciudadanos de nacionalidad extranjera.

Asimismo, Solís (2016) señala que los integrantes de la PNP deben conocer los reglamentos de en la cadena de custodia, en razón que se comete secuencia de indicios materiales que son manipuladas de manera incorrecta durante la función investigativa, lesionando las garantías que forman parte del Estado constitucional de derecho y en contra de él. Sobre las bases de las ideas expuestas es necesario conocer y respetar las fases de la cadena de custodia, las cuales son: la extracción - almacenamiento de datos, la protección - empaque de la prueba y por último el transporte de la prueba; ya que esto permite cumplir con el debido proceso.

En consideración a ello, Araujo y Huanca (2018), señalan que, con la adopción del modelo acusatorio en el derecho penal, se abandonaron las prácticas ilegítimas del modelo inquisitivo, como la tortura, en busca de evidencia incriminatoria. Este cambio se alinea con el progreso social, técnico y científico, desechando las prácticas inquisitivas. Actualmente, el proceso penal acusatorio se caracteriza por ser garantista. La ley ha reformado la metodología de investigación de delitos por parte de la Policía Nacional, asignando la investigación primordialmente al Ministerio Público. Sin embargo, esto no margina a la policía, sino que representa una oportunidad para su modernización y fortalecimiento

institucional en la investigación delictiva y el desarrollo de la criminalística, promoviendo su integración sistemática con otros operadores del sistema procesal penal.

El nuevo papel asignado a la policía en el sistema de justicia penal es de colaboración más estrecha con otros operadores del sistema, especialmente con el fiscal del caso. Su tarea es investigar delitos de manera coordinada, ayudando al fiscal a fundamentar acusaciones con pruebas fácticas, manejadas adecuadamente a través de la cadena de custodia y legalmente incorporadas al proceso. Los policías deben estar preparados para defender oralmente sus hallazgos y métodos, tanto en situaciones de delitos flagrantes como en el manejo de evidencias en la escena del delito y su traslado. En el sistema actual, se enfatiza la importancia del trabajo profesional de investigadores, peritos y expertos en criminalística, dejando atrás la era en la que policías sin especialización dirigían las investigaciones. Bajo la dirección del fiscal y el control del juez de investigación preparatoria, la policía especializada ahora maneja ciertas diligencias iniciales y participa activamente en la cadena de custodia. Esto implica una mayor colaboración desde el inicio del caso (noticia criminal) y la necesidad de seleccionar y capacitar a efectivos policiales dedicados exclusivamente a la investigación criminal para garantizar el éxito de la fase preparatoria y sustentar adecuadamente una acusación fiscal.

Respecto a la ciudad de Lima Metropolitana, Leyva (2021) establece que la tecnología trae consigo grandes beneficios como brindar herramientas para reducir esfuerzos y tiempo en la vida de cada persona, nuestra sociedad estos últimos años ha presenciado el indebido uso de esta misma tecnología para la comisión de delitos, uno de los principales delitos es el fraude informático que ha constituido la vulneración del patrimonio de los ciudadanos, asegurando que la evolución tecnológica ha dado lugar a nuevas formas de delitos que utilizan los sistemas informáticos e Internet, es ahora de es importante saber el cuidado que se debe tener a la hora de recolectar las evidencias, debido a que estas no son

objetos si no se encuentran en la red.

Antecedentes de la investigación

Con lo que respecta a los avances a nivel internacional se encontró las siguientes investigaciones:

Gamboa (2021) en su investigación efectuada en la ciudad de Bogotá- Colombia, llegó a la conclusión que la cadena de custodia es nueva en el litigio, por lo que habrá abogados litigantes que se muestren desorientados al aporte de pruebas y en la contradicción en el juicio oral. Estos abogados desconocen los estándares constitucionales y legal acerca del tema,

Por tanto es perjudicial que las evidencias que se pretendan incorporar como pruebas ante el juez, se decrete como invalidas por adolecer de una o varias afectaciones en la cadena de custodia, por ello se estaría excluyendo, rechazando o señalando como inadmisibles como medio de prueba, dado que no se cumple el valor demostrativo del elemento probatorio y del mismo lado su autenticidad, en tal sentido se perderá credibilidad a la hora de relacionar a la víctima con el imputado y con la escena del crimen, en el peor de los casos se absolverá al imputado o de manera injusta sentenciar a un inocente por no poder defender su postura por una mala praxis en la cadena de custodia, ya que la fiscalía general de la Nación no tiene exclusivamente la responsabilidad de protegerla, sino que lo será también el Defensor quién tiene que protegerla para que al final los elementos que son materiales probatorios sean oficialmente tomados como pruebas.

Ajhuacho (2021) realizó una investigación en Bolivia, bajo el título de “La necesidad de implementar un manual para el manejo de cadena de custodia”, donde afirma que el incumplimiento de este genera la exclusión de la prueba porque se vulnera el principio de legalidad de la prueba, por ello es de urgencia implementar un manual que

proteja los elementos de prueba que se recolectan en la etapa de investigación, debido a la relevancia que tendrá la situación jurídica de los sujetos que forman parte del proceso penal.

Gonzales et al. (2021) realizaron su estudio en Panamá acerca del manejo adecuado de cadena de custodia en el nuevo proceso penal concluyeron lo siguiente que el objeto que forma parte de la evidencia por sí solo no es pertinente para el Juez, por ello antes debe probarse que se encuentran en las condiciones encontradas en los hechos que forman parte del delito, es decir que estas no hayan sufrido modificación alguna o modificación que influya en el resultado que emitirá el juzgador.

Por medio de la utilización del protocolo de cadena de custodia se analizará si la evidencia es auténtica y que esta ha cumplido con el manejo, almacenamiento y traslado por los operadores de justicia, este protocolo es indispensable para las partes en caso más especial para la defensa, además de la construcción de teorías acerca de lo que sucedió.

Gonzales (2021) efectuó un estudio en España acerca de la prueba pericial digital y la relación con cadena de custodia afirmando que, El derecho cumple nuevos retos debido a las nuevas tecnologías, siendo que los delitos informáticos requieren un tratamiento distinto a un delito habitual, por tanto cuando hay ausencia del control judicial de las evidencias y estas se pretenden introducir al proceso penal sin existencia de las obligatorias garantías de custodia policial y el control judicial sobre la integridad e identidad, nos encontramos en algo altamente grave, debido que no se trata de una protección simplemente legal, sino de una que tiene un impacto en la validez constitucional de la prueba, por tanto afectará al momento de dictar o absolver una sentencia.

Paternina (2018) en el estudio presentado en la actual ciudad de Cartagena sobre las vulnerabilidades existentes del protocolo de cadena de custodia de las evidencias en delitos informáticos concluyendo que la evidencia informática son impugnadas o refutadas debido a su facilidad de ser borrada, duplicada o modificada en otros dispositivos informáticos, por

tanto resulta en un peligro para la justicia el incumplimiento del correcto procedimiento de cadena de custodia en este tipo de delitos informáticos, toda vez que el éxito en la reconstrucción del escenario del delito depende del cumplimiento de las exigencias técnicas y legales de este procedimiento.

Por otro lado, se revisó investigaciones de contexto nacional, es así que Mostajo (2021) presento en la ciudad de Lima, una investigación acerca de cadena de custodia de medios probatorios, Afirmando que son cruciales las consideraciones que deben tomarse en el proceso con relación a la cadena de custodia, por ello un trato incorrecto de las evidencias podrá originar inconvenientes que condicionarán la forma correcta en el curso del proceso penal, esto debido que en el recojo de evidencias los efectivos policiales no cuentan con las medidas necesaria para el tratamiento, además que en algunos casos los efectivos de la policía han hecho manipulación para que uno de los procesados obtenga ventaja.

El conocedor Gonzales (2019) planteo una investigación en la ciudad de Chiclayo, sobre la relevancia de la cadena de custodia dentro del proceso penal mencionado que, cuando ocurre un acontecimiento delictual el personal de la policía llega al escenario donde se cometió el crimen, uno de los actos más relevantes que se deben ejecutar es justamente la recolección de evidencias físicas o los elementos materiales como los suelen ser las huellas, proyectiles entre muchos más, para preservar, conservar, mantener el lugar de los hechos, etc. Sin embargo, el incumplimiento en el procedimiento implica que se pierda el soporte o contenido afectando la evidencia que será materia de evaluación dentro del proceso penal, por tanto, esto perjudica a los sujetos para sustentar su defensa o en el apoyo a la parte contraria para solidificar su posición.

Los estudios Carrillo y Montenegro (2018) llevo presente una investigación en la provincia de Calca, estableciendo que el país no posee procesos idóneos para proteger los indicios que se obtengan en el lugar de los hechos, debido que las normas del código penal

señalan al ministerio público como la entidad que protegerá los indicios más cercanos que se pueden usar en el litigio, además que en otros apartados se menciona que las pruebas de mayor relevancia serán protegidas, sin embargo no se menciona cual es el proceso ni el cuidado que se debe tomar a fin de que la cadena de custodia no se rompa o vea afectada, porque esta afectación trae como consecuencia la no autenticidad de la prueba, por tanto se verá reflejada en un veredicto alejado de la realidad en la sentencia emitida por el juez.

La gestión inadecuada del proceso de recoger indicios o los medios probatorios, así como lo es la cadena de custodia por lo general se realizan sin la mediad de protección de seguridad, por tanto, implica que es un problema para los magistrados al momento de ejecutar una sentencia, al punto de absolver la condena del acusado.

Asimismo Monge (2022) en su investigación realizada en la ciudad de Lima, establece que la ausencia de capacitación y especialización acerca de la anteriormente mencionada cadena de custodia y el rompimiento de este perjudica los procesos penales al momento que se quiere valorar una evidencia, además de perder valor probatorio, por tanto, sale a la luz la posibilidad de resquebrajar una adecuada administración de justicia.

Finalmente Rodríguez (2021) planteo una investigación en la ciudad de Huancayo, en la cual señala que el uso de la cadena de custodia pertenece al soporte principal dentro de la investigación, donde la Fiscalía sostendrá su acusación, sin embargo, esta no se realiza de manera idónea, dado que no se encuentran en el lugar correcto, por tanto, tienden a destruirse de manera paulatina.

Por lo expuesto, se planteó como problema de investigación ¿Cómo influye el incorrecto uso del procedimiento de la cadena de custodia en casos de fraude informático, y cuáles son las implicaciones prácticas y teóricas de estos procedimientos en el procesamiento de pruebas en el sistema judicial en Perú durante el año 2022?.

1.2. Formulación del problema

1.2.1. Problema general

¿Cómo influye el incorrecto uso del procedimiento de la cadena de custodia en casos de fraude informático, y cuáles son las implicaciones prácticas y teóricas de estos procedimientos en el procesamiento de pruebas en el sistema judicial en Perú durante el año 2022?

1.2.2. Problemas específicos

¿Cuáles son las consecuencias del incorrecto uso del procedimiento de la cadena de custodia en Perú durante el año 2022?

¿Cuáles son las consecuencias del procesamiento de pruebas en el delito de fraude informático cuando no cumple un correcto uso de la cadena de custodia en el sistema judicial en Perú durante el año 2022?

1.3. Objetivos

1.3.1. Objetivo general

Determinar cómo influye el incorrecto uso del procedimiento de la cadena de custodia en casos de fraude informático, y cuáles son las implicaciones prácticas y teóricas de estos procedimientos en el procesamiento de pruebas en el sistema judicial en Perú durante el año 2022

1.3.2. Objetivo específico:

Determinar cuáles son las consecuencias del incorrecto uso del procedimiento de la cadena de custodia en Perú durante el año 2022.

Determinar cuáles son las consecuencias del procesamiento de pruebas en el delito de fraude informático cuando no cumple un correcto uso de la cadena de custodia en el sistema judicial en Perú durante el año 2022.

1.4. Supuesto

El supuesto dentro de un trabajo de investigación resulta no necesaria cuando está es de tipo cualitativa, dado que esta te permite explorar y expandir los conocimientos acerca del tema, recopilando datos no numéricos, como lo son las observaciones, documentos entrevistas y otros registros de información, por ello este tipo de investigación tiende a desarrollar teorías a partir de recopilación de datos, en lugar de probar los supuestos existentes, acerca del mismo nos señala Amaiquema et al. (2019) En la investigación cualitativa se puede prescindir de la formulación de supuestos porque no se hacen presuposiciones, el objetivo es examinar subjetivamente la interpretación que los sujetos hacen sobre los fenómenos de la realidad de estudio, en consecuencia carece de mediciones posibles.

CAPÍTULO II: METODOLOGÍA

2.1. Enfoque de la investigación

Según Hernández et. al (2014), el enfoque cualitativo se enfoca en una comprensión más profunda con el análisis detallado y minucioso de la realidad social. Este enfoque se basa en la recopilación y evaluación de datos que no se expresan en términos numéricos, como el lenguaje y teoría, lo que permite obtener una comprensión más contextualizada de la realidad social. Es especialmente adecuado para explorar fenómenos complejos, así como para investigar perspectivas y experiencias que no son cuantificables.

El actual trabajo de investigación tuvo un enfoque cualitativo, en razón que se realizó por medio de distintos datos teóricos tales como documentación, doctrina y jurisprudencia, mismos que ayudaron a visualizar de forma más completa el fenómeno de estudio, así como recolectar datos válidos y verídicos.

2.2. Tipo de investigación

Es importante destacar que la investigación fue de tipología básica o fundamental, ya que según Hernández y Mendoza (2018), se centra en la adquisición de nuevos conocimientos y en la contribución a los principios teóricos ya establecidos sobre un fenómeno específico.

La investigación realizada fue de tipo básica porque tuvo como objetivo la obtención de conocimientos teóricos sin una aplicación o utilidad práctica inmediata, es por ello que resultó útil para un mejor entendimiento acerca de la cadena de custodia y el fraude informático, asimismo Baena (2014) indicó que una investigación de tipo básico es cuando el estudio de un problema se dirige únicamente al incremento de conocimiento sobre un área específico.

2.3. Nivel de investigación

El nivel de la investigación fue descriptivo, ya que, conforme a Hernández et al.

(2010), se caracteriza por la descripción del fenómeno o situaciones tal como se presentan en su contexto, sin manipulación de estas.

Este nivel de estudio ayudó a una representación detallada y precisa de la realidad estudiada, proporcionando una visión clara y detallada de la cadena de custodia en la regulación normativa peruana.

2.4. Diseño de investigación

La presente investigación se guio bajo el diseño de teoría fundamentada el cual, según Hernández et al. (2014) busca generar teoría a través de un proceso inductivo y sistemático de análisis de datos. Implica la recopilación y análisis continuo de datos, permitiendo que las teorías emerjan directamente de los patrones y conceptos identificados en los datos recopilados, en lugar de aplicar teorías preexistentes. La teoría fundamentada se caracteriza por su naturaleza flexible y abierta, centrada en descubrir patrones emergentes, lo que la hace especialmente adecuada para explorar fenómenos complejos y poco comprendidos en diversos campos de estudio.

La aplicación de la teoría fundamentada fue fundamental en la investigación sobre la implementación de la cadena de custodia en el delito de fraude informático en Perú durante el año 2021, ya que permitió realizar una indagación exhaustiva a través de la revisión y análisis de diversos documentos, doctrina, jurisprudencia y teorías relacionadas con el tema.

Además, facilitó la identificación de patrones emergentes y la conexión de conceptos relevantes, contribuyendo así a una comprensión más profunda de la aplicación de la cadena de custodia en el contexto específico del fraude informático en el ámbito legal peruano.

2.5. Población y muestra

Al respecto, Hernández et al. (2014), señala que la población es un conjunto completo de elementos, individuos, objetos o unidades que comparten características comunes y son objeto de estudio en una investigación. Esta agrupación puede variar según el contexto,

abarcando desde la totalidad de personas en una región geográfica específica hasta elementos específicos en un estudio experimental.

La población estuvo compuesta por casuísticas derivadas por el delito fraude informático registrados en Perú, jurisprudencia, y documentos relacionados con el fenómeno de investigación.

Ahora bien, la muestra según Hernández et al. (2010), es un subconjunto representativo de una población más amplia, seleccionado con el propósito de realizar observaciones, y análisis para inferir conclusiones sobre la población en su conjunto. Para la determinación de la muestra, se empleó el muestreo no probabilístico por conveniencia, ya que según Hernández y Mendoza (2018), es una técnica de selección de muestra donde los elementos son elegidos de manera conveniente y accesible para el investigador, en lugar de seguir un método aleatorio. Se basa en la disponibilidad y conveniencia de los sujetos. De ahí que la muestra estará compuesta por 18 revistas relacionadas con el fenómeno de estudio y 6 jurisprudencias, con abordaje de casuísticas por delitos informáticos.

2.6. Técnicas e instrumentos de recolección

2.6.1. Técnicas

El estudio empleó el análisis documental, que consiste en la búsqueda de manera minuciosa los documentos relevantes, de diversas fuentes, ya sean primarias o secundarias Hernández et al. (2014). Se ha empleado para este estudio el análisis documental que contenga de manera estructurada la información relevante, donde se ha observado y analizado múltiples documentos con el propósito de obtener un mayor conocimiento acerca de la cadena de custodia y el fraude informático a través de dicha técnica.

Otra técnica que se empleó fue la observación, ya que según la metodóloga Baena (2017), es una técnica de recopilación de datos en investigación que implica la atención directa y sistemática a eventos, comportamientos o fenómenos en un entorno específico. A

través de la observación, el investigador buscó registrar de manera imparcial y objetiva las características relevantes del contexto estudiado, permitiendo una comprensión directa de los elementos. Mismo que se empleó para el análisis de jurisprudencia.

2.6.2. Instrumentos

El instrumento del análisis documental fueron las fichas bibliográficas, que consiste en recopilar información relevante de fuentes bibliográficas, como libros, artículos, informes y documentos técnicos relacionados con el tema de investigación Hernández et al. (2010).

Estas fichas contienen datos como el autor, título, año de publicación, resumen y citas relevantes, permitiendo tener un registro ordenado y accesible de la literatura consultada, para examinar la información contenida en la bibliografía y fuentes jurídicas utilizadas para la investigación, con ayuda de un resumen que proporcione indicios idóneos de los problemas planteados, los cuales se detallan en el análisis realizado de acuerdo con los objetivos a obtener Dulzaides y Molina (2004)

Así mismo el instrumento de la observación, fueron las fichas de análisis jurisprudencial, con la finalidad identificar aquellos delitos informáticos, contenido en la resolución, emitidas por las entidades correspondientes, y analizadas en partes explicativas, considerativas y resolutivas.

Es así que, para la recolección de datos, se seleccionaron artículos científicos de contexto nacional e internacional, además de trabajos de investigación realizados entre los años de 2017 a 2022 en el idioma español, donde su publicación haya sido en repositorios universitarios, revistas indexadas o tesis, así como análisis de jurisprudencia, de modo que permitió recabar información esencial y sustancial sobre el fenómeno de estudio.

2.6.3. Análisis de datos

Para analizar la información recopilada, se utilizó la técnica de triangulación, derivada de la tríada hegeliana que representa la dinámica dialéctica de tesis, antítesis y

La tesis se encargó de exponer los antecedentes y el marco teórico que respaldan la investigación, presentando las perspectivas anteriores sobre el tema.

La antítesis surgió examinar los hallazgos obtenidos después de la recolección y análisis de los datos, revelando contradicciones, tensiones o desafíos identificados en la realidad del fenómeno estudiado. Posteriormente, se realizará la síntesis, integrando las conclusiones y adoptando una posición final que consolide los resultados de la investigación.

La síntesis no sólo comprendió los hallazgos, sino que también buscó superar las contradicciones identificadas, ofreciendo una visión más completa y comprensiva del fenómeno. Esta técnica dialéctica posibilitó una comprensión más profunda y contextualizada del tema de investigación, facilitando la construcción de conocimiento y contribuyendo a la reflexión crítica sobre el objeto de estudio.

2.4. Aspectos éticos

La presente investigación resguardó los derechos de cada autor, citándolos de manera adecuada y en la edición actual que es APA 7ma edición, en observancia a la autoría literaria.

En observancia a lo desarrollado por Concytec (2019) quien hace referencia al código Nacional de Integridad Científica, donde se afirma que se debe tener buenas prácticas al realizar tu investigación, por lo tanto, adoptar estricta y activamente principios éticos, al mismo tiempo afirma que la integridad científica debe aplicarse en las etapas de formulación, implementación y propuesta de la investigación. A través de este, el trabajo tiene buenas prácticas en general, dado que siguió principios como la solidaridad, beneficencia, autenticidad, y se respetó a los derechos de autor.

CAPÍTULO III. RESULTADOS

En este capítulo, se presentó los hallazgos de nuestra investigación A través de un análisis documental meticuloso, hemos explorado las diversas facetas y desafíos que enfrenta la cadena de custodia en el contexto del fraude informático bajo la legislación peruana actual.

La metodología adoptada para esta investigación implicó la recopilación y el análisis de documentos legislativos, casos judiciales relevantes, y literatura académica. Hemos organizado nuestros hallazgos en varias secciones, cada una de las cuales se centra en un aspecto específico de la cadena de custodia en el marco del fraude informático. Esto incluye su definición legal, procedimientos establecidos, desafíos prácticos, y comparaciones con normativas internacionales.

Para facilitar la comprensión y el análisis, los datos recopilados se han presentado en forma de tablas detalladas. Estas tablas no solo resumen la información relevante, sino que también permiten una comparación rápida y eficiente de los distintos elementos de la cadena de custodia. Además, proporcionan un marco claro para entender cómo la legislación peruana actual aborda los desafíos únicos presentados por el fraude informático.

Este capítulo también incluyó una discusión en profundidad sobre los hallazgos, resaltando tanto las fortalezas como las áreas de mejora en la legislación actual. El análisis documental ha permitido identificar brechas legislativas, inconsistencias y áreas que requirieran mayor claridad o refuerzo.

Finalmente, este capítulo no solo reflejó el estado actual de la legislación peruana en lo que respecta al fraude informático y la cadena de custodia, sino que también ofrece una base sólida para futuras investigaciones y posibles recomendaciones legislativas. Con este análisis, aspiramos a contribuir significativamente al entendimiento y al fortalecimiento del marco legal en Perú para combatir el fraude informático de manera efectiva.

ANALISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Artículos de Revista	Jose Miguel Gonzales Reyes	La prueba pericial digital y la cadena de custodia	Revista Anales de la facultad de derecho, 38; 2021, pp. 43-79	Se determina que cuando no se ha aplicado un debido procedimiento de cadena de custodia, da lugar a la pérdida de eficacia de las evidencias electrónicas encontradas, por tanto no será incorporada al proceso para su valoración por el juez, teniendo en cuenta que las pruebas permiten un mayor sustento a la hora de la función decisoria del juez.

Tabla 2: Análisis de la revista Discusiones
ANALISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Artículos de Revista	Antonio Vieira, Saulo Murilo de Oliveira Matto	La cadena de custodia de la prueba en el proceso penal	Revista Discusiones Pags.206-209	Las pruebas conseguidas con violación de la cadena de custodia esta establece como prueba ilícita, generando que sea inadmisibles dentro del proceso penal, siendo que esta no cumple con los parámetros mínimos de integridad y fiabilidad, atentando de la misma manera sobre la producción probatoria y los principios del estado de inocencia, contradictorio y de defensa.

ANALISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Artículo de revista	Elena Villa Boix	La cadena de custodia en el proceso penal	Ficp Pags. 3- 6	Es de suma importancia comprender que la alteración de las pruebas o no seguir adecuadamente los actos de conservación, incurrirá que se pongan en duda su validez, del modo que no serán valorados por el juez y por ello de lugar a alterar el principio de inocencia que tiene el acusado dentro del juicio, posibilitando así que se dicte una sentencia condenatoria, pese a que se hubieran tenido pruebas que demostraban la inocencia del acusado.

Tabla 4: Análisis de la revista Iusta
ANALISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Artículo de Revista	Rodrigo Alberto Plazas Estepas Ludivia Hernández Aros Mario Heimer Flórez Guzmán	El debido proceso y la cadena de custodia frente a las pruebas judiciales presentadas por el auditor forense	Revista Iusta pp. 43-62	Se destaca que la cadena de custodia tiene factores como la recolección, identidad, embalajes y envío, cuando una o varias de esta se incumple al momento de las pericias, no se estará garantizando la autenticidad, entendiendo que dichas evidencias posteriormente serán analizadas para ser presentadas al juez el cual no podrá contrastar el delito con los hechos acontecido, por tanto, no se podrá examinar e incluir como parte del proceso.

Tabla 5: Análisis de la Revista Teorder
ANALISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Artículo de Revista	Pablo Hernández Romo Valencia	La cadena de custodia	Revista Teorder Pags.231-240	Se afirma que en la pérdida de una pieza o una alteración en la cadena de custodia resulta perjudicial en cuanto esta sirve como prueba dentro del proceso penal por lo que implica una afectación a su admisibilidad, reduciendo así el peso probatorio que tiene como objeto la absolución o condena de una de las partes.

Tabla 6: Análisis del Repositorio Dspace
ANALISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Ensayo	Paola del Carmen Rivera Vargas	La cadena de custodia en los delitos flagrantes	Repositorio Dspace	Se resalta la dificultad en acceder a una eficaz cadena de custodia cuando en el lugar de los hechos es un área alejada de la ciudad, debido a que en la mayoría de casos no existe un personal especializado en el cuidado y preservación que se deba tener en cuenta, perdiéndose así la legitimidad en las pruebas y de la misma forma no se estará garantizando justicia de las partes del proceso.

Tabla 7: Análisis de la Revista Ecos Sociales
ANALISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Artículos de Revista	Víctor Hugo Silvan Rodríguez Lenin Méndez Paz	cadena de custodia, su repercusión e importancia en el sistema de justicia penal oral acusatorio	Revista Ecos sociales Págs. 1313 - 1314	Se afirma que la cadena de custodia forma parte fundamental en el sistema de justicia y más aún en la eficiencia del sistema oral, por ello su inobservancia o descuido en su aplicación, repercutirá en las pruebas, que ayudaran a la reducción de impunidad a los delincuentes.

Tabla 8: Análisis de la Revista Semilla Científica
ANALISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Artículos de Revista	González, Diego García, Roberto Barrera, Anthuan Benítez, Luis	Reflexiones sobre manejo adecuado de cadena de custodia en el nuevo proceso penal	Revista semilla científica Págs. 453 - 454	Se establece que el manejo inadecuado de cadena de custodia, implicara una contaminación de las evidencias, que dará lugar a la inautenticidad, logrando que se interprete de una manera incorrecta los hechos suscitados, por tal motivo serán impugnables las pruebas que sean presentadas sin el cuidado debido, debilitando la posición de una de las partes y la credibilidad del mismo.

Tabla 9: Análisis de Tesis de la Universidad Siglo XXI

ANALISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Tesis	Ivan Mauro Lucardi	Cadena de custodia	Tesis (Universidad Siglo 21) Pags. 6- 13	Se aborda a la cadena de custodia como pilar importante en el proceso penal, que el descuido o alteración en el recojo de la escena del crimen o en la exposición en juicio dará lugar a que pierda peso la carga probatoria, debido a que esta comprende información esencial para la investigación, por tal hecho resulta en que la prueba obtenida tiene capacidad de sentenciar o no al acusado.

Tabla 10: Análisis del Diario la Ley N° 8859

ANALISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Diario Digital	Javier Rubio Alamillo	Conservación de la cadena de custodia de una evidencia Informática	Diario La ley N.º 8859 Págs. 3-5	Se sostiene que las evidencias informáticas recogidas equívocamente traerán como consecuencia el resultado final del juicio, debido a que genera desconfianza en el juez, por perder credibilidad de las pruebas presentadas, además se establece que se sancionara a las partes que no apliquen correctamente la cadena de custodia, esto puede ir desde una multa hasta la pérdida de algunos derechos en el juicio.

Tabla 11: Análisis de Tesis de la Universidad de León
ANALISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Tesis	Natalia Natal Marcos	La cadena de custodia: algunos problemas específicos de exclusión probatoria	Universidad de León	Es importante destacar que el no seguir los proceso de recojo y custodia en las evidencias, afectara el derecho a la defensa y el de presunción de inocencia, debido que las pruebas expuestas en el juicio deben ser integras, sin objeto de manipulación, para no afectar la defensa del acusado y que este pueda realizar una efectiva contradicción.

Tabla 12: Análisis de la Revista Chilena de Derecho y Tecnología
ANALISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Artículos de Revista	Laura Mayer Lux y Guillermo Oliver Calderón	El delito de fraude informático: concepto y delimitación	Revista chilena de derecho y tecnología págs. 151-184	El artículo manifiesta el peligro que implica el recojo de evidencias en este tipo de delito, debido a la complejidad que se tiene a la hora de utilizar la cadena de custodia, puesto que no se encuentra frente a evidencia física, si no a evidencia digital, como archivos, correos, base de datos, entre otros. Por tal motivo es simple para el delincuente o un tercero la manipulación y alteración de estas evidencias a fin de librarse de una condena.

Tabla 13: Análisis de Tesis de la Universidad Cesar Vallejo

ANALISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Tesis	Mariel Melissa Mengoia Valdivia	Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú	Repositorio Universidad Cesar Valljeo Pags. 20- 24	Es importante aclarar que el fraude informático afecta tanto al ciudadano de a pie como a empresas en general, por tal hecho no bastara con la aplicación de una cadena de custodia tradicional para asegurar las evidencias en la escena del crimen, debido a la volatilidad de este tipo de evidencias digitales la posibilidad de alteración sin que el perito se de cuenta es muy alta, por tal hecho el peligro de presentar una prueba modificada afecta gravemente el curso del juicio y el resultado final.

Tabla 14: Análisis de Tesis de la Universidad de Cuenca
ANALISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Tesis	Chungata Cabrera, Ana Maribel	El fraude como delito informático	Tesis Universidad de Cuenca Pags. 7 – 10	Se determina que existe características en las personas que cometen fraude informático que va desde los conocimientos técnicos en la informática, hasta la capacidad de eliminar todo rastro posible, a fin de engañar a los operadores de justicia, por tanto un error en el uso de cadena de custodia de las evidencias digitales da lugar a su alteración, que posteriormente será impugnada por parte de la defensa y finalmente perderá peso probatorio en la conexión de la evidencia digital con los acusados.

Tabla 15: Análisis de la Revista de Información Tecnológica y sociedad

ANALISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Artículos de Revista	Carla Maria Mamani Castillo	Phishing: Fraude informático y como evitarlo	Revista de Información tecnológica y sociedad	Es importante afirmar que los criminales a través de sus conocimientos en materia tecnología imposibilitan su rastreo y la información que hayan sustraído a su víctima, , por tanto al encontrar evidencia digital que se utilizara a la hora de juzgar al delincuente, es imprescindible la preservación de este material por las consecuencias legales que esta trae consigo como lo es la absolución del acusado por contener defectos en la evidencia presentada.

Tabla 16: Análisis de la Revista Informática Forense

ANALISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Artículo de Revista	Jhovana Doris Suxo Hinojosa	Pharming, nuevo fraude informático	Revista Informática forense	Se afirma se debe tener una identificación pronta del fraude informático y sus nueva modalidades frente a la escena del crimen, a fin de que el recojo de evidencias sea por forenses especializado en la materia y no otros, ello debido a la complejidad y fragilidad con la que se puede modificar o destruirse, ello conllevaría a una inadmisibilidad de evidencia por el tribunal a cargo.

Tabla 17: Análisis de la Revista Chilena de Tecnología y Derecho
ANÁLISIS DOCUMENTAL

TIPO DE DOCUMENTO	AUTOR	TÍTULO	PAGINA	CONTENIDO
Artículo de Revista	Fernando Muñoz León	Epistemología de la techne: a propósito del fraude informático	Revista Chilena de Tecnología y derecho Pags 247-260	Se amplía el tema de fraude informático señalando que este no debe ser interpretado como un fraude convencional, el legislador a fin de eliminar la presión por adaptar la reglamentación legal a las circunstancias rápidamente cambiantes, este incorporara de manera ineficaz, por tanto existe el riesgo de incluir prueba o evidencias que no cumplen los parámetros mínimos en cuanto a cadena de custodia, por lo que afectaría gravemente la defensa del acusado y posteriormente podrá llevar una sentencia en su contra.

Tabla 18: Análisis del Expediente RN N°001607-2021

CORTE SUPERIOR DE JUSTICIA	
QUINTO JUZGADO PENAL	
DATOS DEL EXPEDIENTE	<p>Recurso de Nulidad 001607- 2021 JUEZ: JORGE LUIS CHAVEZ TAMARIZ IMPUTADO: KARIN JANET MARENGO NUÑEZ DELITO: LAVADO DE ACTIVOS AGRAVIADO: EL ESTADO PERUANO</p>
PARTE EXPOSITIVA	<p>PARTE PROCESAL</p> <p>Se solicita que se declare una nulidad de el "CD" sin marca entregado por el testigo protegido el 13 de enero de 2020, escrito con rotulador negro, así como el des lacrado y el acta de visualización y transcripción de CD”, del mismo modo que se excluyen todos los “audios de Alfredo Benavides Gastelo y acta de visualización y transcripción de CD de fecha 16 de diciembre del año 2021”, y (iii) Proscriba la reincorporación "Audio 2" entregado por el testigo Protegido N° 01-13-2020; por razón que la defensa técnica menciona que los actos lesivos están en relación con el incumplimiento del procedimiento a una debida cadena de custodia.</p> <p>REPRESENTANTE DEL MINISTERIO PUBLICO</p> <p>La solicitud de la fiscal adjunta provincial, es que se declare infundado, la tutela de derechos, en relación a la incorporación del "CD"</p> <p>Menciona que fue en la declaración de un testigo protegido N°01-13-2020 y sigue las pautas de un colaborador eficaz. Se menciona la existencia de la cadena de custodia del elemento probatorio</p>

	<p>"CD". Por tal hecho</p>
<p>PARTE CONSIDERATIVA</p>	<p>Á) Por cuanto al derecho de legitimidad probatoria se regula en el artículo VIII del Título Preliminar del Nuevo Código Procesal Penal, que establece que las pruebas obtenidas de manera contraria a los derechos fundamentales carecen de efecto legal. Así como su interpretación del Tribunal Constitucional peruano en el expediente (N.º 1014-2007-PHC/TC), que sostiene que la actividad probatoria debe ser conforme a los derechos fundamentales y no infringir el orden jurídico en la obtención, recepción y valoración de la prueba.</p> <p>B) Por cuanto a la omisión del procedimiento de cadena de custodia, el juzgado menciona que en principio resulta imprescindible tener presente la diferencia entre fuente de prueba y medio de prueba por lo hace referencia a la interpretación del TC en el expediente N° 05822-2007-PHC/TC LIMA, que establece que la declaración de nulidad de un proceso solo afecta la validez de los medios de prueba relacionados con el proceso, no así de las fuentes de prueba, que son realidades externas al proceso de prueba inherentes al mismo, mas no así de las fuentes prueba.</p> <p>C) El juzgado menciona que el art. 14° del Acuerdo Plenario 6-2012-CJ-116 la ruptura de la cadena de custodia o de su omisión no sigue necesaria o automáticamente que el cuerpo del delito es inauténtico y, por consiguiente, que carece de eficacia probatoria. Recordando, de esta forma, que la cadena de custodia es una de las</p>

	<p>modalidades para acreditar la mismidad de un bien, objeto o cosa incautado, y que solo busca facilitar la demostración de su autenticidad, Siendo así, y de conformidad a lo anterior se desprende que, no hay evidencia que contradiga la autenticidad del "CD" sin marca, identificado como "Audio 2", proporcionado por el Testigo Protegido N° 01-13-2020. Esto no justifica la exclusión probatoria, ya que se puede subsanar con otra actividad probatoria. La solicitud de prohibir la reincorporación del "Audio 2" carece de base para pronunciarse sobre el asunto.</p>
<p>PARTE RESOLUTIVA</p>	<p>El convencimiento que ha expresado el juez en su decisión es la de “FUNDAR EN PARTE el pedido de tutela de derechos de la imputada Karin Janet Marengo Nuñez” en el proceso que se le sigue en contra de la misma. Por tanto se excluye “acta de visualización y transcripción de CD de fecha 16 de diciembre de 2021”</p>
<p>ANÁLISIS</p>	<p>La resolución aborda la solicitud de tutela de derechos de la imputada, por ello se pide la nulidad en la incorporación del CD y el audio que este contiene por no haber seguido los parámetros correctos para resguardar la cadena de custodia para posterior ser utilizada como prueba por el juez, asimismo es de conocimiento que la falta de un eslabón o la omisión de cadena de custodia permite que las evidencias no cumplan con la garantía de</p>

	<p>autenticidad y estas perjudica la validez del medio de prueba , por este hecho se puede desacreditar los puntos que tiene la parte que acusa.</p>
--	--

Tabla 19: Análisis del Expediente N° 1607-2021

<p>CORTE SUPREMA DE JUSTICIA DE LA REPÚBLICA</p>	
<p>SALA PENAL TRANSITORIA – RECURSO DE NULIDAD N° 1607-2021</p>	
<p>DATOS DEL EXPEDIENTE</p>	<p>CUADERNO DE DEBATE N° JUZGADO: IMPUTADO: Karina Rosales Ruis y otros DELITO: Fraude informático AGRAVIADO: Jose Enrique Emilio Solano Alejo. JUEZ: Prado Saldarriaga</p>
<p>IMPUTACIÓN FACTICA</p>	<p>ABOGADO DE LA PROCURADORIA</p> <p>Según la acusación fiscal, los días 18 y 19 de diciembre de 2013, los acusados Karina Rosales Ruiz, Fredy Adolfo de la Cruz Coronado y Bryan Ábner. Díaz Ravello, utilizando diversas artimañas obtuvieron el número 4222240001472691 que corresponde a una cuenta del banco Interbank cuyo titular es José Enrique Emilio Solano Alejo (para ello se valieron también de la línea de teléfono de este agravio y a través de la misma realizaron diversas transacciones). Fue así que lograron transferir 2942,50 soles a la cuenta N.º 0483060023428, el cual le pertenece a la acusada KARINA ROSALES RUIZ e hicieron lo mismo destinando el dinero a la cuenta N.º 0933060408829 cuyo titular era el acusado FREDY ADOLFO DE LA CRUZ CORONADO. Por su parte, el acusado José Enrique Emilio Solano Alejo empleó un documento privado falso el 18 de diciembre de 2013 al concurrir a la empresa telefónica en posesión de una carta poder para solicitar la reposición del número de teléfono 998-839-810 y que también le pertenecía a José</p>

	<p>Enrique Emilio Solano Alejo logrando que activaran la línea de teléfono.</p>
<p>FUNDAMENTO DEL RECURSO DE NULIDAD</p>	<p>La PROCURADURÍA PÚBLICA ESPECIALIZADA EN DELITOS DE ORDEN PÚBLICO DEL MINISTERIO DEL INTERIOR interpuso su recurso de nulidad solicitando que se realice un nuevo juicio oral. Al respecto, señaló lo siguiente</p> <ol style="list-style-type: none"> 1. La sentencia impugnada no expone los motivos por los cuales estiman que no se cumplen los elementos del tipo penal de asociación ilícita. Lo único que indican es que no existen indicios o pruebas de la comisión del delito. 2. Lo que no se tomó en cuenta es que para la comisión del delito de asociación ilícita los acusados acordaron con tiempo el reparto de los roles que ejecutaron. 3. La relativa organización se acredita con el hecho de que la acusada Karina Rosales Ruiz y el acusado Fredy Adolfo de la Cruz Coronado fueron quienes se encargaron de aperturar una cuenta bancaria en la cual se le depositó el dinero. 4. Por su parte, el contumaz Bryan Ábner Díaz Ravello se encargó de elaborar una carta poder con contenido falso para poder reponer el teléfono del agraviado José Enrique Emilio Solano Alejo y logro habilitarlo. Así, a través de la banca por internet, lograron transacciones a las cuentas de Karina Rosales Ruiz y Fredy Adolfo de la Cruz Coronado. 5. El banco Interbank remitió los reportes de las cuentas números

0483060023428 y 093060408829 que corresponden a los acusados Karina Rosales Ruiz y Fredy Adolfo de la Cruz Coronado a donde se transfirió el dinero del agraviado José Enrique Emilio Solano Alejo y que fue obtenido porque el acusado contumaz Bryan Ábner Díaz Ravello logró activar el número del teléfono de la mencionada víctima. Esta descripción permite acreditar la concurrencia de más de dos personas.

6. Se configura la vocación de permanencia porque para desarrollar los actos detallados los acusados necesitaron de tiempo para su planificación, a fin de obtener la información bancaria del agraviado José Enrique Emilio Solano Alejo. Además, se debe tener en cuenta que la propia acusada Karina

Rosales Ruiz declaró en juicio oral que no llegó a cancelar la cuenta bancaria que había aperturado con fines ilícitos. No solo eso, también declaró que llegó a abrir hasta cuatro tarjetas en distintos bancos.

7. También se afectó el derecho fundamental a la prueba, porque en la audiencia del 9 de noviembre de 2020 solicitaron que se actúe en el juicio oral la declaración del agraviado, la de los representantes del banco Interbank y Telefónica del Perú. En el caso de este último para que remitan la documentación que presentaron los imputados para lograr activar el número del agraviado. Sin embargo, en las audiencias de 16 y 25 de noviembre, así como las del 4, 14, 21, 28 y 30 de diciembre de

2020 nunca se dio cuenta del diligenciamiento de las notificaciones para la concurrencia de las mencionadas personas ni de los oficios pertinentes.

OPINIÓN DE LA FISCALÍA SUPREMA EN LO PENAL

1. No basta con la agrupación de más de dos personas, sino que se requiere que se pruebe el dolo de los acusados para conformar una agrupación con vocación de permanencia.

2. En el caso de la imputada Karina Rosales Ruiz, esta manifestó que no conocía a sus coacusados y desconocía la finalidad de la apertura de varias cuentas bancarias. Si bien señaló que abrió más cuentas en otros bancos, esto no se ha probado.

3. Si bien se realizaron dos transferencias desde la cuenta del agraviado, esto por sí solo no configura el delito de asociación ilícita, sino el de fraude informático.

4. No se ha probado que los acusados Fredy Adolfo de la Cruz Coronado y Bryan Ábner Díaz Ravello hayan abierto cuentas en otros bancos para recibir dinero fraudulento.

5. No se afectó el derecho a la prueba de la parte civil. En el caso del agraviado, este ha fallecido. En cuanto a la declaración de los representantes de Telefónica y el banco Interbank su presencia en el juicio no demostraría la responsabilidad en el delito de asociación ilícita.

ANÁLISIS DEL RECURSO

La sentencia de primera instancia decidió absolver a los acusados

Karina Rosales Ruiz, Fredy Adolfo de la Cruz Coronado y Bryan Ábner Díaz Ravello porque consideran que no se cumplen los elementos objetivos del tipo penal. Señalan que solo se demostró que existió un concierto de voluntades

para realizar actos de falsificación material y fraude informático.

Sexto. La Fiscalía Suprema en lo Penal es de la opinión de que, en efecto, no es posible sostener la acusación por delito de asociación ilícita porque no se han identificado los elementos típicos de este delito como son la relativa organización y la permanencia en el tiempo. Además, señalan que la pluralidad de agentes por sí sola no es suficiente para sostener dicha imputación.

Séptimo. Al respecto, este Supremo Tribunal considera que no se ha contextualizado un hecho de relevancia y que podría incidir notablemente en el esclarecimiento del ilícito imputado. Se trata del certificado judicial de antecedentes penales de Brayan Ábner Díaz Ravello quien de los dos antecedentes que registra uno es por el delito de fraude Informático que data de 2017. Esto evidencia que se trata de una persona que estaría inmersa en la comisión de delitos como el que motivó la presente causa y a efectos de descartar la existencia de su pertenencia a una estructura criminal se deberán de actualizar sus antecedentes, no solo penales (recabándose además las sentencias en las que se justifican) sino también policiales y judiciales.

Octavo. Por su parte, en cuanto a la absolución de los acusados Fredy Adolfo de la Cruz Coronado y Karina Rosales Ruiz, este Supremo Tribunal considera que es necesario indagar si se trata de personas que además de verse

involucradas en el presente caso también han operado en forma similar y aperturando otras cuentas en más entidades bancarias. Es importante enfatizar en el hecho de que Karina Rosales Ruiz manifestó que no solo se limitó a abrir la cuenta en el banco Interbank, sino que también lo hizo en otras entidades financieras.

Noveno. Por tanto, resulta pertinente la obtención de la información antes señalada y otras que pidan actuar las partes procesales en tanto sean útiles y pertinentes.

DECISIÓN

I. NULA la sentencia del 30 de diciembre de 2020 emitida por la Sexta Sala Penal para Procesos con Reos Libres de la Corte Superior de Justicia de Lima. En el extremo que resolvió absolver a KARINA ROSALES RUIZ, FREDY ADOLFO DE LA CRUZ CORONADO y BRYAN ÁBNER DÍAZ RAVELLO de la acusación fiscal en su contra por el delito de asociación ilícita para delinquir en agravio del Estado. II. ORDENARON que se remitan los autos a otro colegiado superior para que realice un nuevo juzgamiento que observe lo desarrollado en la presente resolución.

ANÁLISIS

El recurso de nulidad es claro al afirmar que en la actualidad no debe confundirse otros delitos con el de fraude informático, ello pese a existir elementos similares, por tanto tampoco debe confundirse los medios que se utilizan para la recolección de evidencias, en el sentido que se perderá peso probatorio cuando se utilice un procedimiento distinto o incorrecto que dará lugar a la absolución de los acusados debido a no ser idóneo los medios probatorios presentados tal y como ha ocurrido en este caso.

CAPÍTULO IV. DISCUSIÓN Y CONCLUSIONES

4.1. Discusión de resultados

En principio, en cuanto al objetivo general, en el cual nos planteamos, que es, determinar cómo influye el incorrecto uso del procedimiento de la cadena de custodia en casos de fraude informático, y cuáles son las implicaciones prácticas y teóricas de estos procedimientos en el procesamiento de pruebas en el sistema judicial en Perú durante el año 2022. Tenemos que señalar en primera instancia, los antecedentes que se usaron en la presente investigación. Los múltiples instrumentos que fueron objeto de análisis, nos muestran que se hace de uso obligatorio que exista una correcta aplicación en la cadena de custodia al momento de utilizarla en los juicios penales, por ello **Gonzales (2021)** nos informa que a fin de evitar que se altere la información o esta pueda ser manipulada se aplica la bien llamada “función hash” que son los algoritmos creados a partir de una entrada, dicha entrada que puede ser un archivo, una contraseña, algún tipo de texto o documento, esta función permite conseguir una salida alfanumérica estable, fija y constante que consignara el manejo de toda la información que se le ha otorgado; sin embargo, así mismo Ajhuacho (2011), reconoce que el incumplimiento de la cadena de custodia genera la excusión de la prueba porque se vulnera el principio de legalidad de la prueba, denotando la necesidad de implementar un manual que proteja los elementos de la prueba en el momento de la recolección, debido a la relevancia que tendrá la situación jurídica de los sujetos que forman parte del proceso. Encontramos a **Plazas et al (2016)** señala que la debida aplicación de esta cadena de custodia involucra factores como la de recolección, identidad, embalaje y además envió, del cual podemos señalar que este segundo autor se está cñiendo al uso de los procedimientos de cadena de custodia mediante un manual, de ello podemos inferir que en los casos de fraude informático se debe aplicar métodos informáticos especializados en la preservación de la evidencias desde dentro del sistema u ordenador que no

permita la alteración o manipulación del mismo, sin dejar de lado los procesos tradicionales de cadena de custodia que aseguran que el objeto llegue de un punto “x” a un punto “y” sin sufrir deterioros o un tratamiento indebido.

Diversos autores coinciden al señalar que la prueba que se obtuvo sin la aplicación de la cadena de custodia, no puede ser íntegra y fiable, por tanto generaría una exclusión probatoria en tanto que afecta el conocido principio de legalidad de la prueba, a pesar de ello **Hernández (2017)** y el expediente **00041-2019-18-5001-JR-PE-03** establece que la fractura de la conocida cadena de custodia no quiere decir que la evidencia física del hecho delictivo no sea verdadero, en razón que dicha cadena de custodia protege la identidad del objeto, mas no la calidad del mismo, en ese mismo sentido uno de los autores apoya esta versión aclarando que en el caso de existir una pérdida de un elemento o pieza de la cadena de custodia, este no será grave, porque se lograra probar con la prueba y no solo por la admisión. Por ende, los antecedentes tratados en la presente investigación son cruciales para el entendimiento de que en distintas realidades sociales como jurídicas, la cadena de custodia es significativa y relevante dentro de un proceso de delitos o fraudes informáticos, de tal manera que se debe ser cuidadoso desde el inicio de la investigación como en la recolección de datos o elementos que ayuden al tipo penal.

Por otro lado, el presente trabajo de investigación presento una secuencia de limitaciones con respecto a la obtención de resultados, dado que el tema es novedoso en el ámbito jurídico, asimismo el corto tiempo para la obtención de suficiente información, debido que existe escasa jurisprudencia y artículos de revista que contengan datos sobre la investigación. Debido a ello no se contó con amplia variedad de expertos en la materia, que pudiesen expresar su ideas y posturas acerca de la investigación realizada. Sin embargo, se logró crear un concreto conocimiento gracias a los resultados y conclusiones de los autores. En cuanto a las implicancias obtenidas por medio de los resultados de los análisis documentales realizados en esta investigación. Por ello al momento de revisar de manera minuciosa cada

uno de estos, ha posibilitado incrementar el conocimiento jurídico acerca del novedoso tema, del mismo lado permite que la población pueda conocer acerca de la aplicación de la cadena de custodia en cuanto al delito de fraude informático. Asimismo, a manera de prevención cumple un rol fundamental, dado que el conocimiento sobre la materia evita que la población sea víctima, por ello se brinda diversos mecanismos que será de gran utilidad.

En cuanto al primer objetivo específico que no planteamos, que es, determinar cuáles son las consecuencias del incorrecto uso del procedimiento de la cadena de custodia en Perú durante el año 2022, vamos a la relevancia que la cadena de custodia tiene diferentes autores como **Gonzales (2021)** y **Paternina (2018)** concuerdan que la cadena de custodia es eminentemente clave a la hora de impartir justicia, dado que con ella se obtendrá un base sólida para la resolución de los juicios, del mismo lado autores como **Natal (2019)** y **Gonzales (2021)** apoya que dicha cadena de custodia resulta indispensable para la parte de la defensa dentro del juicio, en el sentido que esta repercutirá sobre los análisis periciales, por tanto lograra en el juzgador el ansiado convencimiento. Por otro lado **Lucardi (2019)** expresa que el fracaso de las investigaciones son principalmente por no dotar de mayores herramientas legislativas, que por su vez tienen la capacidad o no de sentenciar a un individuo, ahora bien este argumento se contrasta con **Gamboa (2021)** que afirma dicha postura estableciendo que, muchos de los abogados que litigan se encuentran descaminados en cuanto a los parámetros legales de la ya mencionada cadena de custodia, podemos inferir que es sorprendente que el tema de cadena de custodia sea nuevo en el mundo jurídico, al punto de no estar realmente empapados acerca de la materia y que este eslabón pueda resultar perjudicial a la hora de encontrarnos en un juicio y que se pueda perder el caso o sentenciar a un inocente por la ignorancia del mismo.

Así mismo, es preponderante mostrar que, dentro de la investigación, y dentro de este objetivo específico, tanto en el análisis documental como jurisprudencial, se ha logrado determinar los impactos que tiene del incorrecto uso o procedimiento con la cadena de custodia,

de tal forma que se ratifique estos impactos o consecuencias. Es así que, recurriendo a los mismos, dentro del análisis de la revista chilena de derecho y tecnología, en la tabla 13, se nos refiere que el recojo de evidencias en este tipo de delito, debido a la complejidad que se tiene a la hora de la utilizar la cadena de custodia, puesto que no se encuentra frente a evidencia física, si no a evidencia digital, como archivos, correos, base de datos, entre otros. Por tal motivo es simple para el delincuente o un tercero la manipulación y alteración de estas evidencias a fin de librarse de una condena. Así mismo, dentro de análisis de la revista de información tecnológica, en la tabla 16, nos señala que los criminales a través de sus conocimientos en materia tecnología imposibilitan su rastreo y la información que hayan sustraído a su víctima, , por tanto al encontrar evidencia digital que se utilizara a la hora de juzgar al delincuente, es imprescindible la preservación de este material por las consecuencias legales que esta trae consigo como lo es la absolución del acusado por contener defectos en la evidencia presentada.

Por otra parte, en cuanto la guía de análisis jurisprudencial, podemos ver el expediente, de Recurso de Nulidad N 206-2019, donde se nos señala que el “phishing” es un tipo de estafa altamente utilizado en la actualidad, donde se configura cuando el delincuente suplanta la identidad de empresas bancarias, utilizando el formato, logos, entre otros. Con la finalidad de conseguir datos privados de la víctima y estos puedan ser utilizados para la obtención de aprovechamiento económico. Ahora bien, La ley 30096, ley de delitos informáticos, es clara en su artículo 8 sobre Fraude informático donde esta no señala ninguna cualidad, experiencia o extenuantes conocimientos sobre informática para la comisión de este delito. El phishing es una técnica delictual que se ha con mayor incidencia en el ámbito nacional e internacional, que se desarrolla con la creación de páginas web fraudulentas, para generar desmerito económico en la victima. Es así, que dentro de este apartado de análisis documental y jurisprudencial, se logra el primer objetivo de la investigación, de tal forma que se denota, que las consecuencias de un mal procedimiento de uso de la cadena de custodia, no solamente puede llevar a un perjuicio

económico por parte de los agraviados, sino también un perjuicio para el aparato estatal, debido a que al haberse dado las pruebas, o que en sí mismo no hay una demostración significativa del tipo penal hacia el imputado, no se pueda sentenciar o ejecutar el proceso de delito o fraude informático, por ende la cadena de custodia resulta indispensable para la parte de la defensa dentro del juicio, en el sentido que esta repercutirá sobre los análisis periciales, por tanto lograra en el juzgador el ansiado convencimiento, de tal forma que la consecuencia principal es la afectación al juicio, en principio por la no pertinente recolección de materia probatoria, y en segundo lugar la no demostración de la culpabilidad o antijuricidad del tipo penal refiriéndonos al imputado.

En cuanto a segundo objetivo que nos planteamos, que es, determinar cuáles son las consecuencias del procesamiento de pruebas en el delito de fraude informático cuando no cumple un correcto uso de la cadena de custodia en el sistema judicial en Perú durante el año 2022. Tenemos que partir desde el análisis jurisprudencial para ver cómo se materializa en nuestra realidad social y jurídica las consecuencias de un mal procesamiento de pruebas en un delito informático, es así que vemos el expediente N° 01189-2019-PHC/TC, donde se nos muestra el caso referente a Marcos Morales Vargas, versa sobre los delitos de fraude informático y falsificación de firma en documento privado. El beneficiario, condenado inicialmente a diez años, vio su pena reducida a seis años. La controversia central se centró en la aplicación de la Ley 30096, que regula los delitos informáticos y entró en vigor el 23 de octubre de 2013. El debate giró en torno a si los hechos delictivos, cometidos entre 2013 y 2014, estaban sujetos a esta ley. El Tribunal Constitucional finalmente declaró infundada la demanda de habeas corpus. Siendo así, que el caso demuestra la complejidad en la aplicación de nuevas leyes en delitos informáticos, especialmente cuando los hechos ocurren en un periodo de transición legislativa.

Por otro lado, el expediente N° 00493-2022-20-5001-JR-PE-06, nos muestra el caso de

estafa agravada y organización criminal. Los acusados estaban involucrados en una operación compleja que incluía fraude informático y el uso de cuentas bancarias para desviar fondos ilícitamente. Se abordaron cuestiones como el levantamiento del secreto bancario y de las comunicaciones, así como el análisis de dispositivos electrónicos incautados. Siendo así que la decisión del juez se centró en la prolongación de la prisión preventiva por un período adicional de 4 meses, destacando la necesidad de continuar con las investigaciones y análisis periciales. Este caso ilustra la complejidad y el desafío que representan los delitos de organización criminal y estafa agravada, especialmente en el ámbito del fraude informático. Resalta la importancia del análisis forense digital y la cooperación de las entidades financieras en la investigación de delitos económicos complejos.

Por ende, respecto a lo anteriormente mencionado, los hallazgos fundamentales del presente trabajo de investigación, en donde este contenido el análisis documental de revistas científicas, como de tesis, de jurisprudencia y otros dentro del presente, respecto al tema, generaron lo consiguiente.

Que se respondió al segundo objetivo específico de la investigación, en el cual se conceptualizó que la cadena de custodia al ser un recurso y crucial dentro del proceso como del delito de delito o fraude informático, debe ser tratado de la manera mas cuidadosa posible, es decir, que se debe recolectar materia de evidencia informática, con una debida y pertinente recolección por parte del personal forense, para que se no se dañe cualquiera prueba material y así no se genere una falsa acusación a los imputados, o que estos puedan generar su libertad a raíz de un elemento de evidencia dañado que no pueda probar su culpabilidad. Así mismo, mostrando que las consecuencias de un mal uso o procedimiento de la cadena de custodia, genera una mala acusación, como la liberación espontanea de los imputados, dejando en un estado de indefensión de los agraviados, y que estos avancen día con día en nuevas modalidades de estafa, o en mejorar su modus operandi. Por otra parte también, la investigación nos muestra

que el adecuado tratamiento después del nuevo modelo acusatorio del código penal y procesal penal, genera que los policías que en su mayoría no tenían un conocimiento basto en informática forense vayan a trasgredir la evidencia material de este tipo penal o delito, de tal forma que su adecuada aplicación de la cadena de custodia, pueda generar un estado de justicia y defensa para los agraviados, como también reduciendo el trabajo de diligencias para los policías inmerso, como una mejor adecuación de las formas de recolección de prueba o evidencia material.

En síntesis, se denota que del presente tema de investigación se desprende que autores como Leyva (2020) Mayer y Oliver (2020) hacen mención sobre la importancia del fraude informático, principalmente porque afecta o vulnera el patrimonio de la víctima a través de sistemas informáticos, ahora bien Mengoa (2020) no concuerda con esa línea de ideas aclarando que el fraude informático no tiene como único bien protegido el patrimonio, sino además los DDHH como es el derecho a la libertad, que es un derecho ciertamente subjetivo regulado en el artículo segundo del CP que no es más que aquella donde ningún otro sujeto u individuo pueda ejercer autoridad cuando este no se lo autorizado o consentido. Chungata (2015) que para la comisión de este delito es importante poseer una serie de habilidades que un malhechor común no las tiene, del mismo lado esta idea la apoya Suxo (2019) que plante que los hackers que en términos más coloquiales se le conoce como pirata informático es aquel que posee conocimientos profundos acerca de informática, el cual utiliza dichos conocimiento en favor suyo o de un tercero, continuando con la ilación se resalta la importante labor acerca de la vulnerabilidad que sufre el usuario que ingresa a internet, por ello en el recurso de nulidad N° 206-2019 el juez hizo hincapié en mencionar que para la realización de este delito se requiere de una alta complejidad en manejo de las tecnologías, mientras que los autores Mayer y Oliver (2020) no plantea la misma idea, dado que expresa que el fraude informático solo se materializa bajo el fundamento de los tres elementos, que es como primer lugar conducta, en segundo lugar

resultado y por último el ánimo del agente. Estos tres elementos forman parte de los elementos del delito, olvidándose la tipicidad, antijuricidad y culpabilidad del agente, que en la práctica son elementos de suma importancia a la hora de calificar un delito

Es así que, como conclusión se puede afirmar que la vinculación entre la cadena de custodia y el fraude informático radica en la protección, control y custodia de las evidencias encontradas en la escena del crimen, ello en consecuencia que, los dispositivos informáticos contienen datos e información sumamente valiosa para demostrar que el acusado es culpable o no , permitiendo la correcta conducción del juicio, más aún se debe tomar en cuenta que dichas evidencias son altamente modificables y destruibles, por tal hecho no se podrá en ningún caso utilizar métodos no apropiados de cadena de custodia que impliquen consecuencias negativas en el proceso como lo es la inadmisibilidad de evidencia, que podrá lograr una desvinculación del acusado con las evidencias y con la escena del crimen, arriesgando que este pueda quedar impune. Posteriormente, se puede confirmar que los sujetos que cometan el fraude informático no requirieron de alguna característica o experiencia sobre temas informáticos para la realización de este delito, pero si se requiere de operadores de justicia altamente calificados para poder hacer frente al adecuado procedimiento de cadena de custodia en el país, por ello se requiere una ardua capacitación y puesta en práctica, a fin de evitar un juicio deficiente.

REFERENCIAS

- Amaiquena, F; Vera, J; Zumba, I. (2019). Enfoques para la formulación de la hipótesis investigación científica. *Revista Conrado*, 15(70), 354-360. Recuperado a partir de: <https://conrado.ucf.edu.cu/index.php/conrado/article/view/1148>
- Ajhuacho, E. (2021). *La necesidad de implementar un manual para el manejo de la cadena de custodia, que su incumplimiento genere exclusión probatoria debido a la vulneración del principio de legalidad de la prueba*. [Trabajo de Diplomado, Universidad Mayor de San Simón]. Repositorio Institucional. <https://webcache.googleusercontent.com/search?q=cache:45V7fWd-oUIJ:ddigital.umss.edu.bo:8080/jspui/handle/123456789/22216&hl=es-419&gl=pe>
- Araujo, D y Huanca, K. (2018). *El procedimiento de Cadena de Custodia en la investigación preliminar del Ministerio Público de Lima Sur*. [Tesis para la obtención de Título, Universidad Autónoma del Perú]. Repositorio Institucional. <https://repositorio.autonoma.edu.pe/handle/20.500.13067/738>
- Baena, G. (2014). *Metodología de la investigación*. Grupo Editorial Patria.
- Carrillo, C. y Montenegro, A. (2018). *La criminalidad Informática o Tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticas*. [Tesis de obtención de título, Universidad Señor de Sipán]. Repositorio Institucional. <https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/4514/Carrillo%20Diaz%20%26%20Montenegro%20Davila.pdf?sequence=1&isAllowed=y>

- Concytec. (2019). *Fuentes de información; Memorias institucionales; Investigación y desarrollo; Innovación científica; Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica*. Consejo Nacional de Ciencia.
<http://hdl.handle.net/20.500.12390/2197>
- Chungata, A. (2015). *El fraude como delito informático*. [Tesis para la obtención de Título, Universidad de Cuenca]. Repositorio Institucional. <https://www.doccity.com/es/tesis-el-fraude-como-delito-informatico/2610480/>
- Dulzaides y Molina (2004). *Análisis Documental y de Información: Dos componentes de un mismo proceso*. ISSN 1024-9435.
- Divindat (2020). *Fraudes en línea son los delitos informáticos más frecuentes en el 2020*.
Publicado el 8 de agosto de 2020, Lima.
- El país. (2015). *Robados y difundidos los datos privados de una web para infieles*. Diario El País, 10 de julio, 2015.
- El peruano. (2021). *Ciberdelitos en el Perú: se elevan denuncias de fraude informático y suplantación de identidad*. Publicado el 2 de junio del 2021.
<https://elperuano.pe/noticia/121876-ciberdelitos-en-el-peru-se-elevan-denuncias-de-fraude-informatico-y-suplantacion-de-identidad>
- Egocheaga, J. (2016). *Reclamaciones en materia de internet y redes sociales, 279-308*, en *Reclamaciones en materia de consumo*. Madrid, Ed. Dykinson S.L, 280.
- Fuentes, K. (2021). *Modificación de la Ley 30096 para incorporar los delitos del Phishing, Pharming y Carding como delitos penalizables con prisión, para reducir la ciberdelincuencia*. [Tesis para la obtención de Título, Universidad Señor Sipán].
Repositorio Institucional.

<https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/8345/Fuentes%20Garrido%20Karla%20Vanessa.pdf?sequence=1>

Gamboa, M. (2021). *Efectos jurídicos procesales de la afectación de la cadena de custodia en el sistema penal acusatorio en Colombia*. [Tesis de Posgrado, Universidad Libre].

Repositorio Institucional. <https://hdl.handle.net/10901/20664>

González, D. García, R. Barrera, A y Benítez, L. (2021). *Reflexiones sobre manejo adecuado de cadena de custodia en nuevo proceso penal*. [Tesis para la obtención de Título,

Universidad Metropolitana de Educación, Ciencia y Tecnología]. Repositorio Institucional. <https://repositorio.umecit.edu.pa/handle/001/4707>

González, J. (2021). La prueba pericial digital y la cadena de custodia. Universidad de la Laguna. pp. 43-79; ISSN: e-2530-8319. <http://riull.ull.es/xmlui/handle/915/25818>

Gonzales, J. (2019). *La importancia de la cadena de custodia en la investigación criminal en el proceso penal peruano año 2017 – 2018*. [Tesis para la obtención de Título,

Universidad de Chiclayo]. Repositorio Institucional.

http://repositorio.udch.edu.pe/bitstream/UDCH/689/1/T044_09681059_T.pdf

Hernández, P (2019). Cadena de custodia. *Teorder. Universidad Panamericana, México D.F, N°06, Págs. 231-240*. <https://ojs.tirant.com/index.php/teoria-y-derecho/article/view/276/272>

Hernández, R., Fernández, C., y Baptista, M. (2014). *Metodología de la investigación*. McGraw-Hill.

Hernández, R. y Mendoza, C. (2018). *Metodología de la investigación*. McGraw-Hill.

Leyva, C. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. *Lucerna Iuris Et Investigatio*.

<https://doi.org/10.15381/lucerna.v0i1.18373>

Luccardi, M (2019). Cadena de custodia. [Tesis para la obtención de Título, Universidad siglo 21.]. Repositorio Institucional.

<https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/16171/LUCCARDI%20MAURO.pdf?sequence=1&isAllowed=y>

Mamani, C (2019). Phishing: fraude informático y como evitarlo. *Revista de información*

tecnología y sociedad. <http://www.revistasbolivianas.ciencia.bo/pdf/rits/n3/n3a10.pdf>

Mayer, L & Guillermo, O. (2020). El delito de fraude informático: concepto y delimitación. *Revista chilena de derecho y tecnología*, 9(1), 151.

<https://doi.org/10.5354/0719-2584.2020.57149>

Mengoa, M (2021). *Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú*. [Tesis para la obtención de Título, Universidad Cesar Vallejo].

Repositorio Institucional.

https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/62379/Mengoa_VMM-SD.pdf?sequence=1&isAllowed=y

Monge, L. (2022). *Falta de atención dentro del entorno familiar a jóvenes de 18 a 20 años que produce un incremento de asaltos a mano armada a transeúntes*. [Tesis de Pregrado, Universidad San Ignacio de Loyola]. Repositorio institucional.

<https://repositorio.usil.edu.pe/entities/publication/1c7c3b7c-6c9e-4cba-ba39-106793bf2e60>

- Mostajo, B. (2020). *Cadena de custodia de medios probatorios en delito de tráfico ilícito de drogas Distrito Judicial de Lima Norte, 2020*. [Tesis de Posgrado, Universidad César Vallejo]. Repositorio Institucional. <https://hdl.handle.net/20.500.12692/57446>
- Muñoz, F (2016). Epistemología de la techne: a propósito del fraude informático. *Revista chilena de Derecho y Tecnología*,2(2). <http://dx.doi.org/10.5354/0719-2584.2013.30314>
- Natal, N (2020). *La cadena de custodia: algunos problemas específicos de exclusión probatoria*. [Tesis Posgrado, Universidad de León]. Repositorio Institucional. <https://buleria.unileon.es/bitstream/handle/10612/13161/NATAL%20MARCOS,%20Natalia.pdf;jsessionid=77940231BBD4184AAFB1318D078EEF25?sequence=1>
- Paternina, R. (2018). *Estudio de Vulnerabilidades en el proceso de Cadena de Custodia de evidencias en delitos informativos en la ciudad de Cartagena*. [Proyecto Aplicado- Informática Forense, Universidad Nacional Abierta y a Distancia]. Repositorio Institucional. <https://repository.unad.edu.co/handle/10596/28400>
- Plazas, R. Hernández, L. Flórez, M. (2016). El debido proceso y la cadena de custodia frente a las pruebas judiciales presentadas por el auditor forense. *Revista iusta*, N°046. <https://dialnet.unirioja.es/descarga/articulo/6685077.pdf>
- Peñalosa, B. (2022). *La Cadena de Custodia en los Delitos Informáticos en el año 2021*. [Tesis de grado, Universidad Estatal de Bolívar]. Repositorio Institucional.

<https://dspace.ueb.edu.ec/bitstream/123456789/5730/1/Informe%20Final%20BRENDA%20PE%c3%91ALOZA.pdf>

Revista seguridad 360. (2022). *La cadena de custodia para evidencia digital*. Recuperado de:

<https://revistaseguridad360.com/destacados/la-cadena-de-custodia/>

Rivera, P (2017). La cadena de custodia en delitos flagrantes. *Repositorio Dspace*.

<http://dspace.uhemisferios.edu.ec:8080/xmlui/bitstream/handle/123456789/723/ENSAYO%20.pdf?sequence=1&isAllowed=y>

Rubio, J. (2016). Conservación de la Cadena de Custodia de una evidencia informática.

Diario la Ley N°8859, Ed Wolters Kluwer. <https://peritoinformaticocolegiado.es/wp-content/uploads/Conservacion-de-la-cadena-de-custodia-de-una-evid...pdf>

Rodriguez, R. (2021). *El protocolo de la cadena de custodia y su responsabilidad penal en el*

Distrito fiscal de la Selva Central, 2020. [Tesis Pregrado, Universidad Peruana Los Andes]. Repositorio

Institucional. <http://www.repositorio.upla.edu.pe/handle/20.500.12848/3052>

Rubio, J (2016). Conservación de la cadena de custodia de una evidencia informática. *Diario*

Ley. N°8859. Ed Wolters Kluwer.

<https://peritoinformaticocolegiado.es/wp-content/uploads/Conservacion-de-la-cadena-de-custodia-de-una-evid...pdf>

Silvan, V & Méndez L. (2020) Cadena de custodia, su repercusión e importancia en el sistema de justicia penal oral acusatorio. *Revista Eco*

Sociales. <https://revistas.ujat.mx/index.php/ecosoc/article/download/4627/3565/25383>

Solís, J. (2016). El delito de espionaje informático en el derecho internacional y costarricense:

una modalidad de infracción del derecho humano de la intimidad. *Anuario De*

Derechos Humanos, (12), 103–118. <https://doi.org/10.5354/adh.v0i12.42744>

Suxo, J (2019). Pharming, nuevo fraude informático. *Revista informática forense*.

<http://www.revistasbolivianas.ciencia.bo/pdf/rits/n3/n3a13.pdf>

Torres. (2018) “Una nueva Mirada al Derecho de la Intimidad: Las Redes Sociales. *Revista*

EcoSociales, Vol 07, No 2. http://drevistas.ucv.cl/detalles_autor.php?autorID=19978

Vieira, A., & de Oliveira, S. (2020). La cadena de custodia de la prueba en el proceso penal.

Discusiones, 25(2), 205–258. <https://doi.org/10.52292/j.dsc.2020.2388>

Villa, E (2021). La cadena de custodia en el proceso penal. Fundación internacional de

ciencias penales. *Revista de Comunicación Penal*. [https://ficmp.es/wp-](https://ficmp.es/wp-content/uploads/2018/08/Villa-Boix.-Comunicaci%C3%B3n.pdf)

[content/uploads/2018/08/Villa-Boix.-Comunicaci%C3%B3n.pdf](https://ficmp.es/wp-content/uploads/2018/08/Villa-Boix.-Comunicaci%C3%B3n.pdf)

ANEXOS

PLANTEAMIENTO DEL PROBLEMA	OBJETIVOS	CATEGORIA Y SUB CATEGORIA	METODOLOGIA DE LA INVESTIGACIÓN
<p>¿De qué manera se aplica la cadena de custodia en el delito de fraude informático en Perú,2021?</p>	<p>Objetivo general: Analizar de qué manera se aplica la cadena de custodia en el delito de fraude informático en Perú, 2021</p> <p>Objetivo específico 01: Determinar la importancia de la cadena de custodia en Perú, 2021.</p> <p>Objetivo específico 02: Determinar la importancia del delito de fraude informático en Perú,2021</p>	<p>Categoría 01 Aplicación de la cadena de custodia</p> <ul style="list-style-type: none"> • Derecho • Preservación <p>Categoría 02 Fraude informático</p> <ul style="list-style-type: none"> • Tecnología • Desmerito patrimonial 	<p>Enfoque: Cualitativo Diseño teoría fundamentada Tipo: Básico Nivel: Descriptivo Población: La población se comprende como finita, porque nos indica una determinada población, debido que el número de valores que la componen tienen un fin.</p> <p>Muestra: Análisis documental y Jurisprudencial</p> <p>Tipo de investigación: realizada es de tipo básica, porque brinda un mejor entendimiento acerca del tema.</p> <p>Instrumentos: Guía de análisis documental</p>

Anexo 1 Guía de análisis documental

Tema de investigación	Analizar de que manera se aplica la cadena de custodia en delito de fraude informático
Título	La prueba pericial digital y la cadena de custodia
Autor (es)	Jose Miguel Gonzales Reyes
Organización y año de publicación	España,2021
Referencia de la revista	Revistas anales de la facultad de derecho
Palabras claves	Prueba pericial, cadena de custodia
¿Qué variable analizamos?	Cadena de custodia
Problema que enfrente el investigador	Requisitos que han de tener las pruebas, como lo es la cadena de custodia en la comisión de delitos a través de medios informáticos.
¿Qué resultados obtuvo? (hallazgos concretos)	La correcta aplicación o mantenimiento de la cadena de custodia se realiza con un clonado o copia de los dispositivos, de modo que se obtiene la formulada función hash o huella digital, con ello se garantiza la inalterabilidad de los dispositivos aprehendidos, en ese sentido la integridad del contenido es obtenida realizando una comparación de la información aprehendida y la información original, debiendo estas coincidir en todo momento
Conclusiones relevantes	La cadena de custodia con respecto a las evidencias informáticas es trascendental para lograr el convencimiento al tribunal, exponiendo que la prueba sea autentica, de la misma manera que no haya sido alterada por haber utilizado la función hash.
Link	https://riull.ull.es/xmlui/bitstream/handle/915/25818/AFD_38_%282021%29_03.pdf?sequence=1&isAllowed=y

Tema de investigación	Analizar de qué manera se aplica la cadena de custodia en delito de fraude informático
Título	La cadena de custodia de la prueba en el proceso penal
Autor (es)	Antonio Vieira, Saulo Murillo de Oliveira Matto
Organización y año de publicación	2020
Referencia de la revista	Revista Discusiones
Palabras claves	Cadena de custodia, prueba, proceso penal
¿Qué variable analizamos?	Cadena de custodia
Problema que enfrentó el investigador	Analizar la obra la cadena de custodia de la prueba en el proceso penal
¿Qué resultados obtuvo? (hallazgos concretos)	La prueba obtenida con violación de la cadena de custodia tendrá que ser prueba ilícita, por consiguiente, inadmisibles dentro del proceso penal, dado que no cumplen los presupuestos mínimos de integridad y fiabilidad, ello sin mencionar las cuestiones epistemológicas sobre producción probatoria y los principios del estado de inocencia, contradictorio y de defensa
Conclusiones relevantes	La contaminación de las evidencias por la ruptura de la cadena de custodia debe ser inadmisibles, debido a su obtención por medios ilícitos.
Link	https://ficip.es/wp-content/uploads/2018/08/Villa-Boix.-Comunicaci%C3%B3n.pdf

Anexo 3 Guía de análisis documental

Tema de investigación	Analizar de qué manera se aplica la cadena de custodia en delito de fraude informático
Título	La cadena de custodia en el proceso penal
Autor (es)	Elena Villa Boix
Organización y año de publicación	2021
Referencia de la revista	FICP
Palabras claves	Cadena de custodia
¿Qué variable analizamos?	Cadena de custodia, fraude informático
Problema que enfrento el investigador	¿La cadena de custodia que no sea conservada e inalterada será imposible ser objeto de valoración?
¿Qué resultados obtuvo? (hallazgos concretos)	Los dispositivos informáticos y electrónicos cumplen un rol fundamental para la realización de la cadena de custodia en los delitos informáticos, por los datos que comprenden dentro de los mismo y que tienen como fin de ser incluidos en el juicio oral, sin embargo, existen limitaciones como los derechos de autor, intimidad personal, familiar etc. Por ello es imprescindible el uso de los protocolos frente a este tipo de delitos.
Conclusiones relevantes	La cadena de custodia esta vinculada al aseguramiento de los dispositivos informáticos. La cadena de custodia no debe violar otros derechos en la búsqueda de evidencias.
Link	https://fcp.es/wp-content/uploads/2018/08/Villa-Boix.-Comunicaci%C3%B3n.pdf

Anexo 4 Guía de análisis documental

Tema de investigación	Analizar de qué manera se aplica la cadena de custodia en delito de fraude informático
Título	El debido proceso y la cadena de custodia frente a las pruebas judiciales presentadas por el auditor forense
Autor (es)	Rodrigo Alberto Plazas Estepas Ludivia Hernández Aros Mario Heimer Flórez Guzmán
Organización y año de publicación	Colombia, 2016
Referencia de la revista	Revista Iusta
Palabras claves	debido proceso, cadena de custodia, prueba judicial, auditoria forense
¿Qué variable analizamos?	Cadena de custodia, fraude informático
Problema que enfrento el investigador	¿Explicar por qué la cadena de custodia debe seguir un proceso las cual garantice eficacia y eficiencia?
¿Qué resultados obtuvo? (hallazgos concretos)	La aplicación de la cadena de custodia implica factores como la recolección, identidad, embalajes y envío, del cual se debe tener en cuenta la responsabilidad y preservar toda la evidencia a fin de garantizar la autenticidad, posterior a ello dichas evidencias serán presentadas al juez para que este pueda contrastar la realidad con los hechos controversiales
Conclusiones relevantes	Para que la prueba sea valorada en el proceso judicial debe ceñirse a la legalidad de la cadena de custodia, asimismo que esta sea hecha por un perito experto, destinado por el juez.
Link	file:///C:/Users/jean_/Downloads/Dialnet-EIDebidoProcesoYLaCadenaDeCustodiaFrenteALasPrueba-6685077.pdf

Anexo 5 Guía de análisis documental

Tema de investigación	Analizar de qué manera se aplica la cadena de custodia en delito de fraude informático
Título	La cadena de custodia en los delitos flagrantes
Autor (es)	Paola del Carmen Rivera Vargas
Organización y año de publicación	2017, Ecuador
Referencia de la revista	Repositorio Dspace
Palabras claves	Cadena de custodia, delitos
¿Qué variable analizamos?	Cadena de custodia
Problema que enfrento el investigador	¿cuáles son las dificultades que tiene la cadena de custodia a la hora de investigar un delito?
¿Qué resultados obtuvo? (hallazgos concretos)	La mayoría de investigaciones delictuales son aplicadas desde el escritorio o estas se establecen luego de un extenuante tiempo de ejecución el delito, pudiéndose de esta manera vulnerarse aquellas evidencias encontradas, demostrando una violación a los derechos humanos de las partes en el proceso, por la pronta actuación y la inadecuada aplicación de la cadena de custodia.
Conclusiones relevantes	La poca eficacia y eficiencia que tiene los órganos de justicia no permiten la realización de una adecuada cadena de custodia
Link	http://dspace.uhemisferios.edu.ec:8080/jspui/handle/123456789/723

Anexo 6 Guía de análisis documental

Tema de investigación	Analizar de qué manera se aplica la cadena de custodia en delito de fraude informático
Título	La cadena de custodia
Autor (es)	Pablo Hernández Romo Valencia
Organización y año de publicación	2019
Referencia de la revista	Revista Teorder
Palabras claves	Cadena de custodia
¿Qué variable analizamos?	Cadena de custodia, fraude informático
Problema que enfrento el investigador	¿Identificar que el objeto del lugar de los hechos pertenezca al presunto responsable del delito?
¿Qué resultados obtuvo? (hallazgos concretos)	En cuanto a la aplicación de la cadena de custodia la persona que custodio el material probatorio, será llamado a testificar y en caso de existir una pérdida de un elemento o pieza de la cadena de la custodia no será algo grave, dado que se probará con la prueba y no solo por la admisión de la misma.
Conclusiones relevantes	La cadena de custodia no se limita a un elemento o la desaparición del mismo o a su alteración, dado que estas pruebas muestran rasgos únicos que hace que la cadena de custodia no se relevante.
Link	https://ojs.tirant.com/index.php/teoria-y-derecho/article/view/276/27

Expediente	00041-2019-18-5001-JR-PE-03
Juez	Jorge Luis Chavez Tamariz
Imputado	Karin Janet Marengo Nuñez
Delito	Lavado de activos
Agraviado	El Estado
País y año	Perú, 2019
Análisis del expediente	El juzgador hace un correcto señalamiento sobre la ruptura de la cadena de custodia, donde se menciona que, al momento de la ruptura u omisión del mismo, no dará lugar a que el cuerpo del delito no sea autentico y que por tal motivo llegar a la conclusión de que este no contenga eficacia probatoria, dado que la cadena de custodia tiene por objeto la demostración de algún objeto incautado para expresar la autenticidad del mismo. Ahora bien, el acuerdo plenario 06- 2012 también señala que la cadena de custodia es aquel sistema que permite detallar de manera cierta el cuerpo del delito encontrado en el lugar de los hechos. En este sentido es preciso inferir que la cadena de custodia solo protege la identidad del objeto, mas no la cantidad, ni mucho menos la calidad, por la simple ausencia de la cadena de custodia, por ello no se podría decir que nos encontramos frente una ilegitimidad de la prueba, dado que este no vulnera ningún derecho fundamental.
Conclusiones	La cadena de custodia resguarda aquellas evidencias o indicios encontrados en el lugar de los hechos. La ruptura de la cadena de custodia no implica la inautenticidad del cuerpo del delito.
Link	https://www.pj.gob.pe/wps/wcm/connect/8c63b1804715064aa859fafb82dac87c/18-5+Karen+Marengo+para+publicar.pdf?MOD=AJPERES&CACHEID=8c63b1804715064aa859fafb82dac87c

Tema de investigación	Determinar la importancia de la cadena de custodia en Perú, 2021
Título	cadena de custodia, su repercusión e importancia en el sistema de justicia penal oral acusatorio
Autor (es)	Víctor Hugo Silvan Rodríguez Lenin Méndez Paz
Organización y año de publicación	México, 2020
Referencia de la revista	Revista Ecos sociales
Palabras claves	Cadena de custodia, sistema de justicia, penal
¿Qué variable analizamos?	Cadena de custodia
Problema que enfrentó el investigador	¿Como lograr hacer entender el nuevo sistema denominado cadena de custodia?
¿Qué resultados obtuvo? (hallazgos concretos)	Por medio de la cadena de custodia los órganos encomendados en impartir justicia pueden tener una sólida base con respecto a la resolución de conflictos de los juicios, asimismo son diversos elementos humanos que tendrán contacto directo con la cadena de custodia, por ello al demostrar una falla o manipulación alguna se desestimara como elemento probatorio.
Conclusiones relevantes	La cadena de custodia permite generar credibilidad en el juzgador a fin de obtener un resultado libre de injusticia.
Link	https://revistas.ujat.mx/index.php/ecosoc/article/view/4627

Anexo 9 Guía de análisis

Tema de investigación	Determinar la importancia de la cadena de custodia en Perú, 2021
Título	Reflexiones sobre manejo adecuado de cadena de custodia en el nuevo proceso penal
Autor (es)	González, Diego García, Roberto Barrera, Anthuan Benítez, Luis
Organización y año de publicación	Panamá, 2021
Referencia de la revista	Revista semilla científica
Palabras claves	Cadena de custodia, proceso penal
¿Qué variable analizamos?	Cadena de custodia
Problema que enfrento el investigador	¿Como lograr hacer comprender las parte e importancia de la cadena de custodia en el manejo correcto de las evidencias?
¿Qué resultados obtuvo? (hallazgos concretos)	La cadena de custodia resulta indispensable, por su utilidad a las partes, en especial a la defensa, que podrá con esta disputar las pruebas de proceso, sin dejar de lado que la cadena de custodia incidirá sobre los resultados de los análisis periciales, además de mencionar que la cadena de custodia es aquel conjunto de medidas que se deben tomar para preservar, sin manipulaciones individuales sobre la evidencia que forma parte de la escena del crimen.
Conclusiones relevantes	La cadena de custodia importa a la parte de la defensa dentro del juicio, debido a su repercusión en la valoración del juez.
Link	https://repositorio.umecit.edu.pa/bitstream/handle/001/4707/2021-Semilla-Cientifica-2_full_lite-452-458.pdf?sequence=1&isAllowed=y

Anexo 10 Guía de análisis documental

Tema de investigación	Determinar la importancia de la cadena de custodia en Perú, 2021
Título	Cadena de custodia
Autor (es)	Ivan Mauro Lucardi
Organización y año de publicación	Argentina, 2019
Referencia de la revista	Universidad Siglo 21
Palabras claves	Cadena de custodia, protección de la prueba, proceso penal
¿Qué variable analizamos?	Cadena de custodia
Problema que enfrente el investigador	¿Como analizar la cadena de custodia desde la prueba encontrada en la escena de crimen?
¿Qué resultados obtuvo? (hallazgos concretos)	Es importante señalar que la Cadena de custodia brinda protección a aquella prueba recaudada en el lugar que se cometió el delito, por ello este punto se convierte de vital interés, resultando que el fracaso de las investigaciones suele darse por no dotar de mayores herramientas legislativas, dando como resultado que la prueba obtenida tiene capacidad de sentenciar o no al individuo, dado que estamos frente a un sistema donde se parte de la inocencia del sujeto.
Conclusiones relevantes	La cadena de custodia puede lograr el fracaso de las investigaciones si no se realiza con las adecuadas herramientas legislativas.
Link	https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/16171/LUCCARDI%20MAURO.pdf?sequence=1&isAllowed=y

Anexo 11 Guía de análisis documental

Tema de investigación	Determinar la importancia de la cadena de custodia en Perú, 2021
Título	Conservación de la cadena de custodia de una evidencia informática
Autor (es)	Javier Rubio Alamillo
Organización y año de publicación	Argentina, 2016
Referencia de la revista	Diario la Ley
Palabras claves	Cadena de custodia, evidencia informática
¿Qué variable analizamos?	Cadena de custodia
Problema que enfrento el investigador	¿Cómo determinar una posible la alteración de la cadena de custodia en las evidencias?
¿Qué resultados obtuvo? (hallazgos concretos)	La cadena de custodia cumple un rol de suma importancia cuando se hace hincapié a las pruebas que se utilizaran a manera de evidencia dentro de un proceso, por ello se establece que es una cuestión matemática, dado que la prueba o ha sido alterada o no lo ha sido. Por ello se evaluará que la prueba no haya sido alterada o manipulada desde su recolección hasta su estudio forense, para que los tribunales no denieguen su validez.
Conclusiones relevantes	Es común encontrar como evidencias una mala practica de la cadena de custodia, que trae consigo la inadmisión en los juicios.
Link	https://peritoinformaticocolegiado.es/wp-content/uploads/Conservacion-de-la-cadena-de-custodia-de-una-vid....pdf

Tema de investigación	Determinar la importancia de la cadena de custodia en Perú, 2021
Título	La cadena de custodia: algunos problemas específicos de exclusión probatoria
Autor (es)	Natalia Natal Marcos
Organización y año de publicación	España,2020
Referencia de la revista	Universidad de León
Palabras claves	Cadena de custodia, Derechos fundamentales, mismidad, prueba de cargo
¿Qué variable analizamos?	Cadena de custodia
Problema que enfrente el investigador	¿Como analizar la institución de la cadena de custodia, desde la figura de nuestro sistema procesal penal?
¿Qué resultados obtuvo? (hallazgos concretos)	Es notable que la cadena de custodia toma importancia desde el derecho a la defensa, presunción de inocencia, entre otras garantías. Por ello para que la prueba sea considerada como lícita, se debe haber practicado la prueba pericial, desde que realizo la toma de muestras hasta la valoración por los peritos especialistas en la materia, a fin de ratificar el informe pericial dentro del juicio oral.
Conclusiones relevantes	La cadena de custodia no comprende una total regulación en el sistema legal, por ello es necesario utilizar jurisprudencia
Link	https://buleria.unileon.es/bitstream/10612/13161/1/NATAL%20MARCOS%2C%20Natalia.pdf

Anexo 13 Guía de análisis documental

Tema de investigación	Determinar la importancia del delito de fraude informático en Perú,2021
Título	El delito de fraude informático: concepto y delimitación
Autor (es)	Laura Mayer Lux y Guillermo Oliver Calderón
Organización y año de publicación	Chile,2020
Referencia de la revista	Revista chilena de derecho y tecnología
Palabras claves	Phishing, Cibercrimen, sabotaje informático, espionaje, estafa
¿Qué variable analizamos?	Fraude informático
Problema que enfrento el investigador	¿Como se relaciona el delito de fraude informático frente a otros delitos informáticos?
¿Qué resultados obtuvo? (hallazgos concretos)	El fraude informático tiene importancia práctica, dado que dicho delito es el protagonista de la actual cibercriminalidad, porque es este tiene exclusivamente el ánimo de lucro, que permite hacer distinción sobre los delitos que pueda confundirse bajo el mismo termino, del mismo modo la noción de fraude informático en ocasiones es vinculada con conducta que aún son etapas de ejecución imperfecta e incluso actos preparatorios.
Conclusiones relevantes	El fraude informático se diferencia a otros delitos informáticos por el ánimo de lucro, esta característica hace su distinción.
Link	https://www.scielo.cl/pdf/rchdt/v9n1/0719-2584-rchdt-9-1-00151.pdf

Tema de investigación	Determinar la importancia del delito de fraude informático en Perú,2021
Titulo	Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú
Autor (es)	Mariel Melissa Mengoa Valdivia
Organización y año de publicación	Perú,2021
Referencia de la revista	Repositorio Universidad Cesar Valljeo
Palabras claves	Delitos informáticos, ignorancia (Derecho), penas
¿Qué variable analizamos?	Fraude informático
Problema que enfrento el investigador	¿Cómo el fraude informático atenta contra el patrimonio y como otra figura llamada phisermule no está aún clara?
¿Qué resultados obtuvo? (hallazgos concretos)	Es importante considerar que el fraude informático no solo tiene como bien protegido el patrimonio, donde a través del engaño la victima obra por error, sino además que con este delito nos encontramos a la lesión de los derechos humanos, como lo es la libertad, asimismo se hace importante la vinculación de este delito con otras conductas criminales como phiser-mule que forma parte de la consumación del acto delictual y sobre el daño al patrimonio del agraviado.
Conclusiones relevantes	El fraude informático vulnera el patrimonio y no se considera los derechos humanos que provienen también de este delito.
Link	https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/62379/Mengoa_VMM-SD.pdf?sequence=1&isAllowed=y

Anexo 15 Guía de análisis documental

Tema de investigación	Determinar la importancia del delito de fraude informático en Perú,2021
Título	El fraude como delito informático
Autor (es)	Chungata Cabrera, Ana Maribel
Organización y año de publicación	2015
Referencia de la revista	Universidad de Cuenca
Palabras claves	Fraude informático, delitos informáticos
¿Qué variable analizamos?	Fraude informático
Problema que enfrento el investigador	¿Cómo analizar las diversas modalidades de fraude informático y su tipificación?
¿Qué resultados obtuvo? (hallazgos concretos)	La relevancia del fraude informático que ha obtenido a lo largo de los años, ha permitido que diversos países ofrezcan cobertura ante este tipo de delitos, teniendo en cuenta que quien suelen cometerlos son personas que poseen una serie de habilidades o características que el delincuente común las carece, por último, es de señalar que este tipo de delito en muchos casos no se han descubierto, porque las personas evitar hace la denuncia correspondiente.
Conclusiones relevantes	El fraude informático es cometido por sujetos con conocimientos en materia informática, por ello es difícil perseguir el delito
Link	http://dspace.ucuenca.edu.ec/bitstream/123456789/21321/1/TESIS.pdf

Anexo 16 Guía de análisis documental

Tema de investigación	Determinar la importancia del delito de fraude informático en Perú,2021
Título	Phishing: Fraude informático y como evitarlo
Autor (es)	Carla Maria Mamani Castillo
Organización y año de publicación	2019
Referencia de la revista	Revista de Información tecnológica y sociedad
Palabras claves	Fraude informático, phishing
¿Qué variable analizamos?	Fraude informático
Problema que enfrento el investigador	¿Cómo lograr que el ciber navegante no sea víctima del delito de fraude informático?
¿Qué resultados obtuvo? (hallazgos concretos)	Es importante identificar que se encuentra frente a un posible fraude informático al momento de que se le solicite información personal o financiera, dado que ello permite a los criminales acceder a los datos ofrecidos a través de correos electrónicos o páginas web fraudulentas, que dan la sensación de estar frente un sitio web legítimo.
Conclusiones relevantes	Este tipo de delito consiste en simular ser una página web verídica, para que accedas a brindar tu información, y los delincuentes usen ello en provecho económico.
Link	http://www.revistasbolivianas.ciencia.bo/pdf/rits/n3/n3a10.pdf

Anexo 17 Guía de análisis documental

Tema de investigación	Determinar la importancia del delito de fraude informático en Perú,2021
Título	Pharming, nuevo fraude informático
Autor (es)	Jhoavana Doris Suxo Hinojosa
Organización y año de publicación	2019
Referencia de la revista	Revista Informática forense
Palabras claves	Fraude informático, pharming, código o lenguaje de virus, Malware, troyano o caballo de trola
¿Qué variable analizamos?	Fraude informático
Problema que enfrente el investigador	¿Cómo identificar la nueva técnica de fraude informático y evitar ser víctima del mismo?
¿Qué resultados obtuvo? (hallazgos concretos)	Es de suma importancia reconocer que el fraude informático tiene nuevas técnicas que hacen vulnerable a aquel usuario que accede a internet, más aún cuando la propagación acelerada de software maliciosos que se encuentran disponibles a los hackers, por ello a fin de disminuir los ataques informáticos se debe instalar sistemas de detección de las acciones que se llevan en el ordenador o computadora.
Conclusiones relevantes	El fraude informático tiene nuevas técnicas que hacen al usuario de internet cada ves mas vulnerable, por ello se urge la instalación de sistemas que prevengan la comisión de este ilícito.
Link	http://www.revistasbolivianas.ciencia.bo/scielo.php?script=sci_pdf&pid=S1997-40442009000200013&lng=en&nrm=iso&tlng=es

Expediente	Recurso de nulidad N° 206- 2019
Juez	Salas Arenas
Imputado	David Ricardo Moretti
Delito	Fraude informático
Agraviado	El Estado
País y año	Perú,2019
Análisis del expediente	En lo que respecta sobre el tema de delito de fraude informático, el juzgador vincula el término “phishing” que es un tipo de estafa altamente utilizado en la actualidad, donde se configura cuando el delincuente suplanta la identidad de empresas bancarias, utilizando el formato, logos, entre otros. Con la finalidad de conseguir datos privados de la víctima y estos puedan ser utilizados para la obtención de aprovechamiento económico. Ahora bien, el Juzgador menciona de manera inequívoca que para realizar el delito ya mencionado se requiere de una alta complejidad en el uso de las tecnologías para lograrlo, cuando en la práctica un sujeto con mínimos conocimientos sobre página web e incluso abundan los tutoriales de como empezar de cero a crear páginas, logos, diseños
Conclusiones	La ley 30096, ley de delitos informáticos, es clara en su artículo 8 sobre Fraude informático donde esta no señala ninguna cualidad, experiencia o extenuantes conocimientos sobre informática para la comisión de este delito. El phishing es una técnica delictual que se ha con mayor incidencia en el ámbito nacional e internacional, que se desarrolla con la creación de páginas web fraudulentas, para generar desmerito económico en la victima.
Link	https://img.lpderecho.pe/wp-content/uploads/2020/10/RN-206-2019-Lima-LP.pdf

Anexo 19. Guía de análisis jurisprudencial

Expediente	EXP. N.º 01189-2019-PHC/TC
Juez	Sardón de Taboada
Imputado	Primera Sala Penal de la Corte Superior de Lima
Delito	Fraude informático
Agraviado	El Estado
País y año	Perú, 2019
Análisis del expediente	El caso del Expediente N.º 01189-2019-PHC/TC, referente a Marcos Morales Vargas, trata sobre los delitos de fraude informático y falsificación de firma en documento privado. El beneficiario, condenado inicialmente a diez años, vio su pena reducida a seis años. La controversia central se centró en la aplicación de la Ley 30096, que regula los delitos informáticos y entró en vigor el 23 de octubre de 2013. El debate giró en torno a si los hechos delictivos, cometidos entre 2013 y 2014, estaban sujetos a esta ley. El Tribunal Constitucional finalmente declaró infundada la demanda de habeas corpus, confirmando la aplicación de la Ley 30096.
Conclusiones	El caso demuestra la complejidad en la aplicación de nuevas leyes en delitos informáticos, especialmente cuando los hechos ocurren en un periodo de transición legislativa. Resalta la importancia de la fecha de vigencia de las leyes en relación con la comisión de los delitos. Además, subraya el papel del Tribunal Constitucional en interpretar y aplicar la ley, asegurando que se respeten los principios de legalidad penal y justicia. Este caso establece un precedente importante en la jurisprudencia peruana sobre la aplicación de la legislación en casos de fraude informático y falsificación de documentos
Link	https://tc.gob.pe/jurisprudencia/2020/01189-2019-HC.pdf

Anexo 20. Guía de análisis jurisprudencial

Expediente	CASACIÓN N.º 536-2020
Juez	Sequeiros Vargas
Imputado	Sala Superior Mixta de Emergencia de la Corte Superior de Justicia de Arequipa
Delito	Fraude informático
Agraviado	El Estado
País y año	Perú, 2020
Análisis del expediente	El expediente CAS 536-2020 aborda el caso de Roberto Víctor Salas Vilca, condenado por los delitos de peculado y fraude informático en perjuicio del Estado peruano. El enfoque principal del caso fue la solicitud de Salas Vilca para convertir su pena privativa de libertad en una medida alternativa, como servicio comunitario o vigilancia electrónica, argumentando su condición de salud y la situación de la pandemia de COVID-19. Sin embargo, la Corte Suprema de Justicia de la República declaró infundado su recurso de casación, sosteniendo la aplicación del principio de legalidad y la igualdad ante la ley, confirmando así la improcedencia de su pedido de conversión de pena.
Conclusiones	El caso destaca la rigurosidad del sistema judicial peruano en el tratamiento de delitos graves como el peculado y el fraude informático, especialmente cuando afectan al Estado. La decisión de la Corte Suprema subraya la importancia de la aplicación estricta de la ley, respetando los derechos constitucionales, pero también enfatizando la necesidad de cumplir con las penas impuestas en casos de delitos contra la administración pública. Este caso es un claro ejemplo de cómo las circunstancias personales del condenado, incluso en el contexto de una pandemia, no eximen del cumplimiento de las sanciones impuestas por delitos de alta gravedad.
Link	https://cdn.www.gob.pe/uploads/document/file/2322074/CAS%20536-2020.pdf.pdf

Anexo 21 Guía de análisis jurisprudencial

Expediente	EXP: 00493-2022-20-5001-JR-PE-06
Juez	JORGE LUIS CHAVEZ TAMARIZ
Imputado	Cristian Ysla Peña, John Eddy Solís Cáceda, Jordán Fernando Vergara Zapata y la procesada Karol Pilar Linares Santillán Justicia de Arequipa
Delito	Fraude informático
Agraviado	El Estado
País y año	Perú, 2022
Análisis del expediente	El Expediente versa sobre un caso de estafa agravada y organización criminal. Los acusados estaban involucrados en una operación compleja que incluía fraude informático y el uso de cuentas bancarias para desviar fondos ilícitamente. Se abordaron cuestiones como el levantamiento del secreto bancario y de las comunicaciones, así como el análisis de dispositivos electrónicos incautados.
Conclusiones	La decisión del juez se centró en la prolongación de la prisión preventiva por un período adicional de 4 meses, destacando la necesidad de continuar con las investigaciones y análisis periciales. Este caso ilustra la complejidad y el desafío que representan los delitos de organización criminal y estafa agravada, especialmente en el ámbito del fraude informático. Resalta la importancia del análisis forense digital y la cooperación de las entidades financieras en la investigación de delitos económicos complejos.
Link	https://www.pj.gob.pe/wps/wcm/connect/3c6858004bb678fcb7e1b7dd50fa768f/7JIP+FINAL.pdf?MOD=AJPERES&CACHEID=3c6858004bb678fcb7e1b7dd50fa768f

Anexo 22 Guía de análisis jurisprudencial

Expediente	EXP. N.º 04310-2016-0-1801-JR-PR-23
Juez	Tirado Sevillano Luis Armando
Imputado	Pantoja Torres Karol
Delito	Fraude informático
Agraviado	Empresa Prosegur Tecnología Peru S.A y Banco Interbank
País y año	Perú, 2016
Análisis del expediente	El Expediente versa sobre un caso de estafa agravada en modalidad de fraude informático por parte de la imputada Karol Pantoja, de tal forma que usando métodos de estafa informática y cibernética ha estafado versando fondos en cuentas bancarias, como la realización de envíos de productos por parte de la empresa de Prosegur afectado directamente a cada una de estas empresas, y definiendo e tipo de penal de la sentencia.
Conclusiones	La decisión del juez se centró en la prolongación de la prisión preventiva por un período adicional de 3 años, destacando la necesidad de continuar con las investigaciones y análisis periciales. Este caso ilustra la complejidad y el desafío que representan los delitos de organización criminal y estafa agravada, especialmente en el ámbito del fraude informático. Resalta la importancia del análisis forense digital y la cooperación de las entidades financieras en la investigación de delitos económicos complejos. Así como falla en favor de las empresas Interbank, y Prosegur, condenándola a 4 años de pena privativa de Libertad.
Link	https://es.scribd.com/document/525547823/EXP-04310-2016-FRAUDE-INFORMATICO

Anexo 23. Guía de análisis jurisprudencial

Expediente	EXP. N.º 04310-2016-0-1801-JR-PR-23
Juez	Tirado Sevillano Luis Armando
Imputado	Pantoja Torres Karol
Delito	Fraude informático
Agraviado	Empresa Prosegur Tecnología Peru S.A y Banco Interbank
País y año	Perú, 2016
Análisis del expediente	El Expediente versa sobre un caso de estafa agravada en modalidad de fraude informático por parte de la imputada Karol Pantoja, de tal forma que usando métodos de estafa informática y cibernética ha estafado versando fondos en cuentas bancarias, como la realización de envíos de productos por parte de la empresa de Prosegur afectado directamente a cada una de estas empresas, y definiendo e tipo de penal de la sentencia.
Conclusiones	La decisión del juez se centró en la prolongación de la prisión preventiva por un período adicional de 3 años, destacando la necesidad de continuar con las investigaciones y análisis periciales. Este caso ilustra la complejidad y el desafío que representan los delitos de organización criminal y estafa agravada, especialmente en el ámbito del fraude informático. Resalta la importancia del análisis forense digital y la cooperación de las entidades financieras en la investigación de delitos económicos complejos. Así como falla en favor de las empresas Interbank, y Prosegur, condenándola a 4 años de pena privativa de Libertad.
Link	https://es.scribd.com/document/525547823/EXP-04310-2016-FRAUDE-INFORMATICO