UNIVERSIDAD CATÓLICA DE TRUJILLO

BENEDICTO XVI

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

PROGRAMA DE ESTUDIOS DE DERECHO

ACTOS DE INVESTIGACIÓN EFICACES PARA LA IDENTIFICACIÓN DEL SUJETO EN EL DELITO DE FRAUDE INFORMÁTICO EN LIMA CENTRO, 2024

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE ABOGADA

AUTORAS

BR. Corpus Machahua Joanna Dayan

https://orcid.org/0000-0002-0753-2937

BR. Ojeda Velasquez Geivi

https://orcid.org/0000-0003-0329-7359

ASESORA

Mg. Rodríguez Monzón Yesica Liliana

https://orcid.org/0000-0002-1594-5838

LÍNEA DE INVESTIGACIÓN

Análisis de las instituciones del derecho público y privado

TRUJILLO – PERÚ

2025

DECLARATORIA DE ORIGINALIDAD

Señora Decana de la Facultad de Derecho y Ciencias Políticas:

Yo, Rodríguez Monzón Yesica Liliana con DNI N° 43609819, como asesora del trabajo de investigación titulado "Actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro, 2024" desarrollado por las egresadas Br. Corpus Machahua Joanna Dayan con DNI N° 71327298 y la Br. Ojeda Velasquez Geivi con DNI N° 76812594 del Programa de estudios de Derecho; considero que dicho trabajo reúne las condiciones técnicas y científicas, las cuales están alineadas a las normas establecidas en el Reglamento de Titulación de la Universidad Católica de Trujillo Benedicto XVI y en la normativa para la presentación de trabajos de graduación de la Facultad Derecho y Ciencias Políticas; Por tanto, autorizo la presentación del mismo ante el organismo pertinente para que sea sometido a evaluación por los jurados designados por la mencionada facultad.

Rodríguez Monzón Yesica Liliana

Asesor

DNI N°43609819

AUTORIDADES UNIVERSITARIAS

EXCMO. MONS. GILBERTO ALFREDO VIZCARRA MORI, SJ

Arzobispo Metropolitano de Trujillo.

Gran Canciller.

Universidad Católica de Trujillo Benedicto XVI.

DRA. MARIANA GERALDINE SILVA BALAREZO.

Rectora de la Universidad Católica de Trujillo Benedicto XVI.

DRA. ROMY ANGELICA DÍAZ FERNÁNDEZ

Vicerrectora académica.

DRA. ENA CECILIA OBANDO PERALTA

Vicerrectora de Investigación

MG. BETSY SUCETY CÁRDENAS GARCÍA

Decana de la Facultad de Derecho y Ciencias Políticas.

DRA. TERESA SOFÍA REATEGUI MARÍN

Secretaria General

DEDICATORIA

A mis padres Michell Corpus y Sara Machahua, quienes siempre me alientan para lograr cada una de mis metas, enseñándome e inculcando el respeto y la responsabilidad. A mis hermanas Danna y Xianna Corpus , ellas me inspiran a ser mejor persona y profesional. Mi gratitud también a mis tíos Verónica, Aurelia, Alberto Machahua y a mis abuelos , quienes en conjunto me han motivado y han reflejado en mí el verdadero valor y apoyo incondicional.

Br. Corpus Machahua Joanna Dayan

Dedico esta tesis a mi madre, también a mi padre, hermanos, y a mi abuelita Jesús porque con su fortaleza, sabiduría y apoyo incondicional han guiado cada paso en mi vida, han sido mi guía en todo momento para lograr todos mis objetivos planteados. También le dedico a Dios porque gracias a él aprendí a ser paciente, y entender que las cosas y tiempos que vienen de él son perfectos.

Br. Ojeda Velasquez Geivi

AGRADECIMIENTO

Agradecemos a Dios, por todos los logros obtenidos y momentos maravillosos, uno de ellos fue permitirnos terminar los estudios universitarios y haber obtenido los conocimientos necesarios en la carrera de Derecho.

Agradecemos a nuestros padres y hermanos por estar en cada momento de nuestras vidas apoyándonos, con sus palabras de aliento para nunca rendirnos, han sido de gran motivación en el proceso de formación universitaria.

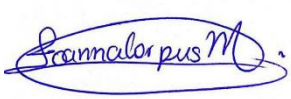
Agradecemos a nuestra apreciada asesora Mg. Yesica Rodríguez, quien nos compartió sus conocimientos para lograr esta investigación, motivándonos para seguir adelante.

DECLARATORIA DE AUTENTICIDAD

Nosotras , Corpus Machahua Joanna Dayan con DNI 71327298 y Ojeda Velasquez Geivi con DNI 76812594 , Bachilleres de la Escuela de Derecho de la Universidad Católica de Trujillo Benedicto XVI, otorgamos fe que hemos cumplido rigorosamente los procedimientos académicos y administrativos emanados por la Facultad de Derecho y Ciencias Políticas, para la elaboración y sustentación del informe de tesis titulada **“** Actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro, 2024 **”**, el cual consta de un total de 62 páginas, las que incluye tablas y figuras, haciendo un total de 77 páginas con anexos.

De tal manera dejamos constancia de la originalidad y autenticidad de la mencionada investigación y declaramos bajo juramento en razón a los requerimientos éticos, que el contenido del dicho documento, corresponde a nuestra autoría respecto a redacción, organización, metodología análisis y argumentación, asimismo, garantizamos que los fundamentos teóricos están respaldados por el referencial bibliográfico, asumiendo un mínimo porcentaje de omisión involuntario respecto al tratamiento de cita de autores, lo cual es de nuestra completa responsabilidad.

Las autoras,



…….. ……

JOANNA DAYAN CORPUS MACHAHUA

71327298

GEIVI OJEDA VELASQUEZ

76812594

ÍNDICE

ÍNDICE DE TABLAS

RESUMEN

La presente investigación tiene como problema principal cuales son los actos de investigación eficaces para la identificación del sujeto que ejerce fraude informático en Lima Centro 2024. Con el tiempo, el fraude informático ha generado y causado aspectos significativos, afectando la integridad, vulnerabilidad de derechos e hiriendo incluso la confidencialidad de datos personales, generando perjuicios patrimoniales y la desconfianza de las personas con el sistema financiero, es por ello que se tiene como objetivo general, establecer los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024. Ahora bien, para la metodología de esta investigación se ha utilizado un enfoque cualitativo, de tipo básico aplicando un diseño no experimental, la población está conformada por 10 especialistas entre abogados, fiscales y policías. Teniendo como técnica a la entrevista, como instrumento a la guía de entrevista. Finalmente, como conclusión, señalamos que los actos de investigación eficaces para la identificación del sujeto que comete fraude informático en Lima Centro son el levantamiento del secreto de las comunicaciones, el levantamiento del secreto bancarios, las pericias y la solicitud de información.

Palabras claves: *Actos de investigación, sujeto, fraude informático.*

ABSTRACT

The main problem of this research is the lack of effective investigative acts for the identification of the subject who commits computer fraud in Lima Centro 2024. Over time, computer fraud has generated and caused significant aspects, affecting the integrity, vulnerability of rights and even harming the confidentiality of personal data, generating patrimonial damages and distrust of people with the financial system, which is why the general objective is to establish effective investigative acts for the identification of the subject in the crime of computer fraud in Lima Centro 2024. Now, for the methodology of this research, a qualitative approach has been used, of a basic type, applying a non-experimental design, the population is made up of 10 specialists. Using observation and interview as techniques, and the interview guide as an instrument. Finally, as a conclusion, we point out that the effective investigative acts for the identification of the subject who commits computer fraud in Lima Centro are the lifting of the secrecy of communications, the lifting of bank secrecy, expert reports and the request for information.

Keywords: *Research acts, subject, computer fraud.*

I. INTRODUCCIÓN

A lo largo de la historia el uso del internet ha aumentado en gran magnitud, en la actualidad, a través de este se pueden cometer actos ilegítimos y deliberados, siendo así un problema perjudicial para la sociedad. Siendo necesario determinar los Actos de investigación para la identificación del sujeto que comete este tipo de delitos a través del internet. Cabe resaltar que el internet es muy favorable para la sociedad, pero ala vez es considerado un instrumento u objeto para la comisión de verdaderos delitos. Desde la pandemia COVID -19 del año 2020, los datos referentes a la comisión de fraudes informáticos aumentaron en grandes cantidades, donde fue mucho más visible saber que no se determinan actos de investigación eficaces que logren la identificación del sujeto que comete fraude informático, estas infracciones a la ley penal hacen referencia al abuso de las comunicaciones, lesionando los bienes jurídicos de las personas , poniéndolas en peligro, generándoles pérdidas y además amenazando la seguridad de los sistemas sociales. Lo que busca lograr la investigación es identificar los actos de investigación eficaces, donde los infractores sean sancionados. Para esto es necesario que se identifiquen enfoques dentro del ámbito internacional, nacional y local, teniendo como finalidad realizar futuros aportes.

En el ámbito internacional el crecimiento de las nuevas tecnologías ha sido beneficioso para todos, las personas comunes han quedado expuestas al manejo de la información, pero esto no quita que se cometan delitos. Desde la década de los 80, ha ocurrido un gran avance sobre el internet. En un estudio de Estados Unidos se tuvo como porcentaje que el 78.3% tenía uso de este acceso, en Europa se determinó un 58.3% de porcentaje, y un 37% se obtuvo en toda América (p.620). Con estos datos se puede determinar que el uso del internet ha ido avanzando en el tiempo, su uso a la vez ha incentivado a que se generen maneras de cometer delitos y uno de estos es el fraude informático. Dentro de la problemática se haya que los precedentes para la identificación de los sujetos que cometen este delito no son identificados correctamente debido a la falta de elementos esenciales que los sancionen. Todos estos malos usos solo han dado como resultados efectos nocivos. Cada país tiene leyes diferentes, dentro de sus respectivos marcos legislativos y jurídicos de cada uno de ellos. (Puerta Cortés & arbonell, 2013). La Organización para la Cooperación y el Desarrollo Económico (OCDE), empezó unos estudios con la finalidad de luchar contra el problema del uso de la internet. También se hace mención dentro del nivel Latinoamericano, donde en Chile se incluyó

penalidades de castigo, siendo de los primeros países en hacerlo, en otros países se aprobaron leyes de comercio a través del uso del internet, implementando las firmas electrónicas.

En un informe de la (PNP) se registraron 247 denuncias del delito de fraude informático, siendo este más al del año 2018, que en un total de denuncias se registraron solo 227. Los especialistas informaron que se encontraban con fotos falsas, con el fin deobtener un beneficio económico. Dentro de la problemática se haya que no se realiza eldebido proceso, iniciándose desde la investigación. No se han obtenido medidas referentes, observado con los resultados obtenidos. La falta de información y concientización hace que se genere un perjuicio social. Otras de las cifras registradas en el informe es que este delito obtuvo la mayor cantidad de denuncias.Fueron en total 2,097 (2019). La cifra fue aumentada en un 8% al año anterior con solo1928 denuncias.

En Lima, según informes emitidos por Instituciones referentes al control y sanción de los delitos de fraudes informáticos se identifica a esta como la ciudad con más casos. Este delito se consuma con el perjuicio patrimonial, la identificación de los sujetos se vuelve problemática cuando no se obtienen Actos de investigación de identificación, generando esto un proceso inconcluso, así como se buscan Actos de investigación eficaces estos agentes se valen de los mismos para no ser identificados. En el año 2021 el Ministerio Público brindó datos, en estos se indicaron que fueron 18,596 las denuncias recibidas por el delito de fraude informático. Se indicó un comparativo con el año 2020 y se obtuvo un incremento de 92,9 %. La pandemia fue identificada como una causa para la realización del delito, las personas al no poder salir realizaban grandes cantidades de compras a través del internet y los sujetos se las ingeniaban para sacar un provecho ilícito. Lo que se necesita y busca es generar futuros aportes del tema investigado. (Peruano, 2022). Durante el año 2023, se presentó un caso de fraude bancario mediante el uso de phishing (suplantación de identidad a través de correos electrónicos fraudulentos), en el que cientos de usuarios de una entidad financiera fueron víctimas del robo de sus datos personales y bancarios. A pesar de la rápida denuncia por parte de las víctimas, la identificación de los responsables fue lenta, debido a la falta de pruebas directas y al uso de herramientas como VPNs (red privada virtual) y números telefónicos falsificados, lo que complicó la tarea de rastrear las actividades fraudulentas. Este caso reflejó la necesidad urgente de mejorar las estrategias de investigación y los procedimientos operativos para garantizar una respuesta más efectiva ante estos delitos.

La razón fundamental para llevar a cabo esta investigación radica en la creciente incidencia del delito de fraude informático, que afectan tanto a individuos como a empresas y entidades. A medida que la tecnología y los medios digitales avanzan, los criminales también adoptan técnicas cada vez más sofisticadas para cometer fraudes. Esto genera desafíos en términos de identificación y persecución de los responsables. En Lima y en muchas otras ciudades, el fraude informático ha aumentado en los últimos años, y con ello, la necesidad de que las autoridades cuenten con métodos eficaces y legales para poder identificar a los culpables. La eficacia de ciertos actos de investigación, como la escucha telefónica, el levantamiento secreto de las comunicaciones, y pericias informáticas, es crucial para garantizar que se puedan realizar investigaciones que conduzcan a la identificación clara de los responsables de estos delitos, respetando siempre los derechos fundamentales de las personas.

En base a lo antes señalado es que se planteó el siguiente problema: ¿Cuáles son los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024?

Con respecto a la justificación teórica de esta investigación, está basada en la necesidad de expandir y actualizar los marcos conceptuales relacionados con el fraude informático, un fenómeno emergente en el ámbito de la criminología y la seguridad informática. Aunque el fraude informático es un tema que ha comenzado a recibir atención, las teorías existentes sobre su investigación y resolución son limitadas o, en muchos casos, desactualizadas. esta investigación tiene como objetivo garantizar que los métodos utilizados sean tanto eficaces como legales, asegurando que la identificación de los sujetos en fraudes informáticos sea precisa y justa.

Desde una perspectiva práctica, el fraude informático representa un desafío considerable para las autoridades encargadas de la investigación y la administración de justicia. La investigación proporcionará una guía concreta de los actos de investigación eficaces que pueden utilizarse en la identificación de los sujetos en el delito de fraude informático, lo que mejorará la práctica investigativa en este campo. Dado el crecimiento de la criminalidad cibernética y la sofisticación de los métodos empleados por los delincuentes, esta investigación tiene un impacto directo en la mejora de los procedimientos y la optimización de recursos en la persecución de estos delitos. Los resultados permitirán a los

investigadores, fiscales y jueces aplicar prácticas más eficientes, reducir tiempos de investigación y aumentar la tasa de resolución de casos relacionados con fraudes informáticos.

Esta investigación tiene un fuerte componente social, ya que contribuirá a mejorar la seguridad cibernética en la región y protegerá a los ciudadanos y organizaciones de ser víctimas de fraudes informáticos. Al mejorar los métodos de identificación de los delincuentes, se incrementa la confianza de la sociedad en el sistema judicial y en las instituciones encargadas de proteger sus derechos. Además, las soluciones planteadas permitirán la prevención de futuros fraudes, beneficiando a una población cada vez más dependiente de las plataformas digitales.

Desde el enfoque de una perspectiva metodológica, esta investigación se basa en la necesidad de evaluar y aplicar diversas técnicas de investigación, tanto tradicionales como tecnológicas, para abordar la identificación de los sujetos en fraudes informáticos. Al ser un campo complejo que involucra aspectos técnicos y legales, la investigación propondrá un análisis detallado de las metodologías actuales y emergentes en la investigación de delitos informáticos. Las técnicas cualitativas (como entrevistas a expertos) permitirá una visión integral de las mejores prácticas en la identificación de los delincuentes. Además, la investigación evaluará la efectividad de diversas herramientas digitales, como el análisis de patrones de comportamiento en línea y el uso de algoritmos forenses, para obtener resultados que sean prácticos y aplicables en el terreno.

La investigación tiene una justificación jurídica clave, dado que aborda la identificación de los sujetos implicados en el delito de fraude informático dentro del marco legal vigente en Perú. La regulación del fraude informático, a través de leyes como la Ley N° 30096 (Ley de Delitos Informáticos), es relativamente nueva, por lo que aún existen lagunas en los procedimientos y estrategias de investigación. Esta investigación tiene como fin identificar los procedimientos y normas necesarias para que las pruebas obtenidas en el marco de la investigación de fraudes informáticos sean válidas, admitidas y útiles en los tribunales. Además, la investigación puede proponer recomendaciones sobre el uso de la legislación actual, como la Ley de Delitos Informáticos en Perú, y su implementación efectiva.

Lo que busca la investigación es proporcionar información que sea útil, a fin de conocer cuáles son los fundamentos, criterios y técnicas para la identificación de los sujetos que cometen fraude informático, considerando también cómo se establece la normativa con relación a este delito. Logrando resultados que generen un cambio dentro del tema que se está estudiando.

En cuanto a los objetivos, de forma general se pretende establecer los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024. Como objetivos específicos se tiene: OE 01. Determinar si la escucha telefónica es un acto de investigación eficaz para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024. OE 02. Identificar como el levantamiento del secreto de las comunicaciones es un acto de investigación eficaz para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024. OE 03. Analizar las deficiencias que afronta el Ministerio Público para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024.

A fin de brindar mayor comprensión y relación con los objetivos de la investigación, se señalan los siguientes antecedentes:

Molinos (2020), en su tesis "El fraude informático y telemático: Perspectiva penal", tesis para optar el título profesional de abogado. sustentada en la Universidad de Valladolid (España). El objetivo principal de esta investigación es la aproximación de la legislación penal de los Estados miembros frente a los ataques informáticos, logrando cooperación policial y penal. Presenta un enfoque de tipo cualitativo, con el propósito de conocer la perspectiva penal del fraude informático y telemático. Como conclusión menciona que el delito de fraude informático e España se encuentra regulado en el artículo 248.2 a) del CP. Se introdujo en el CP de 1995 para regular aquellos delitos que, si bien se asemejaban en algunos aspectos al fraude informático tradicional, no terminaban de encajar con todos sus elementos, los cuales son el engaño, el error, el acto de disposición patrimonial por el sujeto activo, el perjuicio en la víctima, el ánimo de lucro y el nexo causal entre todos los requisitos, en este sentido la principal diferencia se va a encontrar con la necesidad de que la estafa o fraude se lleve a través de una manipulación informática.

Paguay & Granizo (2021), en su tesis para optar el título profesional de abogado, titulado "Las nuevas perspectivas regulatorias de delitos informáticos en las compras a través

de internet" sustentada en la Universidad Nacional de Chimborazo (Ecuador). Como objetivo de investigación planteado fue identificar cuáles son las perspectivas regulatorias de delitos informáticos en las compras a través de internet. Esta investigación por enfoque es de tipo cualitativo, por su propósito de identificar de qué manera se está afectando a las víctimas a través del internet. Se ha utilizado los métodos analítico sintético. Con respecto a la técnica e instrumento de recolección de información se empleó un caso práctico que evidencia que se vulnera los derechos de las personas que intervienen en el comercio electrónico a través de la internet, con lo que se deja evidenciado que se debería ampliar el campo de regulación de los delitos, teniendo como resultado la identificación de las perspectivas regulatorias de los delitos informáticos a través del internet. Se llega a la conclusión de que, en Ecuador, hay millones de personas con acceso a computadoras y teléfonos móviles en general, a través de los cuales pueden conectarse a internet, lo que las convierte en posibles consumidores de productos y servicios mediante el comercio electrónico. Sin embargo, estas personas necesitan una adecuada protección por parte del Estado para evitar la violación de sus derechos constitucionales en la red, especialmente el derecho a la propiedad, tal como se establece en el artículo 66, numeral 26 de la Constitución.

Por otro lado, Tenesaca & Cedeño (2021), en su tesis para optar el título profesional de abogado, titulado "El delito de fraude informático en redes sociales en medios electrónicos en la ciudad de Guayaquil a consecuencia de la cuarentena producto de la pandemia del coronavirus en el año 2020", sustentada en la Universidad de Guayaquil (Ecuador). Se tuvo como objetivo de investigación que se realice un análisis jurídico exhaustivo respecto a la implementación del delito de fraude informático mediante las redes sociales a causa de la pandemia. Esta investigación por su enfoque es de tipo cualitativo, por su propósito de determinar los elementos circunstanciales que inducen al cometimiento masivo de este tipo de delito penal y proponer un modelo evaluativo para disminuir la problemática planteada. Se trata de una investigación jurídica básica, en virtud de la importancia a los términos jurídicos, que utilizando técnicas y recursos del método de investigación teórico permita la búsqueda en las fuentes formales y materiales del Derecho. Con respecto a la población y muestras se realizaron 50 encuestas a profesionales en la materia, en la que obtendrá información con respecto a su percepción de los delitos y sobre la vulnerabilidad de los derechos inherentes a la calidad humana. Como conclusión señala que este delito le produce una disminución con respecto al patrimonio de la víctima, el

favorecido es el sujeto activo ya que obtiene un ingreso, a la vez que el virus aún influye mucho para la consumación de los delitos de fraude informático a través del internet.

Por otra parte, como antecedentes nacionales, se tiene a:

Huamán (2020), en su tesis para optar el título profesional de abogada, titulada "Los delitos informáticos en Perú y la suscripción del convenio de Budapest", sustentada en la Universidad Andina de Cusco (Perú). El objetivo de esta investigación fue explicar la manera en que la suscripción del convenio de Budapest influye en el tratamiento de los delitos informáticos. La metodología utilizada presenta un enfoque cualitativo, orientado en la revisión y obtención de datos de carácter teórico y legislativo. Los resultados de la investigación explican cómo influye el tratamiento de los delitos informáticos en la suscripción del convenio de Budapest. Indicando que, estos no han trascendido más allá de la normativa de nuestro país en relación de los delitos informáticos siendo que los avancen tecnológicos han influenciado en el avance. Siendo que los delitos informáticos en nuestro país generan mayor trascendencia a nivel interno. A modo de conclusión, se señala la necesidad de establecer normas procesales orientadas a adecuar el tratamiento normativo de los delitos informáticos.

Además Beraún (2021), en su tesis para obtener el título profesional de Abogado. Titulada "El delito de fraude informático por medios tecnológicos en tiempos de la covid-19, Lima, 2020" sustentada en la Universidad Cesar Vallejo (Perú). El objetivo de la investigación fue el analizar cómo incrementó el delito de fraude informático por medios tecnológicos en tiempos de la COVID-19, Lima, El nivel de investigación utilizado en la investigación fue de enfoque cualitativo y de tipo básico, orientado a un diseño de teoría fundamentada. se emplearon métodos de entrevistas a especialistas en el delito de fraude informático, como instrumentos de recolección de datos se utilizaron la guía de entrevista y guía de análisis documental. como resultado de todo lo empleado y en base a los especialistas y la norma pues advierten que en efecto el delito de fraude informático con uso de medios tecnológicos, bajo las modalidades de compra por internet como maleta retenida u otras se incrementó de forma relevante por la pandemia de la COVID-19. Como conclusión se afirma que debido a la pandemia que se está atravesando hubo un incremento de los delitos de fraude informático a través de los medios tecnológicos y esto ha generado un gran perjuicio en las personas.

Luego, Delgado & Villanueva (2022), en su Tesis para optar el título profesional de abogado, titulada "Fraude informático en la modalidad de phishing y la necesaria actualización de la legislación para una eficiente persecución y sanción penal", sustentada en la Universidad Señor de Sipán (Perú). El objetivo de esta investigación fue aplicar una actualización de la legislación para una eficiente persecución y sanción penal del delito de fraude informático en la modalidad de phishing. La metodología que se utilizó para esta investigación corresponde es de tipo descriptiva, con un enfoque cualitativo, teniendo un diseño no experimental simple. A modo de conclusión se menciona que través de los avances tecnológicos se han incrementado nuevas modalidades de fraudes informáticos he ahí la nueva modalidad del delito de phishing, que en la legislación peruana no se encuentra regulada generando así que personas con conocimientos informáticos cometan estos actos ilícitos en su nueva modalidad, ocasionando así una desprotección directa a la sociedad por su falta de incorporación en la legislación peruana.

Malca (2023) en su tesis para obtener el grado académico de Maestra en Derecho Penal y Procesal Penal. Titulada "Eficacia de la persecución penal en la investigación preparatoria del delito de fraude informático, Callao 2022" sustentada en la Universidad Cesar Vallejo (Callao). El objetivo de esta investigación fue Analizar cómo la eficacia de la persecución penal influye en la investigación preparatoria del delito de fraude informático, Distrito Fiscal de Lima, 2022. La metodología que se llevó a cabo tuvo un enfoque cualitativo de tipo básico, de diseño fenomenológico. Los resultados de esta investigación nos señalan que la persecución penal resulta de suma importancia en la etapa de investigación preparatoria, toda vez que al realizar una investigación eficaz la misma podría conllevar a romper las limitaciones existentes al investigar el delito de fraude informático en el distrito fiscal de Lima, 2022. Como conclusión se han detectado varias deficiencias en la investigación fiscal del distrito fiscal del Lima, lo que limita significativamente la investigación del delito de fraude informático. Estas deficiencias se deben a la falta de información sobre el tema y el caso específico, la dificultad para identificar al autor presunto del delito y proteger la información, así como la evolución tecnológica y la obtención de evidencia digital, entre otras.

De igual forma, Carbajal (2022), en su Tesis para optar el grado académico de Maestra en Derecho de Ciencias Penales, titulada "Las fiscalías especializadas en delitos informáticos como mecanismo para la lucha contra el cibercrimen", sustentada en la

Universidad de San Martín de Porres (Lima). El objetivo de la investigación es en como las fiscalías especializadas en delitos informáticos determinen mecanismos eficaces para luchar contra el cibercrimen. La metodología que trató fue de enfoque cualitativo, de tal manera que se analizaron las dificultades de la investigación. Dentro de los resultados de investigación se encontraron que los ciberdelitos representan daños inmateriales en el ciberespacio, contrario a los comunes que expresan resultados en el mundo exterior con daños físicos. En las conclusiones planteadas se especificaron que el fraude informático tiene una gran incidencia delictiva dentro de sus modalidades más recurrentes como transferencias y retiros no autorizadas, compras fraudulentas. Lo impreciso de lo investigado es que no se especifican normas expresas para la aplicación de las sanciones por delitos de fraudes informáticos.

De otra manera, Vargas (2022), en su tesis para obtener el grado académico de doctor en derecho. Titulada "Necesidad de tipificar la estafa básica en la ley de delitos informáticos para reducir la impunidad en el Perú" sustentada en la Universidad Cesar Vallejo (Lima). El presente estudio de investigación tiene como objetivo sustentar los fundamentos socio jurídicos para tipificar del eje data el fraude informático básica en el capítulo de los delitos patrimoniales de la ley de delitos informáticos donde se sancionaría a los agentes delictivos que hacen uso de internet y de las distintas TIC para que induzcan al error y engañen a las personas con el objetivo de adueñarse de su patrimonio. El enfoque que presenta es cualitativo, el tipo de investigación empleado en este presente trabajo de investigación es la aplicada por qué se va a orientar a que se resuelva, el diseño para esta investigación es de la teoría fundamentada en este caso el investigador va a explicare o dar como hipótesis respecto al fenómeno que corresponde al contexto específico que tiene relación con el tema a desarrollar y todo esto obtenido en el trabajo de campo. Se concluye que los desafíos que enfrentan policías y fiscales en la investigación de ciberdelitos están relacionados con la escasez de personal capacitado y especializado, la falta de equipos informáticos y la carencia de una logística adecuada que les permita obtener evidencia digital respaldada por dictámenes periciales favorables para llevar a juicio a los ciberdelincuentes.

Finalmente, Calderón (2023), en su tesis para obtener el grado académico de abogada. Titulada "las Fintech y el delito de fraude informático" sustentada en la Universidad Cesar Vallejo (Lima). Esta investigación tiene como objetivo determinar si existen riesgos de que las Fintech sean utilizadas como medios para llevar a cabo delitos de

fraude informático mediante el uso de servicios financieros y tecnológicos. El enfoque adoptado es cualitativo, y el tipo de investigación corresponde a un método básico. El diseño de investigación empleado en esta tesis es la teoría fundamentada, con el propósito de analizar los datos obtenidos de libros, artículos, tesis, doctrina, entre otros, ya que dicha información facilita la interpretación de los diversos paradigmas que emergen durante el estudio del tema propuesto en la tesis: las Fintech y el delito de fraude informático. En este sentido, la investigadora debe examinar la realidad a partir de su interacción con ella. Los resultados muestran que efectivamente existe un riesgo de que las Fintech sean utilizadas para llevar a cabo actos ilícitos. Se concluye que la falta de conocimiento por parte de los usuarios sobre los servicios a través de aplicaciones o sitios web ocasiona ser víctimas de este delito. y también la negligencia del Estado al no desarrollar leyes o normativas adecuadas.

En cuanto a las bases teóricas, el autor Acurio (2021) señala que la posición de la doctrina referente al tema del fraude informático es utilizada como la ciencia jurídica con el fin de explicar los alcances de la víctima, en gran parte dentro de la doctrina se sostiene que la víctima en el delito de fraude informático ya no es considerada como un objeto sobre el cual va a caer esta acción delictiva, sino que su comportamiento va a ser el causante del resultado perjudicial para su patrimonio. En el derecho penal y en algunos casos con el tiempo se ha llegado a determinar que el engaño de la víctima ha sido consumando negligentemente por parte de la víctima ya que ellos rompieron sus deberes de autoprotección.

Para la definición de los delitos informáticos, estos son la acción antijurídica que se desarrolla en el marco informático o digital, que quiere decir esto, aplica herramientas tecnológicas para cometer un delito tipificado dentro de la normal legal. Sobre los aspectos históricos del fraude informático. Según la RAE (2022) el fraude viene a ser la acción que va contra la rectitud o veracidad en perjuicio de un tercero. El bien protegido en este tipo de delito es el patrimonio en general, y el hecho punible es la acción y comportamiento que dañan el patrimonio a través del uso de los sistemas de información.

Según indica Acurio (2015), todas las dimensiones de la actividad humana existen el engaño, las maniobras ilícitas, la codicia, las ganas de venganza, el fraude, en conclusión, el delito; por lo que los delitos informáticos, “Es aquella conducta orientada a engañar los

sistemas de dispositivos de seguridad, esto es, a la ocupación ilegal a computadoras, correos o sistemas de datas aplicando una clave de acceso; actos típicos que solamente se cometen a través de los medios tecnológicos. (p. 6)

Por su lado, Urdanegui (2023) señala que:

Los delitos informáticos pueden ser definidos con la acción ilícita que es ejercida en un ambiente tecnológico, donde se utilizan recursos informáticos como computadoras , Dada las nuevas tecnologías , se fue dando concurrencia a más delitos informática, el uso de las TIC produce una ventaja a los delincuentes para ejercer delitos , incluso en algunos casos se observa como estos incluso superan barreras territoriales, a su vez, borran la información con el fin de no conocer sus fechorías (pág. 23).

Autores como Chuco (2023), afirman que "los delitos informáticos protegen intereses en función a la naturaleza del tipo penal".

Sobre los aspectos históricos del fraude informático:

Mayer y Liver (2020), refieren que en el año 1822, el Código Penal español es quien aplica por primera vez el fraude informático, denominándola las conductas por las cuales el autor se va a valer por medio del engaño o de cualquier medio fraudulento para que la víctima le otorgue de forma voluntaria cierta parte u en totalidad su patrimonio. En nuestro país como base teórica referente se tiene como antecedente legislativo recién en el año 1924 al artículo 244 del Código Penal, el cual establecía que : "El que con nombre supuesto, calidad simulada, falsos títulos, influencia mentira, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación, o valiéndose de cualquier otro artificio, Astucia o engaño, se procure o procure a otro un provecho ilícito con perjuicio de tercero, será reprimido con penitenciaria o prisión no mayor de seis años ni menor de un mes" (págs. 156-161).

Sobre la teoría de este delito por la Pandemia COVID-19, Espinoza (2020) señala que, que el delito de violación a las medidas sanitarias es una medida típica de características preventivas que proviene de disposiciones jurídicas hacia el derecho penal como delito. Este aumento explosivo resultó detectado por comunidades y grupos técnicos orientados a

descubrir fraudes. “Hay grupos criminales que tienen infraestructura armada para fraudes y más en situaciones propicias, donde se produce un aumento del tráfico de Internet” (p. 95)

El fraude informático por su parte es el acto antijurídico en el cual se realiza un fraude a través del uso de herramientas principales de tecnología, ya sea de internet o computadora, este involucra la intersección de la transmisión electrónica. El fraude informático también determinado fraude cibernético, es referido al fraude realizado a través del uso de internet o computadora, hay muchas formas comunes para cometer este tipo de delito, sobre todo con el avance que han tenido las herramientas tecnológicas, otra delas formas es donde se involucra la intercepción de transmisiones electrónicas, ocasionando robos de accesos personales (contraseñas), el número de una tarjeta u otra información confidencial sobre la identidad de una persona. (Pueblo, 2023, págs. 10-16)

Diversos autores se han referido al fraude informático, para (Custodio Cumpa, 2021) el cibercrimen adhiere el concepto de la capacidad para acceder a datos personales, los cuales presentan una gran importancia para los gobiernos y nación pero a su vez son utilizados para la afectación del sujeto pasivo. (Ávila Trivelli , 2023) señala que el fraude informático es la actitud idónea para dañar las redes de internet, medios electrónicos , a su vez el comportamiento que tienen los agentes que cometen este delito es doloso. Muchos doctrinarios con conocimiento refieren que los delitos informáticos ponen en riesgo la seguridad de la información, poniendo también en riesgo a otros bienes jurídicos que son protegidos, considerándose especiales por ser cometido a través de un medio informáticos.

Nazario y Villanueva (2022) coinciden en que;

El delito de fraude informático arremeta en contra del patrimonio de una persona, ya sea natural o jurídica, el lucro es considerado como el elemento principal de este delito , dentro de los supuestos del fraude informáticos, se tiene a el engaño, error y disposición del dinero o sujeto que cometa el acto ilícito, Los individuos sin escrúpulos siempre existirán, estos se aprovechan de las vacíos legales o mecanismos de identificación eficaces para ejecutar fechorías penales en distintas modalidades.

El Perú, dentro de sus definiciones, señala que el fraude electrónico es la acción ilícita que se realiza con el uso de una computadora, tiene la finalidad de distorsionar datos para inducir a otra persona a que deje de hacer o haga que ocasione una pérdida. Siendo que los

agentes autores de este delito se hacen valer de medios para distorsionar los datos de diferentes maneras e incluso alterando o borrando información almacenada. Nuestra legislación mediante la ley N.º 30096 (2013), regula los delitos informáticos, publicada en el año 2013 y la cual tiene por finalidad la prevención y castigo de las conductas delincuenciales que concierne al sistema e informaciones digitales, el secreto a las comunicaciones y la libertad sexual, la intimidad, impactando al patrimonio de la persona y a la fe pública del Estado, por lo cual el sujeto delincuencial, usa como herramienta la tecnología informática para cometer sus actos delincuenciales.

A su vez, esta ley ha pasado por modificaciones. Como el Art. 8 de la Ley (2014), modificado por Ley 30171 (2014), configura el delito de fraude informático como la acción ilegal que busca el aprovechamiento para sí u otro sujeto a través de la introducción, borrado, la alteración, la clonación de datos, la supresión u otros medios que interfieren o manipulen los datos del sistema informático, serán acreedores de una pena privativa de libertad entre 3 a 8 años; y entre 5 a 10 años cuando se tratase de afección del patrimonio del Estado. Los verbos rectores en este tipo de delitos es el diseño, la introducción, alteración, borrado, supresión o clonación de datos informativos,

Por su parte LLaja y Castañeda (2023) pretenden que, aun cuando la Ley N°30096 se encuentre tipificada dentro de los delitos contra el patrimonio, esta también vulnera los datos personales en distintas fuentes informáticas, evidenciándose así lo complejo de las conductas que se subsumen en un tipo penal determinado.

Respecto a los verbos rectores de este delito, Ávila (2023), refiere que la introducción es la acción de “entrar a un lugar”, para este tipo de delito corresponde al acceso que tiene el sujeto para ingresar a transgredir la información de la víctima. Sobre la alteración, se entiende a la modificación de los datos informáticos que se realizan para cometer el ilícito, el cual comprende agregar o adicionar datos que no existían. Por supresión, entendemos a que los datos informáticos serán desaparecidos, para ello, el sujeto tiene como fin no dejar registro del ilícito cometido. Para la clonación de los datos informáticos, esta comprende la creación de datos similares a los originales (pág. 167) .

El convenido de Budapest, o también conocido como el Convenio sobre la Ciberdelincuencia fue firmado en Hungría en el año 2001, el cual define a las conductas en cuatro topo de delitos: a) delito contra la confidencialidad, disponibilidad e integridad de los

datos y sistemas informáticos; b) delitos informáticos propiamente dichos; c) delitos contenidos ilícitos y d) infracciones al derecho de autor. Dicho convenio garantiza que las partes que realicen toda ayuda mutua posible tengan como fin las victorias de las investigaciones y junto con ellas las pruebas necesarias para la comprobación del delito.

Anteriormente, la División de Estafas de la Dirección de Investigación Criminal (Dirincri) era quien realizaba la investigación del delito de fraude informático. Asimismo, las comisarías y Departamentos de investigación criminal (Depincri) no tenían la suficiente especialización, incluso la Fiscalía. Luego, esta situación tuvo un cambio a la expedición de la Resolución Directoral N° 1695-2005- DIRGFN/EMG, del 8 de agosto del 2005, la cual creó la División de Investigación de Delitos de Alta Tecnología (Divindat). Dicha división fue creada debido al crecimiento del ciberdelito. Asu vez, las Fiscalía de la Nación publicó el 1 de enero del 2021, la Res. N° 1503- 2020-MP-FN, en la que se señala la creación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público, con el fin de brindar asesoría a fiscales en las investigaciones de los delitos que correspondan a la Ley de Delitos informáticos. (Nazario Delgado & Villanueva Sanchez, 2022)

Che León (2024), distingue que el Perú, al adherirse a este Convenio de Budapest, refleja un importante esfuerzo por querer adaptar dentro de su legislación estándares internacionales, permitiendo así poder establecer procedimiento que ayuden mejorar las investigaciones del delito de fraude informático. Lamentablemente con el tiempo no ha sido efectivo el uso de herramientas eficaces para la identificación del sujeto, evidenciándose en las cantidades de archivamientos fiscales y las pocas sentencias condenatorias,

Este convenio, es considerado como un instrumento jurídico que permite a los jueces y fiscales realizar distintos requerimientos de cooperación, conectado a los delitos informáticos. La relevancia de este convenio es de suma importancia porque permite que toda solicitud formulada por el operador jurídico sea remitida de manera célere a los Estados parte del Convenio. (Nación, 2020)

El personaje de mayor interés en los fraudes informáticos es el sujeto pasivo, este causará un perjuicio en el sujeto pasivo o víctima, la acción de solo un sujeto está descrito en el tipo penal, tratándose del sujeto activo. Respecto al estudio de la psicología de la delincuencia (López Latorre, 2006) configura que también los sujetos poseen ciertas definiciones para la conducción de los medios de internet, siendo estos situados en lugares

estratégicos o siendo muy hábiles con el manejo de las nuevas tecnologías a través del internet.

Asimismo, sobre el sujeto activo, diversos autores se refieren al sujeto activo por tal que acciona parte del delito descrito en el delito penal o toda. Garrido (1992) indica que también los sujetos posees ciertas definiciones que el denominador común de los delincuentes no presenta, estos tienen ciertos mecanismos que el común de otros delincuentes, siendo estos situados en lugares estratégicos o siendo muy hábiles con el manejo de las nuevas tecnologías a través del internet.

(Cervera Vargas, 2020) propone que:

Respecto a un artículo, autores como Lara señala que "el sujeto pasivo tiene un conocimiento especializado con respecto al internet (…) se puede ubicar como sujeto activo de un delito a un conocido en la materia o a un empleado que tenga un mínimo conocimiento en los usos de las nuevas tecnologías". (p. 16)

El sujeto activo, a su vez puede ser cualquier persona natural, sin la necesidad de estar calificado o preparado, basta que este tenga conocimientos suficientes para herir la seguridad de los sistemas informáticos. (Kerr, 2006)

Michael (2016) sobre el sujeto pasivo, lo refiere como la persona titular del bien jurídico y sobre el cual recae la actividad típica del sujeto activo, en el sujeto pasivo va a recaer toda la conducta de acción u omisión que realiza el sujeto activo. A su vez, el sujeto pasivo puede ser una persona natural, jurídica, institución u organización que maneje sistemas de información y que puedan ser afectadas.

(Mejía Barrera & Correa Alcaráz, 2018)nos dicen que:

Es de suma importancia al hablar del sujeto pasivo que se reafirme que en el delito de fraude, este será el que tendrá el perjuicio patrimonial, su derecho será aprovechado de forma ilícita por el otro sujeto, quien a consecuencia de los actos para que se cometa este delito logra su fin, esta persona se desfavorece y pierde parte de su patrimonio. El sujeto pasivo no siempre va a sintonizar con la persona que está siendo engañada, ya que hasta un tercero puede ser el intermediario ya que no va a recaer el patrimonio en este tercero sino en la víctima, también denominado sujeto pasivo de la relación (p.13).

Schlack (2008), refiere al bien jurídico como importante para las ciencias penales, la afectación que recae sobre un bien jurídico permite el fundamento del castigo punitivo a las conductas que transgreden o ponen en peligro la sociedad. La tipificación de una conducta como delito, tiene un bien jurídico protegido, este viene a ser la razón de la tipificación de este, siendo así el eje de la teoría del delito. Por otro lado, el perjuicio patrimonial es considerado una consecuencia del fraude informático, además para que se constituya fraude informático pues este elemento debe ser probado. El perjuicio no es una condición objetiva de punibilidad, tratándose este de un elemento del tipo penal, por esto el pago posterior de la suma de fraude informático no desaparece ni por la declaración de que se haya reparado. Todos los delitos presentan una serie de elementos que los diferencian de los otros y el delito de fraude informático no es la excepción, el elemento esencial y característico del fraude informático es el engaño, este será la diferencia para la figura de la apropiación indebida, de esta manera en la jurisprudencia se encontrará establecidos los elementos distintivos que distinguirá a este delito de los que pueden ser similares, también distinguirá a los que guardan relación en la materia civil.

Por otra parte, los actos de investigación son aquellas diligencias realizadas por la policía o el fiscal durante la investigación preparatoria, definida también como diligencias preliminares investigación formalizada, la cual está destinada a descubrir tanto los hechos punibles cometidos, así como las circunstancias de su perpetración y los posibles daños que han podido ocasionar de uno u otro modo. Estos actos, se llevan a cabo en una de las etapas que tiene por finalidad la de formular el caso y en caso de ser procedente, formular una acusación. Las sospechas o probabilidades de la comisión de un delito son motivos suficientes para los elementos de convicción. Desde una perspectiva procedimental, es de demostrar el desenvolvimiento de la investigación preparatoria, la cual está conformada por actuaciones heterogéneas, sin poseer una secuencia lineal o recta.

Dentro de los tipos de actos de investigación consideramos. El reconocimiento en rueda busca encausar la investigación y consiste en la exposición del implicado junto con un número variable de otras personas con características físicas similares, a fin de que la víctima o testigo lo señalen. Los seguimientos consisten en una labor de vigilancia de lugares y personas, normalmente a cargo de la policía, con el objeto de que los movimientos y hábitos que se observen durante el seguimiento puedan contribuir al descubrimiento de delitos. La intervención de comunicaciones consiste en obtener datos referidos a un sospechoso y un

concreto delito partiendo del contenido de su correspondencia, bien sea esta postal, telegráfica, telefónica, telemática o electrónica -en las primeras se procederá a la detención y apertura para tomar conocimiento de ella de la correspondencia postal y telegráfica, y en la última se intervendrá y observarán las comunicaciones telefónicas o telemáticas.

El levantamiento del secreto de las comunicaciones, para este acto de investigación es necesario que se cumplan con dos presupuestos, 1) fumus comissi delicti, es decir, existencia de suficientes elementos investigativos que sostengan la fundabilidad de los cargos iniciales; y, luego, (2) el respeto del de los presupuestos y requisitos del principio de proporcionalidad. Este acto es destacado como una medida instrumental restrictiva de derechos que son fundamentales, con carácter excepcional, considerándose como un medio excepcional de investigación y no como uno normal.

En el caso de los agentes encubiertos, se debe cumplir con un procedimiento especial autorizado por el fiscal con la reserva del caso, mediante el cual un agente policial, ocultando su identidad, se infiltra en una organización criminal con el propósito de determinar su estructura e identificar a sus dirigentes, integrantes, recursos, modus operandi y conexiones con asociaciones ilícitas. En relación con el fraude informático se usan agentes especiales en conocimiento de informáticas y nuevas tecnologías.

Por otra parte, el levantamiento del secreto bancario, La protección del secreto bancario, se encuentra regulado en la constitución política del Perú en el artículo 2 inciso 5, y hace referencia a la conservación que las instituciones financieras y los bancos tienen que establecer a sus usuarios con respecto a sus datos privados sobre sus movimientos bancarios y depósitos de cualquier índole, pero este derecho puede ser vulnerado mediante resolución fundada por el órgano jurisdiccional o también por autorización del titular de la cuenta bancaria. También existen casos excepcionales para que las entidades bancarias sean requeridas a entregar información de sus clientes sin orden formal. Esta responsabilidad recae sobre el juez, Comisión Investigadora del Congreso, Superintendencia de Banca y Seguros, Fiscal de la Nación, Administradoras Privadas de Fondos de Pensiones, esto también se encuentra establecido en la ley N°26702, articulo 143, lo cual especifica que las autoridades señaladas tienen la facultad de solicitar información directamente a la SBS. Si el fiscal provincial no cuenta con el documento que autorice el levantamiento del secreto bancario emitida por el titular de la cuenta, puede solicitar al juez mediante el requerimiento

la autorización. Cuando el juzgado declare fundado el requerimiento se puede proceder a solicitar la entrega de información a las entidades bancarias, ya sea nombre del titular de cuenta, la fecha que se apertura, movimientos activos y pasivos, y también los lugares donde se haya realizado retiros, como también datos relevantes concernientes al titular. El levantamiento del secreto bancario se encuentra reglamentado en la Ley 27379, y también en el código procesal penal artículo 235.

Sobre la Intercepción de las comunicaciones, se establece como la actividad criminal, neutraliza actividades criminales e individualiza interlocutores. Seguimientos, espionaje. Técnica considerada como arte porque se hace uso de la observación y seguimiento. Las personas que realizan estos actos son como considerados también como agentes de inteligencia o vigilante. Consisten en el acto de aplicación o técnica, el objetivo es identificar al autor del fraude informático.

Con respecto al acto de investigación de geolocalización, este se encuentra regulado por Decreto Legislativo 1182, desde el 2015, y en el código Procesal Penal artículo 230 inciso 4. La geolocalización tiene como finalidad establecer la ubicación del dispositivo móvil u aparato similar, en este procedimiento la autoridad policial encargada de una investigación solicitada por el fiscal pide a la unidad especializada (DIVINDAT), realizar geolocalización del dispositivo. Esta unidad solicita de inmediato la información, una vez que se obtiene la información, se genera un informe para presentar a la fiscalía. Luego la fiscalía solicita Convalidación Judicial ante el Juzgado, con la finalidad de obtener la ubicación física exacta del poseedor del dispositivo móvil. La mayoría de los dispositivos móviles están equipados con sistemas de geolocalización, como el GPS, Wi-Fi o la red 3G pueden desempeñar una función similar. En conclusión, la geolocalización es una herramienta de investigación que le permite al fiscal que tiene a cargo un caso para obtener la localización de los teléfonos, con el objetivo de identificar a la persona que lo está utilizando en ese momento y así localizar al autor del delito.

Por otra parte, las pericias, refiere a un análisis especializado con enfoques técnicos, científicos, artísticos u otros conocimientos realizados por expertos de alguna área determinada. La oficina de peritajes que dispone el Ministerio Público, se organiza en cinco áreas de Análisis Digital Forense, se realizan las actividades como: a) Acreditación de archivos digitales en formato de imagen, audio y video; b)se realiza el procesamiento de las

imágenes con el fin de identificación; c) búsqueda de archivos electrónicos en USB, teléfonos, computadoras, entre otros; d)verificación de los sistemas informáticos para poder determinar las manipulaciones ilegales, e)restauración de imágenes de cámaras; f)desbloqueo de celulares; g)restauración de WhatsApp, mensajes de texto y otros. De igual forma la dirección de Criminalística de la PNP tiene una División de Laboratorio de Criminalística, se organiza en ocho departamentos, uno de los cuales es el departamento de Laboratorio Digital, realiza funciones parecidas al área de peritaje que corresponde al Ministerio Público.

Las características de los actos de investigación pueden clasificarse en dos puntos de vista: Actos 1. que dirigen a buscar y adquirir las fuentes de la investigación y los 2. Actos que proporcionan por sí mismos las fuentes de investigación. La finalidad de los actos de investigación es acreditar o descartar los presupuestos condicionales de la apertura del juicio oral.

En cuanto a los tipos y formas de fraude (Oxman, 2013) nos menciona que la modalidad denominada Phishing tiene un origen etimológico inglés, denominado pesca. Este tipo de fraude informático se da a través del internet, por correo electrónico, lo que se busca con este tipo de fraude informático es que se engañe a la víctima para poder tomar acceso de sus cuentas bancarias, contraseñas, códigos de identificación personal e informaciones privadas. Para que se cometa este delito solo basta con efectuar a una persona indicada, así se arrojará los resultados eficaces para el agente activo, es necesario que se tenga en cuenta la prevención adecuada en la sociedad. En la actualidad muchas compras y transacciones se realizan por internet, el avance de la tecnología ha logrado que se cometa más de este delito. Basta que la persona haga un click para que los agentes activos puedan tener acceso a todo, de este tipo se desarrolla al invitar a la víctima a descartar la transacción si es conocida para él. Respecto al estudio de las Principales características, modos de perpetración y vulneración de la seguridad informática a través de la modalidad jardín, Duran señala que (2020) se puede “consideras que este tipo de fraude informático es de las más comunes, empezadas por el incumplimiento de los agentes, siendo que el producto no llegó a tiempo, no hay stock para realizar la entrega o la calidad no es la misma de la descripción” (p. 36).

Sobre el pharming, este tipo de fraude informático, el usuario al ingresar el nombre de su entidad bancaria en un motor de búsqueda como Google, o la dirección web del banco,

puede ser redirigido a un sitio falso creado por el delincuente. Como primer caso tenemos, cuando en el buscador agregas el nombre del banco, este sitio fraudulento aparece como primer resultado, lugar donde comúnmente están páginas ilegítimas, y es muy probable que la víctima vaya al enlace falso en los resultados. En el segundo caso (cuando se ingresa la dirección web del banco directamente), puede ocurrir que el sitio falso aparezca de inmediato o que se abra una ventana en el navegador con el sitio fraudulentamente creado.

Por otra parte, el método de la clonación de tarjetas de crédito se da cuando clonan una tarjeta mediante reproducción de su banda magnética. Los delincuentes obtienen los datos de la banda magnética al pasarla por un skimmer (un dispositivo que guarda esa información). Además, se encargan de obtener tu PIN (usando diferentes métodos) y con estos datos crean una tarjeta idéntica a la tuya pero falsa, que luego la utilizan para llevar a cabo los fraudes.

Sobre el Auction fraud, Miró (2020, Pág. 70) lo describe como un "fraude en las subastas, que implica la manipulación de un producto o la no entrega del mismo según lo acordado en las plataformas de subasta en línea como eBay".

Así mismo el denominado scam (Ciber fraudes burdos): Según Miró (2021, Pág. 69), los "Scam" o ciber fraudes burdos son aquellos fraudes en los que se promete una gran cantidad de dinero a cambio de pequeñas transferencias vinculadas a ofertas de trabajo, loterías, premios u otros similares.

Los antivirus falsos, son otros de los métodos para realizar el delito de fraude informático, ya que no siempre tienen una infección previa. Al visitar nosotros una página que a primera vista se ve de una apariencia profesional, se muestra una información falsa, advirtiendo que existe algo malicioso en el código, se llega a estas páginas a través de enlaces de otras páginas web, ya sea al pulsar enlaces en aplicaciones de mensajería instantánea o través de un correo no deseado. Cabe también mencionar que los fraudes se aprovechan en la instalación de un falso antivirus recién comprado.

Para que se evite este tipo de fraude, es necesario que se mantenga actualizado, teniendo las últimas firmas de los virus, se recomienda que no se pulse cualquier enlace, y más si este es nuevo o no reconocido teniendo una dudosa credibilidad, no descargar la protección de fuentes no confiables. Las nuevas actualizaciones y el avance de las nuevas

tecnologías, más la creación de muchas redes sociales a través del internet y con el tiempo, este tipo de fraude informático ha ido en incremento, muchas cifras se han ido conociendo y estas solo hacen evidencia de lo mencionado. Dentro de los tipos que se muestran son los perfiles atacados por un pirata informático, pidiendo dinero, esto puede suceder cuando un usuario roba dinero a través de una filtración de datos, suplantación de identidad, los sujetos activos se hacen valer de todo esto para cometer el delito de fraude informático. Las citas por internet también se han hecho muy comunes a través del tiempo, esto se da cuando los sujetos crean perfiles falsos, utilizando promesas de amor falsas hacia las víctimas haciendo que se les envíe dinero, una vez logrando la confianza de la víctima les dicen que necesitan de dinero para que se les envíe el dinero y próximo a eso desaparecen.

Muchas personas alquilan casas a través de las redes sociales buscando pasar un momento agradable, los sujetos agentes para cometer este delito toman fotos a casa que no son de su propiedad para así después a través del internet subir estas fotos y alquilarlas, este tipo de fraude informático es cometido de gran magnitud en las vacaciones, ya que muchos buscan pasar momentos fuera de casa o alejados de la ciudad, es necesario que se tomen medidas para no caer en estos fraudes informáticos.

De la misma forma, dentro de los tipos de alquileres de viviendas para cometer el delito de fraude informático, se tiene a los anuncios pirateados, para el cual se apropian de un verdadero listado de propiedades en alquiler, solo cambian los datos del agente inmobiliario, publicando el anuncio modificado a través de otro lugar de sitio web. Muchos no llegan ni a cambiar los nombres y piratean las cuentas de los verdaderos propietarios.

Para el tipo de alquileres fantasmas, los sujetos alquilan propiedades inexistentes, prometiendo bajos costos de alquiler. Muchos acceden a los bajos precios a modo de ahorro, pero lo único que se da es un fraude informático, los agentes que cometen el delito solo buscan favorecerse con el dinero, teniéndolo como objetivo. Así mismo, a través de internet se pueden realizar muchas acciones para acometer el delito de fraude informático, y el comprar de forma online es una de ellas. Los fraudes informáticos son muy comunes, en la pandemia que estuvimos atravesando se presentaron muchos casos, las personas al no poder salir tanto de casa debido a las restricciones impuestas por la autoridad buscaban adquirir cosas a través de compras en línea. Este tipo de fraude informático empieza a través de una página web, muchas tiendas falsas son creadas con el objetivo de cometer el delito de fraude

informático, incluso algunos invierten para poder cometerlo fácilmente otros ofrecen métodos y ventajas como un envío gratuito o entrega de un día a otro, de esta manera se aprovechan de las personas que hacen compras a través de la internet.

II. METODOLOGÍA

2.1 Enfoque y tipo de investigación

El enfoque de la presente investigación fue cualitativo por la relación de sus variables. Pulido, Quintero y Gutiérrez (2024) refieren que este enfoque fundamentalmente es la observación de fenómenos teóricos tal y como se han dado en su contexto para después ser analizados. Este tipo de enfoque utiliza la recolección de datos sin la intercepción numérica, ayudará además a determinar los actos de investigación eficaces para la identificación del sujeto que comete fraude informático.

El tipo de investigación de la presente tesis es básica, se observará que esta ampliará el conocimiento, a través de este tipo, se logrará el cumplimiento de los objetivos propuestos dentro de la investigación, el fin de este es aportar y orientar a lograr nuevos conocimientos de modo sistemático. (Huaire Inacio, 2019)

2.2 Diseño metodológico

El diseño aplicado fue el no experimental, el cual se emplea cuando no es posible manipular variables o cuando se busca estudiar situaciones tal y como ocurren en su contexto natural. En este tipo de diseño, el investigador observa las variables tal y como se presentan en la realidad, sin intervenir. (Martinez Mediano, 2014, págs. 31-38)

2.3 Procedimiento de muestreo

El procedimiento del muestreo se basó en entrevistas a varios expertos en el tema, su determinación es no probabilística, en consecuencia, no tendrá fórmulas de delimitación. Basándose la muestra en entrevistas a fiscales y policías de la Ciudad de Lima, con un total de 10 especialistas.

2.4 Técnicas e instrumentos de recojo de datos

La técnica que se utilizó fue la entrevista.

La entrevista por su parte es una técnica de gran utilidad para la investigación cualitativa, a fin de recabar datos importantes y precisos para el desarrollo de la investigación, propone un fin determinado desde la acción de conversar. Siendo además un instrumento técnico. (Diaz Bravo, 2013)

Como instrumento se utilizó la guía de entrevista:

La autora (Elaica,2018) señala que la guía de Entrevista es una herramienta creada para organizar y guiar una entrevista, con el fin de obtener información relevante y consistente. Facilita a los investigadores la recopilación eficiente de datos.

El autor (Tejero González, 2021), en su libro señala que: "La observación y la entrevista permiten al investigador adentrarse en la realidad social de los sujetos de estudio, obteniendo datos que no siempre son accesibles a través de otras técnicas. Ambas herramientas, proporcionan información valiosa para la interpretación de los fenómenos estudiados."

Para el recojo de información se utilizó como instrumento a la guía de entrevista. Siendo la observación una técnica que facilita la adquisición de la información. registrándose en bases de la investigación (Fernández A., 2024, Pag.84).

2.5 Técnicas de procesamiento y análisis de datos

La técnica elegida es la guía de entrevista, porque nos ayudó a obtener información rica y compleja que solo se puede capturar a través de preguntas abiertas y dialogadas. En investigaciones cualitativas, el objetivo no es solo obtener datos superficiales, sino entender las experiencias, percepciones y enfoques de los participantes en profundidad. Los participantes serán abogados, fiscales y policías, cada uno podría tener una perspectiva diferente sobre el fraude informático, dependiendo de su experiencia profesional. Después de realizar las entrevistas se procederá a transcribir de forma literal todas las respuestas de los entrevistados, incluyendo pausas, enfatizaciones y cualquier otro elemento que ayude a comprender el contexto y así proceder analizar dichas respuestas. Y al final se podrá extraer los resultados, recomendaciones y conclusiones que serán útiles para mejorar la identificación de sujetos en fraudes informáticos.

La información obtenida fue procesada con la realización del análisis descriptivo, siguiendo con la ejecución de la encuesta y finalizando con el análisis de la información para esclarecer los datos de la investigación.

2.6 Aspectos éticos en investigación

El estudio estuvo enmarcado conforme a las normas establecidas en el campo de la investigación y en el principio de originalidad; además, resaltando que se utilizó un cuestionario y observación, por ser un estudio social, además del consentimiento informado de los profesionales, el cual garantiza la autorización de estos, asegurando la confidencialidad de la información proporcionada.

Para finalizar, la presente investigación fue realizada con plena observancia del informe de tesis proporcionado por la Universidad, por lo que se ha cumplido con todos los lineamientos.

III. RESULTADOS

A continuación, presentamos los resultados que fueron obtenidos a través de la aplicación de la guía de entrevista:

Objetivo General: Establecer los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024.

Tabla 1

Pregunta 01 Para usted, ¿Cuáles son los actos de investigación eficaces para la identificación del sujeto que comete fraude informático en Lima Centro 2024?
Entrevistado 01
Como acto de investigación que conlleve a identificar e individualizar al presunto responsable en las actividades ilícitas como el fraude informático, son: 1. Recabar la declaración de la parte agraviada a fin de que brinde más información respecto a los hechos denunciados por la presunta comisión de fraude informático. 2. Oficiar al Organismo supervisor de inversión privada en telecomunicaciones OSIPTEL de la ciudad de Lima para que brinde información sobre el número incriminado.3. Solicitar a la agraviada autorizar el levantamiento del secreto bancario para tener conocimiento de las transferencias bancarias realizas desde el número de cuenta de la agraviada a otras cuentas bancarias, los titulares de estas, los montos dinerarios, fecha y hora, así como la agencia que se haya hecho efectivo el pago no autorizado por la agraviada.4. Solicitar al banco que se ha efectuado las transacciones el movimiento de la cuenta del titular. 5. Solicitar al banco y a la agraviada el procedimiento administrativo de reclamo efectuado y la situación del mismo por transferencias no autorizadas por su titular.6. Recabar los antecedentes de los presuntos responsables consultando: denuncias policiales, sistema integrado de gestión fiscal, así como antecedentes penales de los presuntos responsables.
Entrevistado 02
En Lima Centro, la combinación de levantamiento del secreto de las comunicaciones, levantamiento del secreto bancario, pericias informáticas, geolocalización, y monitoreo de tráfico de internet conforma un conjunto de actos

de investigación que permiten identificar y procesar a los responsables de fraude informático de manera eficaz y legal. La colaboración con las empresas tecnológicas y bancarias es también un factor clave en la detección temprana y la prevención de estos delitos.
Entrevistado 03
Para la identificación del sujeto que comete fraude informático en Lima Centro en 2024, los actos de investigación más eficaces deben adaptarse a la evolución de la tecnología y a las técnicas que utilizan los delincuentes. Estos actos de investigación abarcan un conjunto de herramientas tanto tradicionales como avanzadas, que permiten rastrear y obtener pruebas clave en los casos de fraude informático.
Entrevistado 04
El uso de análisis forense digital, levantamiento del secreto bancario, geolocalización, interceptación de comunicaciones, y la colaboración con proveedores tecnológicos son actos fundamentales para rastrear el origen del fraude y, en última instancia, identificar al sujeto responsable. La integración de testimonios de las víctimas también sigue siendo una herramienta clave.
Entrevistado 05
Considero que es clave aplicar actos de investigación eficaces que combinen técnicas forenses digitales con métodos tradicionales de inteligencia.
Entrevistado 06
Recibir la denuncia y consignar los datos detallados como hora, lugar, nombres, dirección, teléfonos, correos electrónicos y cuentas bancarias. Así como recabar los indicios como Boucher, comprobantes de depósito y/o pago y declaraciones.
Entrevistado 07
Requerir información a las entidades bancarias y comercios, para que puedan orientar el esfuerzo de búsqueda a fin de identificar a los autores.
Entrevistado 08
Mantener una fluidez con las entidades telefónicas, bancos y canales y/o redes sociales. Para la persecución de cuentas, titularidad de números y titulares de cuentas bancarias.
Entrevistado 09

Los actos de investigación son diversos pero fundamental es el manejo de la evidencia digital para el trato adecuado de la información, y con ello poder tener investigaciones sobre delitos informáticos.
Entrevistado 10
La información de informantes y comprobantes respecto de personas que cometen delitos informáticos. Declaración de titulares de las cuentas receptoras.

Interpretación: De acuerdo con los resultados obtenidos, podemos señalar que la mayoría de los entrevistados manifiesta que los mecanismos más eficaces para la identificación del sujeto que comete fraude informático son el levantamiento del secreto de las comunicaciones, la solicitud de información, las pericias y el levantamiento del secreto bancario, puesto que estos solo pueden ser solicitados por el fiscal y ordenado por el juez. Dichos actos tienen el objetivo de esclarecer los hechos e identificar al sujeto.

Tabla 2

Pregunta 02 Para usted, ¿Cuál es el principal reto que afronta usted como autoridad para identificar al responsable del fraude informático en Lima Centro?
Entrevistado 01
El principal reto que se afronta para identificar e individualizar al ciberdelincuente quien suele ser una persona con cierto nivel de inteligencia y educación, como programadores, analistas de sistemas, analistas de comunicaciones, supervisores, personal técnico y de mantenimiento, entre otros; y para identificar al responsable en el delito de fraude informático el principal reto es el desarrollo de la tecnología que no solo ha traído consigo grandes ventajas, sino también nuevas formas y modalidades delictivas que están en aumento y convierten en un desafío para el ordenamiento jurídico que genera cambios en el derecho penal, trasladando la espacio cibernético y los autores poseen conocimientos especializados en informática, mientras que los operadores de justicia (policía, fiscalía, jueces) quienes carecen de formación en ésta área.
Entrevistado 02

El principal reto que enfrentan las autoridades para identificar al responsable del fraude informático en Lima Centro, así como en otras zonas urbanas, es la complejidad y el anonimato que ofrecen las tecnologías digitales.
Entrevistado 03
El principal reto que enfrenta como autoridad para identificar al responsable del fraude informático en Lima Centro es, sin duda, la complejidad y anonimato de las tecnologías involucradas. Los fraudes informáticos suelen emplear métodos sofisticados que hacen difícil rastrear a los delincuentes y obtener pruebas claras.
Entrevistado 04
El principal reto que enfrenta la autoridad para identificar al responsable del fraude informático en Lima Centro es la complejidad y la naturaleza transnacional de los delitos informáticos. Este tipo de fraude, a menudo, se lleva a cabo utilizando tecnologías avanzadas, que permiten a los delincuentes operar desde cualquier parte del mundo, lo que complica su identificación y captura.
Entrevistado 05
La falta de colaboración de empresas tecnológicas, limitaciones en la legislación y procesos judiciales y la falta de recursos tecnológicos.
Entrevistado 06
La demora de la solicitud de respuesta al pedido de información (banco y empresa de telefonía). Las evidencias digitales mientras más se demora, las evidencias son eliminadas.
Entrevistado 07
Los requerimientos de información, ya que muchas veces las entidades bancarias y comercios no brindan la información solicitada, así como la falta de comunicación con sus partes internaciones.
Entrevistado 08
Agotar los medios protocolares que suelen ser muy lentos por temas burocráticos que restringen el acceso.
Entrevistado 09
Es la poca información y el poco acceso a la información puesto que la normativa vigente protege datos importantes para la identificación de puntos de conexión de donde se efectuaron los actos ilícitos.

Entrevistado 10
La falta de acceso y manejo de información para la obtención de la información de los autores de los delitos de fraude informático.

Interpretación: Los entrevistados señalan que la falta de acceso, demoras en el proceso y normativa vigente son los principales retos que afrontan como autoridades, dado que dentro de este tipo de delito es indispensable que la ejecución de los métodos de identificación tenga convicción.

Objetivo Específico 01: Determinar si la escucha telefónica es un acto de investigación eficaz para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024.

Tabla 3

Pregunta 03 ¿Cree usted que la escucha telefónica es una herramienta adecuada y eficaz para identificar a los autores de fraude informático en Lima Centro?
Entrevistado 01
Es un acto de investigación la escucha telefónica proporcionada por la entidad bancaria y/o parte agraviada. Sin embargo, ello no significa que sea un acto de investigación eficaz para identificar al sujeto del delito de fraude informática, se escucha la voz sea femenina o masculina, pero poder relacionar esa voz con una persona atribuible a la llamada sea el investigado o testigo.
Entrevistado 02
La escucha telefónica puede ser útil en la identificación de los autores de fraude informático en Lima Centro, siempre que se cumpla con los requisitos legales y se utilice en combinación con otras herramientas de investigación. Es especialmente eficaz cuando los delincuentes están utilizando las comunicaciones telefónicas para coordinar actividades fraudulentas o para discutir detalles operativos del fraude.
Entrevistado 03
La escucha telefónica puede ser una herramienta útil en la identificación de los autores de fraude informático en Lima Centro, pero su adecuación y eficacia dependen de diversos factores que deben ser considerados con cautela.

Entrevistado 04
La escucha telefónica puede ser una herramienta útil para identificar a los autores de fraude informático, especialmente cuando los delincuentes comunican directamente con las víctimas o coordinan acciones fraudulentas por teléfono. No obstante, la eficacia de esta herramienta está limitada en casos donde los delincuentes utilizan otros medios de comunicación, como correo electrónico, mensajería encriptada, o plataformas de pago online para llevar a cabo sus actividades delictivas.
Entrevistado 05
Considero que si es una herramienta útil, pero su eficacia depende de varios factores como el requerimiento judicial y uso de mensajería cifrada.
Entrevistado 06
La escucha telefónica es una herramienta adecuada que nos va a brindar información de sindicaciones y/o coordinaciones que se realizan para cometer el fraude informático. Cabe mencionar que en este tipo de delito se utiliza las transferencias bancarias. Lo que se necesita es conocer los titulares de las direcciones IP.
Entrevistado 07
Sería importante siempre y cuando se realicen a fin de desarticular una organización criminal dedicada al fraude informático, debido a que es una herramienta especial de investigación.
Entrevistado 08
No, la ciberdelincuencia se ha actualizado y se usa inteligencia artificial, además de ello no hay logística que sea adecuada.
Entrevistado 09
La escucha telefónica no ayuda a la identificación neta de los actores puesto que ahora con la ayuda de la inteligencia artificial IA, los delincuentes pueden suplantar voces.
Entrevistado 10
Si, siendo una herramienta de utilidad para la identificación de los autores de los delitos de fraude informático.

Interpretación: Para esta pregunta, dentro de los entrevistados se observaron apreciaciones distintas puesto que, algunos consideran que la escucha telefónica es una herramienta eficaz

porque su intervención ayuda a determinar la responsabilidad de los sujetos en este delito, no obstante, otra parte de los entrevistados no está de acuerdo en su eficacia, pues consideran que con el avance de la tecnología estas puedan ser distorsionadas, para ello sería esencial el uso de las pericias.

Tabla 4

Pregunta 04 En cuanto a la privacidad de los usuarios, ¿cómo se determina la eficacia de la escucha telefónica en la investigación del delito de fraude informático?
Entrevistado 01
La eficacia de la escucha telefónica en la investigación del delito de fraude informático es de suma importancia, se establece a través de una prueba pericial de reconocimiento de voz que es clave para identificar a los responsables de un delito o demostrar la inocencia de un investigado, considerada válida en la investigación.
Entrevistado 02
La eficacia de la escucha telefónica en la investigación de delitos como el fraude informático debe ser evaluada cuidadosamente, especialmente cuando se toma en cuenta la privacidad de los usuarios. En este contexto, la eficacia de la escucha telefónica no solo depende de su capacidad para identificar a los responsables, sino también de si se lleva a cabo respetando los principios legales de privacidad y la protección de derechos fundamentales.
Entrevistado 03
La eficacia de la escucha telefónica en estos casos debe analizarse desde diversas perspectivas, que incluyen su legalidad, proporcionalidad, necesidad y respeto a los derechos fundamentales. A continuación, exploro cómo se determina la eficacia de esta herramienta en el contexto del fraude informático, considerando también la privacidad de los usuarios.
Entrevistado 04
La eficacia de la escucha telefónica en la investigación de fraude informático, en cuanto a la privacidad de los usuarios, se determina por una evaluación conjunta de

necesidad, proporcionalidad, autorización judicial, minimización de la invasión a la privacidad, y el manejo adecuado de la información recopilada.
Entrevistado 05
Considero que se determina por diferentes criterios como la calidad de la información, la identificación, ubicación, entre otros al, al respecto quiero indicar que los delincuentes usan mensajería cifradas.
Entrevistado 06
En la actualidad, en estos delitos de fraude informático se utiliza el WhatsApp como medio de comunicación para la coordinación y las transferencias bancarias son por internet. La escucha telefónica sería como indicios.
Entrevistado 07
Con la finalidad de obtener información relevante en cuanto a la organización y funciones de la organización criminal dedicada al fraude informático.
Entrevistado 08
Por medios y técnicas forenses digitales.
Entrevistado 09
Como lo indiqué en el punto anterior, la escucha no apoya a la identificación de los autores de delitos informáticos,
Entrevistado 10
A la fecha, no tengo conocimiento del uso de la escucha telefónica en casos de fraude informático.

Interpretación: Conforme a la información recabada, la eficacia de la escucha telefónica se determina a través de una prueba pericial, donde es de suma importancia que se respeten los principios legales de privacidad y la protección de derechos fundamentales.

Objetivo Específico 02. Identificar como el levantamiento secreto de las comunicaciones es un acto de investigación eficaz para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024.

Tabla 5

Pregunta 05
¿Qué mejoras usted considera necesarias en la legislación sobre interceptación de comunicaciones para enfrentar eficazmente el fraude informático en los próximos

años?
Entrevistado 01
Se necesita fomentar una cultura digital que promueva el uso correcto y responsable de internet en toda la sociedad, la instrucción sobre los delitos informáticos no debe limitarse exclusivamente a las fiscalías especializadas, sino que debe extenderse a todas las fiscalías, las comisarías, los juzgados y las demás instancias, ya que estos delitos pueden ocurrir en cualquier parte de nuestro país. Por ello, es esencial proporcionar formación a la población y realizar campañas de divulgación y prevención mediante charlas en escuelas, asociaciones, medios de comunicación, entre otros.
Entrevistado 02
Para enfrentar eficazmente el fraude informático en los próximos años, es fundamental que la legislación sobre interceptación de comunicaciones evolucione y se adapte a los avances tecnológicos, la globalización del cibercrimen y las nuevas metodologías utilizadas por los delincuentes. La normativa actual en muchos países, incluyendo Perú, tiene un marco legal robusto pero, en algunos casos, necesita actualizarse y mejorarse.
Entrevistado 03
Para enfrentar eficazmente el fraude informático en los próximos años, es fundamental que la legislación sobre la interceptación de comunicaciones evolucione y se adapte a los avances tecnológicos y a las nuevas tácticas utilizadas por los delincuentes cibernéticos.
Entrevistado 04
Para enfrentar eficazmente el fraude informático en los próximos años, las mejoras en la legislación sobre interceptación de comunicaciones deben abordar los avances tecnológicos, los nuevos métodos de fraude y las garantías para proteger los derechos fundamentales de los individuos.
Entrevistado 05
Permitir la intercepción de comunicaciones digitales en plataformas digitales (redes sociales, mensajerías) bajo suspensión judicial.
Entrevistado 06

Revisar el levantamiento del secreto de las comunicaciones u el levantamiento del secreto bancario. Para este tipo de delito de fraude informático, el investigador para una investigación eficaz solo requiere conocer la titularidad del teléfono, IP y cuenta bancaria.
Entrevistado 07
Considero que las técnicas especiales de investigación están detalladas y deben ser utilizadas para las investigaciones de organizaciones criminales en fraude informático.
Entrevistado 08
Determinar las nuevas leyes en conjunto a esta nueva problemática donde el estado o entidades privada puedan actualizar al personal.
Entrevistado 09
Modificar la ley de protección de datos e implementar normas de acceso a la información.
Entrevistado 10
Que estas medidas deben ser parte de la Dirección de investigación y no solo de otro grupo como la DIRANDRO.

Interpretación: De los resultados obtenidos por esta pregunta, la mayoría de los entrevistados concuerdan en la necesidad de promover el uso correcto del internet. Así como realizar mejoras dentro de la normativa, donde el proceso no se vea alargado ni interrumpido por la falta de desconocimiento de las autoridades.

Tabla 6

Pregunta 06 ¿Cómo considera usted que ha influido el uso del levantamiento secreto de las comunicaciones en las investigaciones de los casos de fraude informático?
Entrevistado 01
El levantamiento del secreto de las comunicaciones en los casos de fraude informático resulta importante debido a que permite alcanzar la verdad y sancionar a los responsables. De lo contrario, solo estaremos ante esfuerzos parciales que no

solucionarán los problemas producidos por la interceptación de las comunicaciones que han erosionado la institucionalidad democrática en nuestro país.
Entrevistado 02
El levantamiento del secreto de las comunicaciones es una herramienta clave en las investigaciones de fraude informático, ya que permite a las autoridades acceder a las comunicaciones privadas de los sospechosos con el objetivo de obtener pruebas que ayuden a esclarecer el delito. Esta medida, aunque efectiva, tiene implicaciones tanto positivas como negativas que deben ser evaluadas cuidadosamente.
Entrevistado 03
El uso del levantamiento del secreto de las comunicaciones ha sido un elemento crucial en la lucha contra el fraude informático, ya que ha facilitado la obtención de pruebas directas, la desarticulación de redes criminales y el seguimiento de flujos ilegales. Sin embargo, este recurso debe utilizarse de manera estrictamente controlada y proporcionada, garantizando siempre que se respete la privacidad y los derechos fundamentales de los ciudadanos.
Entrevistado 04
El levantamiento del secreto de las comunicaciones ha tenido una influencia significativa en las investigaciones de los casos de fraude informático, ya que permite a las autoridades acceder a información clave para la identificación y desmantelamiento de redes delictivas. Sin embargo, su uso también plantea desafíos relacionados con la privacidad y el abuso de poder.
Entrevistado 05
Si, pero con limitaciones.
Entrevistado 06
El levantamiento secreto de las comunicaciones es fundamental siempre y cuando se brinde de forma rápida y oportuna.
Entrevistado 07
Ha influido en la identidad de titular del proveedor del servicio de internet y a partir de ahí se ha podido identificar a los autores del delito de fraude informático.
Entrevistado 08
De modo considerable para el esclarecimiento de varios casos donde “L.Q.R.R.” se escuchaban bajo la fachada de la privacidad.

Entrevistado 09
Muchísimo, puesto que brinda el punto exacto en donde se efectuaron los hechos ilícitos.
Entrevistado 10
Que a la fecha no se ha promovido mucho esta medida, pero sería una herramienta importante.

Interpretación: En relación con esta pregunta, los entrevistados están en la misma línea al mencionar que el levantamiento del secreto de las comunicaciones en los casos de fraude informático influye, igual este es considerado como una herramienta clave para la identificación del sujeto, puesto que permite a las autoridades acceder a las comunicaciones privadas de los posibles culpables, teniendo como objetivo recaba pruebas para esclarecer el delito.

Objetivo Específico 03. Analizar las deficiencias que afronta el Ministerio Público para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024.

Tabla 7

Pregunta 07
¿Cuál considera usted que son las deficiencias que afronta el Ministerio Público para la identificación del sujeto activo en el delito de fraude informático en Lima Centro 2024?
Entrevistado 01
Las deficiencias que afronta el Ministerio Público para la identificación del sujeto activo en el delito de fraude informático en el Lima, siendo que, en la actualidad no se asignen valores a los nuevos bienes jurídicos y se necesitan que promulguen leyes que los protejan, para así abordar los vacíos legales presentes en nuestra normativa. Estas son cuestiones de urgencia que deben captar la atención de los legisladores; de lo contrario, persistirá un considerable grado de impunidad. Así, también se necesita fomentar una cultura digital que promueva el uso correcto y responsable de internet en toda la sociedad, la instrucción sobre los delitos informáticos no debe limitarse exclusivamente a las fiscalías especializadas, sino

que debe extenderse a todas las fiscalías, las comisarías, los juzgados y las demás instancias, ya que estos delitos pueden ocurrir en cualquier parte de nuestro país. Por ello, es esencial proporcionar formación a la población y realizar campañas de divulgación y prevención mediante charlas en escuelas, asociaciones, medios de comunicación, entre otros, a fin de que no exista impunidad y sancionar a los responsables del ilícito penal de fraude informático.
Entrevistado 02
El Ministerio Público enfrenta una serie de deficiencias y obstáculos en la identificación de los sujetos activos en los delitos de fraude informático en Lima Centro. Estos problemas están relacionados tanto con limitaciones tecnológicas como con carencias estructurales y operativas dentro de las instituciones encargadas de la persecución del crimen cibernético.
Entrevistado 03
El Ministerio Público enfrenta una serie de desafíos para identificar a los responsables de fraude informático en Lima Centro, que van desde la falta de capacitación especializada, la insuficiencia de herramientas tecnológicas y la colaboración internacional limitada, hasta las deficiencias en la recolección de pruebas digitales y el uso de técnicas de anonimato por parte de los delincuentes.
Entrevistado 04
El Ministerio Público en Lima Centro enfrenta varias deficiencias al intentar identificar al sujeto activo en los delitos de fraude informático en 2024. Estas deficiencias son consecuencia de diversos factores, como el avance tecnológico, la complejidad de los delitos informáticos y las limitaciones estructurales del sistema judicial y de investigación.
Entrevistado 05
La falta de acceso rápido a la información digital y uso de técnicas avanzadas.
Entrevistado 06
Tanto el Ministerio Público y la Policía, afrontan el retraso de la entrega de información con el pedido del levantamiento del secreto de las comunicaciones y el secreto bancario.
Entrevistado 07

Los mecanismos informáticos que enmascaran la identificación IP, la asignación masiva de IP para los usuarios.
Entrevistado 08
El determinar los tipos de delitos por fraude informático; Phishing, pharming, salto de rana, pago de servicios – Smishing , vishing, suim sopienng y otros que comprendan.
Entrevistado 09
No podría precisar esa pregunta porque no labora en esa Institución.
Entrevistado 10
El conocimiento que tienen sobre los actos eficaces de investigación.

Interpretación: Para esta pregunta, los entrevistados no solo mencionan las deficiencias sino también las limitaciones entorno al fraude informáticos, pues están de acuerdo en la promulgación de nuevas leyes. Tanto los fiscales como jueces han afrontado dentro del proceso obstáculos para la identificación de los sujetos en el delito de fraude informático, señalando que la falta de capacitación solo refleja la cantidad de casos impunes.

Tabla 8

Pregunta 08 ¿Qué recomendaciones daría a las víctimas de fraude informático para protegerse y colaborar con las autoridades durante la investigación?
Entrevistado 01
Que, si detecta una víctima movimientos sospechosos en sus tarjetas debe comunicase con su banco, bloquear la tarjeta de débito o crédito, acudir a cualquier comisaria del Perú o directamente con la División de Investigación de Delitos de Alta Tecnología (Av. España 323-Cercado de Lima). Asimismo, deben conservar todas las evidencias, no eliminar los mensajes ni correos electrónicos, ya que esto facilitará el rastreo de los ciberdelincuentes.
Entrevistado 02
Las víctimas de fraude informático deben actuar rápidamente para proteger su información, denunciar el fraude y colaborar con las autoridades. Cuanto más

rápido se actúe y mejor se gestione la evidencia, mayor será la probabilidad de identificar a los responsables y recuperar los fondos. Además, la prevención futura a través de la educación y las medidas de seguridad puede ayudar a reducir el riesgo de caer nuevamente en fraudes digitales.
Entrevistado 03
Las víctimas deben ser proactivas en la adopción de medidas de seguridad para proteger sus datos y, en caso de ser víctimas de fraude, deben actuar rápidamente y cooperar de manera efectiva con las autoridades para asegurar que el delito sea procesado adecuadamente.
Entrevistado 04
Aunque las víctimas deben protegerse y colaborar activamente con las autoridades, también deben adoptar una mentalidad preventiva. La educación continua y el fortalecimiento de las medidas de seguridad pueden ayudar a reducir la probabilidad de ser víctimas de fraude informático en el futuro.
Entrevistado 05
Que interpongan la denuncia en la brevedad posible para preservar las evidencias en la brevedad.
Entrevistado 06
No brindar ninguna información personal (DNI, teléfono, claves y cuentas bancarias). Así somo verificar los enlaces de conexión antes de brindar información y/o realizar transferencias bancarias por internet.
Entrevistado 07
No brindar contraseñas, ni datos de cuentas bancarias en enlaces de dudosa procedencia. Contar con un antivirus actualizada y original.
Entrevistado 08
Compartir sus malas experiencias , mantener informados y actualizados , cumplir con los mecanismos de seguridad.
Entrevistado 09
Que se informen por redes sobre los delitos de fraude informático. Eviten de tener información relevante en sus móviles. No brindar información a desconocidos y no compartir información en redes sociales.
Entrevistado 10

Que denuncien si son víctimas del fraude informático y que aseguren sus datos y sistemas informáticos para evitar el ilícito.

Interpretación: Dentro de las recomendaciones que brindan los especialistas, refieren la importancia de mantenerse informados y actualizados en referencia a los mecanismos de seguridad. También, denotan la importancia de cuidar las informaciones y no compartirla a través de medios electrónicos donde el alcance es mucho mayor.

Tabla 9

Pregunta 09 ¿Qué otros actos de investigación consideran usted útil para la identificación del sujeto activo en el delito de fraude informático en Lima Centro 2024?
Entrevistado 01
Los investigadores (policía especializada) utilizan herramientas y programas especiales para recopilar, guardar y estudiar pruebas digitales cuando investigan delitos cibernéticos. Estas herramientas ayudan a identificar a las personas malintencionadas, rastrear lo que hicieron y reunir pruebas para construir un caso en su contra como son: Software de análisis forense digital, Herramientas de monitoreo de red, Herramientas de análisis de malware, Herramientas para descifrar contraseñas, Herramientas de seguimiento de redes sociales.
Entrevistado 02
Además de los actos de investigación tradicionales como el levantamiento del secreto de las comunicaciones, el secreto bancario y la geolocalización, existen diversas herramientas y estrategias investigativas adicionales que pueden ser útiles en la identificación de los responsables del fraude informático en Lima Centro. La combinación de análisis digital, colaboración con proveedores de servicios, intervención de redes sociales y cooperación internacional contribuye a construir un caso sólido que permita identificar al sujeto activo, desarticular las redes de fraude y asegurar la recuperación de fondos y la justicia para las víctimas.
Entrevistado 03
Para identificar al sujeto activo en casos de fraude informático en Lima Centro, las autoridades deben contar con una combinación de herramientas y actos de

investigación. Estos incluyen desde el análisis de registros electrónicos, seguimiento de transacciones financieras, hasta la colaboración internacional y la investigación en redes sociales y plataformas de pago.
Entrevistado 04
Para la identificación del sujeto activo en casos de fraude informático en Lima Centro en 2024, una estrategia integral que combine múltiples fuentes de información es esencial. A través de la cooperación entre las autoridades, el uso de tecnologías de rastreo avanzadas y el análisis de diversas fuentes como metadatos, redes sociales y plataformas en línea, se puede desmantelar una red de fraude informático.
Entrevistado 05
Que exista un software para la identificación de personas donde se visualice el delincuente, efectuando el hecho delictivo.
Entrevistado 06
Realizar y reglamentar el alcance del secreto de las comunicaciones y secreto bancario, a fin de tener información oportuna. Como conocer la titularidad de los teléfonos, IP, cuentas bancarias y no tener que solicitar las medidas limitativas de Derecho.
Entrevistado 07
Levantamiento del secreto de las comunicaciones y el levantamiento del secreto bancario.
Entrevistado 08
El Renteseg y la geolocalización.
Entrevistado 09
Las vigilancias o patrullaje virtual, la persecución de información, visualizaciones y el análisis de datos por zona criminal.
Entrevistado 10
Dentro de los más importantes y efectivos es el manejo de información y geolocalización.

Interpretación: En el transcurso de la recolección de datos, los entrevistados señalan como acto de investigación útil a la geolocalización, puesto este acto transforma y protege la

información, su capacidad de rastreo en tiempo real facilita la identificación del sujeto, Otro mecanismo que podría ser implementado es un software que permita identificar al delincuente efectuando el hecho delictivo.

IV. DISCUSIÓN

En esta sección, procederemos a analizar y explicar los resultados obtenidos.

En ese sentido, encontraremos como resultados, interpretaciones, hallazgos, análisis y comparaciones con otros estudios.

Considerando el objetivo general, el cual consiste en establecer los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro. Cada persona que interviene dentro de un sistema jurídico ya sea como ciudadano, intérprete, especialista o magistrado, cumple un rol para la aplicación de las normas jurídicas, la finalidad de esto es controlar el cumplimiento de cada una de las normas que competen y específicamente están relacionadas a la identificación de los sujetos que cometen fraude informático.

Haciendo una comparación con otros antecedentes, el autor Molinos (2020) , nos dice que el delito de fraude informático suele ser cometido por personas que tienen habilidades o ciertas características de las que puede tener un delincuente común. Por otro lado Paguay (2020) , señala que el sujeto no necesariamente debe tener un alto conocimiento en informática

Los delitos informáticos y los vacíos legales que generan afectaciones a los ciudadanos dan a conocer la realidad de la ineficacia de la aplicación de los actos de investigación que identifican a los sujetos que cometen fraude informático. Las consecuencias de estos vacíos jurídicos solo denotan el problema en la falta de profundidad de las normas. Dentro de los resultados recogidos, producto de la aplicación de la guía de entrevista, evidencian que los actos de investigación eficaces para la identificación del sujeto que comete fraude informático son el levantamiento del secreto de las comunicaciones, las pericias y el levantamiento del secreto bancario.

Para identificar y perseguir a los responsables de fraude informático se tiene que enfrentar a varios desafíos obtenidos de vacíos legales, la falta de medios económicos. La identificación y persecución de los responsables del fraude informático se enfrenta a una serie de desafíos derivados de los vacíos legales, la falta de recursos y la resistencia de los actores privados. Sin embargo, los actos de investigación como el levantamiento del secreto de las comunicaciones, las pericias informáticas, la solicitud de información y el

levantamiento del secreto bancario siguen siendo herramientas cruciales en la lucha contra este tipo de delitos. Para mejorar la efectividad de estos actos, es fundamental que se refuercen las leyes, se mejore la cooperación entre los sectores público y privado, y se capacite adecuadamente a los operadores judiciales. Solo a través de un enfoque integral se podrá avanzar en la lucha contra el fraude informático y proteger adecuadamente a los ciudadanos.

Prosiguiendo con los objetivos específicos, se tendrá en cuenta el primero que es determinar si la escucha telefónica es un acto de investigación eficaz para la identificación del sujeto en el delito de fraude informático, los especialistas establecen que esta es esencial pero que no se sigue en todos los procesos por la falta de conocimiento de este acto, generando así inconsistencias. La falta de capacidad resalta la poca eficiencia del tratamiento fiscal.

Vitteri (2022), concluye en que el avance tecnológico también da paso a la delincuencia, por esta razón, el medio en la investigación precedente es defectuoso y en el juicio no hay como comprobarlo. De otra manera, refiere que este acto de investigación al cumplir la función de monitorear una conversación telefónica podría vulnerar el derecho a las comunicaciones personales, pues es importante señalar que estos son lícitos mientras se busque garantizar la seguridad y luche en contra de los delitos, no obstante, esta debe ser realizada siempre bajo los lineamientos que impone la ley.

En continuación de los objetivos específicos, identificar como el levantamiento secreto de las comunicaciones es un acto de investigación eficaz para la identificación del sujeto en el delito de fraude informático en Lima Centro. Como bien ya sabemos, los delitos informáticos generan perjuicio en el patrimonio y con el incremento a razón de la pandemia, es que sucede mucho que las entidades financieras no contribuyen con el ejercicio de este acto de investigación, incluso el plazo fijado por la norma resulta inviable por la misma carga procesal, tratándose de información confidencial, la cual no es fácil su obtención.

El levantamiento secreto de las comunicaciones es un acto de investigación indispensable en el contexto del fraude informático, pero a su vez, enfrenta serias barreras que limitan su efectividad. La falta de cooperación de las entidades financieras, los plazos procesales inviable, las dificultades técnicas para garantizar la autenticidad de las pruebas, y la carencia de herramientas especializadas son factores que afectan su eficiencia. Para

superar estos desafíos, es necesario mejorar la colaboración público-privada, adaptar la normativa a las nuevas realidades tecnológicas y dotar a las autoridades de los recursos y capacitación necesarios.

Si bien el levantamiento secreto de las comunicaciones sigue siendo un elemento clave en la identificación de los sujetos responsables de fraudes informáticos, su efectividad depende de la capacidad del sistema judicial y de las fuerzas del orden para adaptarse a los rápidos cambios en el panorama digital. Por otro lado Valdivia (2023) , señala que este acto de investigación es indispensable pues permite identificar a los sujetos que conforman la organización, permitiendo obtener pruebas que van a lograr identificarlos .

Sobre el objetivo específico que busca analizar las deficiencias que afronta el Ministerio Público para la identificación del sujeto en el delito de fraude informático son múltiples y complejas. La falta de capacitación especializada, la insuficiencia de recursos tecnológicos, la falta de coordinación interinstitucional y la resistencia del sector privado son algunos de los factores que limitan la eficacia de las investigaciones. Para superar estos obstáculos, es fundamental que se refuercen los protocolos de colaboración, se invierta en la capacitación continua de los fiscales y se mejoren los recursos tecnológicos disponibles. Asimismo, es necesario revisar los plazos procesales y promover una mayor colaboración público-privada, de manera que se logre una respuesta más efectiva frente al fraude informático.

Por otro lado, en Lima, Matos (2022), finalizó en que la normativa es mala para la ciberdelincuencia, pues no se capacita al personal, ni se profundiza con expertos de la materia. El estado no se abastece; esta investigación es parecida en el punto de la profundización con expertos de la materia. La Institución responsable también es la División de Investigaciones de Delitos de Alta Tecnología (DIVINDAT) de la DIRINCRI – PNP, no obstante, esta no tiene las capacidades ni herramientas para su actuación. Además, que, no se tienen fiscales especializados en este tipo de delito, por lo que muchos casos quedan con los vacíos legales propios y posteriores archivamientos.

V. CONCLUSIONES

PRIMERO. - Sobre el objetivo general, que busca establecer los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro, podemos concluir que son los siguientes: El levantamiento del secreto de las comunicaciones, el levantamiento del secreto bancario, las pericias y la solicitud de información, estos actos de investigación son eficaces porque facilitan acceder a información muy importante, que ayudaría para encontrar a los culpables que cometen este delito. Sin embargo, estos resultan ser insuficientes cuando diversos factores como el anonimato del sujeto, la falta de capacitación especializada y las pocas herramientas tecnológicas afectan a la investigación. Además, otros actos de investigación serían las pruebas directas y al uso de herramientas como VPNs (red privada virtual) e implementar un software que permita identificar al delincuente efectuando el hecho delictivo.

SEGUNDO. - Respecto al primer objetivo específico que es, determinar si la escucha telefónica es un acto de investigación eficaz para la identificación del sujeto en el delito de fraude informático en Lima Centro, concluimos en que este acto de investigación es una herramienta importante y eficaz para identificar a los sujetos implicados en el fraude informático, ya que permite captar comunicaciones clave que pueden proporcionar información directa sobre los métodos y actores involucrados. Sin embargo, su implementación debe estar alineada con las normativas legales y garantizar el respeto a los derechos fundamentales de las personas. No obstante, también puede denotar una dificultad cuando el autor de los hechos se encuentre en el anonimato o distorsione las comunicaciones.

TERCERO. - En el segundo objetivo específico, para identificar como el levantamiento secreto de las comunicaciones es un acto de investigación eficaz para la identificación del sujeto en el delito de fraude informático en Lima Centro, concluimos en que el levantamiento secreto de las comunicaciones es un acto de investigación eficaz, pues facilita el acceso a conversaciones electrónicas privadas que, de otro modo, serían inaccesibles. Este acto debe ser cuidadosamente regulado y supervisado para evitar abusos y garantizar su legalidad, ya que las evidencias obtenidas de esta manera son cruciales para demostrar la implicancia del sujeto en el delito.

CUARTO. - Para finalizar con respecto al tercer objetivo específico, que busca analizar las deficiencias que afronta el Ministerio Público para la identificación del sujeto en el delito de fraude informático en Lima Centro, señalamos que esta Institución enfrenta varias deficiencias en la identificación de los sujetos responsables de fraude informático. Estas incluyen la falta de recursos tecnológicos adecuados, la capacitación insuficiente de los fiscales en el manejo de evidencia digital y las deficiencias en la coordinación entre las instituciones encargadas de la investigación. Además, la rápida evolución de la tecnología y las técnicas utilizadas por los delincuentes dificulta el proceso de identificación efectiva. Por otro lado, la labor que cumple la División de Investigación de Delitos de Alta Tecnología – DIVINDAT constituye parte esencial e importante para la lucha contra el delito de fraude informático.

VI. RECOMENDACIONES

PRIMERO. - Se recomienda implementar programas de capacitación continua para los fiscales y otros operadores de justicia en técnicas de investigación digital y el manejo adecuado de evidencias electrónicas. Esto les permitirá estar mejor preparados para enfrentar los desafíos del fraude informático. Es crucial que el Ministerio Público invierta en tecnologías avanzadas y en el desarrollo de herramientas especializadas para la investigación de delitos informáticos. Estas tecnologías podrían incluir software de análisis forense digital, herramientas de monitoreo y detección de fraudes, y bases de datos especializadas que faciliten la identificación de patrones criminales.

SEGUNDO. - A fin de preservar los derechos fundamentales de los investigados y garantizar la validez de las pruebas, es fundamental que el uso de actos de investigación como la escucha telefónica y el levantamiento secreto de comunicaciones se realice bajo estrictos estándares legales. Se recomienda establecer procedimientos claros y transparentes que garanticen la supervisión judicial y el respeto a las normas constitucionales.

TERCERO. - Se debe mejorar la coordinación entre las diferentes instituciones encargadas de la investigación y persecución del delito de fraude informático, tales como la Policía Nacional, el Ministerio Público y las entidades privadas que prestan servicios de tecnología y telecomunicaciones. Esto permitirá una respuesta más eficiente y un intercambio de información más fluido, lo que puede agilizar el proceso de identificación y captura de los responsables.

CUARTO. - Se recomienda que el Ministerio Público establezca colaboraciones más estrechas con expertos en informática forense, quienes pueden aportar conocimientos técnicos en la identificación y análisis de evidencias digitales que a menudo son esenciales para resolver casos de fraude informático.

VII. REFERENCIAS BIBLIOGRÁFICAS

Álvaro Mendo, E. (2014). Delitos y redes sociales : mecanismos formalizados de lucha y delitos más habituales . El caso de la suplantación de identidad. *Revista General de Derecho Penal*. Recuperado el julio de 2021, de https://d1wqtxts1xzle7.cloudfront.net/60703226/Delitos_y_redes_sociales20190925-118603-1ov5zut.pdf?1569437092=&response-content-disposition=inline%3B+filename%3DDelitos_y_redes_sociales_mecanismos_form.pdf&Expires=1627087964&Signature=asJgS24NJ4d~15ocMWB~

Ávila Trivelli , A. A. (abril de 2023). Análisis del delito de fraude informático. Lima, Perú. Recuperado el febrero de 2025, de https://dialnet.unirioja.es/descarga/articulo/9502860.pdf

Beraún López, C. J. (2021). El delito de estafa por medios tecnológicos en tiempos de la COVID-19, Lima, 2020. Lima, Perú. Recuperado el enero de 2025, de https://repositorio.ucv.edu.pe/handle/20.500.12692/81913

Calderon Fernandez, F. G. (2023). Las fintech y el delito de fraude informático. Lima, Perú. Recuperado el enero de 2025, de https://repositorio.ucv.edu.pe/handle/20.500.12692/141533

Carbajal Camones, M. (2022). Las fiscalías especializadas en delitos informáticos como mecanismo para la lucha contra el cibercrimen. Lima, Perú. Recuperado el enero de 2025, de https://repositorio.usmp.edu.pe/handle/20.500.12727/11398

Castells, M. (2013). *Internet y la sociedad red.* Recuperado el julio de 2021, de http://commons.cc/antropi/wp-content/uploads/2013/02/castells_intro.pdf

Cervera Vargas, L. M. (2020). Criterios de interpretación del sujeto activo en el delito de feminicidio en confrontación con el acuerdo plenario. Chiclayo. doi:https://orcid.org/0000-0003-0120-7444

Custodio Cumpa, Y. (2021). Las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático. Chiclayo, Perú. Recuperado el febrero de 2025, de https://repositorio.ucv.edu.pe/handle/20.500.12692/74797

Granizo Castillo, J. O., & Paguay Calderón, V. L. (26 de abril de 2021). Las nuevas perspectivas regulatorias de delitos informáticos en las compras a través de internet. Ecuador. Recuperado el enero de 2025, de http://dspace.unach.edu.ec/handle/51000/7607

Huaire Inacio, E. J. (2019). *Método de investigación.* Recuperado el febrero de 2025, de https://www.aacademica.org/edson.jorge.huaire.inacio/78.pdf

Huamán Cruz, M. Y. (2025). Los delitos informáticos en Perú y la suscripción del Convenio de Budapest. Cusco, Perú. Recuperado el enero de 2025, de https://repositorio.uandina.edu.pe/item/5d18fb80-74f6-49c2-80d0-0b3aba8efbd8

López Latorre, J. (2006). *Psicología de la delincuencia.* Salamanca, España. Recuperado el junio de 2021, de https://www.rediberoamericanadetrabajoconfamilias.org/psicologiadeladelincuencia.pdf

Malca Leandro, E. C. (2023). Eficacia de la persecución penal en la investigación preparatoria del delito de fraude informático, Callao, 2022. Perú. Recuperado el enero de 2025, de https://repositorio.ucv.edu.pe/handle/20.500.12692/129112

Martinez Mediano, C. (junio de 2014). Técnicas e instrumentos de recogida y análisis de datos. 31-38. Recuperado el febrero de 2025, de https://books.google.es/books?hl=es&lr=&id=iiTHAwAAQBAJ&oi=fnd&pg=PA7&dq=2.3.2.%09Dise%C3%B1o+metodol%C3%B3gico.++El+dise%C3%B1o+aplicado+es+el+no+experimental,+el+cual+se+emplea+cuando+no+es+posible+manipular+variables+o+cuando+se+busca+estudiar+situacio

Mayer Lux, L., & liver Calderón, G. (junio de 2020). El delito de fraude informático: concepto y delimitación. *SciELO*, págs. 156-161. Recuperado el febrero de 2025, de https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000100151

Mejía Barrera, I., & Correa Alcaráz, M. A. (2018). La estafa. Distinción entre el delito de estafa y el ilícito civil : una mirada jurisprudencial a la corte suprema de justicia. Lima, Perú. Obtenido de https://repository.eafit.edu.co/bitstream/handle/10784/12691/Isabel_Mej%C3%ADaBarrera_Mar%C3%ADaAlejandra_CorreaAlcar%C3%A1z_2018.pdf?sequence=2&isAllowed=y

Molinos Cóbreces, A. (2020). El fraude informático y telemático: perspectiva penal. Valladolid, España. Recuperado el enero de 2025, de https://uvadoc.uva.es/handle/10324/46997

Muñoz Conde, F., & García Arán , M. (2004). *Derecho Penal. Parte General* (Vol. 6). Valencia, España: Tirant Lo Blanch.

Nación, M. P. (15 de setiembre de 2020). Convenio sobre la Ciberdelincuencia" permite a jueces y fiscales realizar requerimientos de cooperación internacional. Lima, Perú. Recuperado el febrero de 2025, de https://www.gob.pe/institucion/mpfn/noticias/302628-convenio-sobre-la-ciberdelincuencia-permite-a-jueces-y-fiscales-realizar-requerimientos-de-cooperacion-internacional

Nazario Delgado, N. Y., & Villanueva Sanchez, L. V. (2022). Fraude informático en la modalifaf de Pishing y la necesaria actualización de la legislación para una eficiente persecución y sanción penal. Pimentel, Perú. Recuperado el febrero de 2025, de https://repositorio.uss.edu.pe/handle/20.500.12802/10002

Oxman, N. (diciembre de 2013). Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming". *SciELO*(41). doi:http://dx.doi.org/10.4067/S0718-68512013000200007

Peruano, E. (04 de setiembre de 2022). Denuncias por delitos informáticos se incrementaron en más del 90% en el Perú. *El Peruano*. Obtenido de https://www.elperuano.pe/noticia/188048-denuncias-por-delitos-informaticos-se-incrementaron-en-mas-del-90-en-el-peru

Pueblo, D. d. (mayo de 2023). La ciberdelincuencia en el Perú: Estrategias y retos del Estado. págs. 10-16. Recuperado el febrero de 2025, de https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Puerta Cortés, D. X., & arbonell, X. (2013). Uso problemático de Internet en una muestra de estudiantes universitarios colombianos. *SciELO*. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-47242013000300012

Súarez Sánchez, A. (2008). Estafa informática. España. Obtenido de https://dialnet.unirioja.es/servlet/tesis?codigo=183835

Tejero González, J. M. (2021). *Técnicas de investigación cualitativa en los ámbitos sanitario y sociosanitario.* Recuperado el febrero de 2025, de https://www.torrossa.com/es/resources/an/4943831?digital=true

Tenesaca Gusqui, V. S., & Cedeño Heras, I. A. (2021). Análisis del delito de estafa en redes sociales en medios electrónicos en la Ciudad de Guayaquil a consecuencia de la cuarentena producto de la pandemia del Coronavirus en el año 2020. Guayaquil, Ecuador. Recuperado el enero de 2025, de https://repositorio.ug.edu.ec/items/beb795cf-ce14-4bb3-8cec-21e57b7f44fd

Urdanegui Rangel, A. (diciembre de 2023). Los delitos informáticos y la vulneración del derecho fundamental de protección de datos personales en Lima Metropolitana. Lima, Perú. Recuperado el febrero de 2025, de https://repositorio.autonoma.edu.pe/handle/20.500.13067/2999

Vargas Miñan, W. (2022). Necesidad de tipificar la estafa básica en la ley de delitos informáticos para reducir la impunidad en el Perú. Lima, Perú. Recuperado el enero de 2025, de https://repositorio.ucv.edu.pe/handle/20.500.12692/83704

ANEXOS

Anexo 1: Instrumentos de recolección de datos

GUÍA DE ENTREVISTA

I. Título de Tesis:	Actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro, 2024
II. Datos generales del entrevistado	
- Nombre y apellidos:	DANIEL EDUARDO CONDORI FLORES
- Institución donde labora:	DIVISIÓN PNP
- Fecha:	10 / 03 / 2025
- Lugar:	AV. ESPAÑA 323 - PISO 9 - LIMA
III. Instrucciones:	
Leer detenidamente cada interrogante de la presente Guía de Entrevista y responda desde su experiencia, conocimiento y dé su opinión con claridad y veracidad. Sus respuestas consignadas serán el fundamento para corroborar los objetivos planteados en esta investigación.	

Objetivo General: Establecer los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024.

1. Para usted, ¿Cuáles son los actos de investigación eficaces para la identificación del sujeto que comete fraude informático en Lima Centro?

CONSIDERO QUE ES CLAVE APLICAR ACTOS DE INVESTIGACIÓN EFICACES QUE COMBINEN TECNICAS FORENSES DIGITALES CON METODOS TRADICIONALES DE INTELIGENCIA.

2. Para usted, ¿Cuál es el principal reto que afronta usted como autoridad para identificar al responsable del fraude informático en Lima Centro?

- FALTA DE COLABORACIÓN DE EMPRESAS TECNOLOGICAS
- LIMITACIONES EN LA LEGISLACIÓN Y PROCESOS JUDICIALES
- FALTA DE RECURSOS TECNOLOGICOS

Objetivo Específico 01: Determinar si la escucha telefónica es un acto de investigación eficaz para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024.

3. ¿Cree usted que la escucha telefónica es una herramienta adecuada y eficaz para identificar a los autores de fraude informático en Lima Centro?

CONSIDERO QUE SI ES UNA HERRAMIENTA UTIL, PERO SU EFICACIA DEPENDE DE VARIOS FACTORES COMO EL REQUERIMIENTO JUDICIAL Y USO DE MENSAJERIA CIFRADO

4. En cuanto a la privacidad de los usuarios, ¿Cómo se determina la eficacia de la escucha telefónica en la investigación del delito de fraude informático?

CONSIDERO QUE SE DETERMINA POR DIFERENTES CRITERIOS COMO: LA CALIDAD DE LA INFORMACIÓN, LA IDENTIFICACIÓN, UBICACIÓN, ENTRE OTROS AL RESPECTO QUIERO INDICAR QUE LOS DELINCUENTES USAN MENSAJERIAS CIFRADAS.

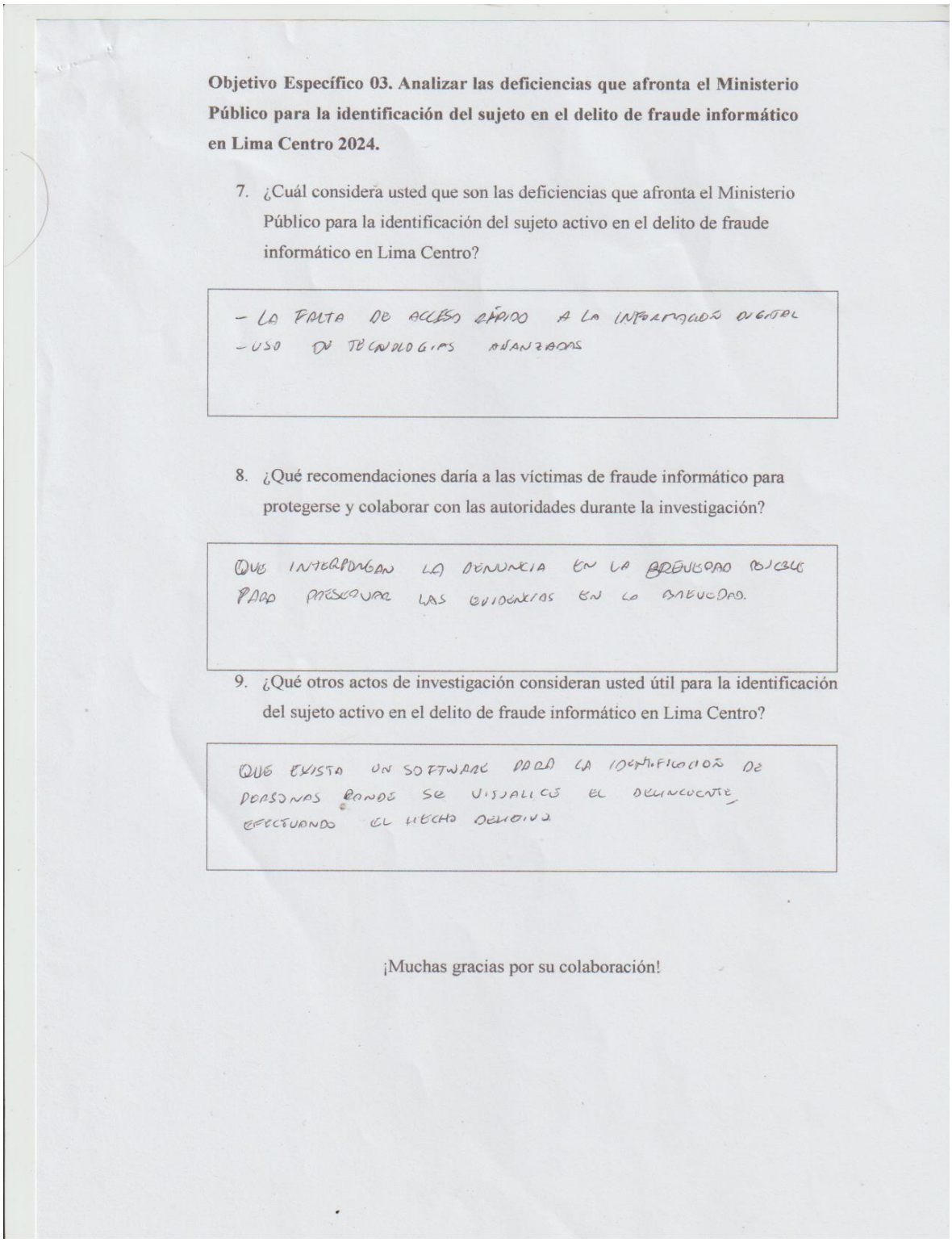
Objetivo Específico 02. Identificar como el levantamiento secreto de las comunicaciones es un acto de investigación eficaz para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024.

5. ¿Qué mejoras usted considera necesarias en la legislación sobre interceptación de comunicaciones para enfrentar eficazmente el fraude informático en los próximos años?

- PERMITIR LA INTERCEPTACIÓN DE COMUNICACIONES DIGITALES EN PLATAFORMAS DIGITALES (REDES SOCIALES - MENSAJERIA) BAJO SUPERVISIÓN JUDICIAL

6. ¿Cómo considera usted que ha influido el uso del levantamiento secreto de las comunicaciones en las investigaciones de los casos de fraude informático?

SI, PERO CON LIMITACIONES



Objetivo Específico 03. Analizar las deficiencias que afronta el Ministerio Público para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024.

7. ¿Cuál considera usted que son las deficiencias que afronta el Ministerio Público para la identificación del sujeto activo en el delito de fraude informático en Lima Centro?

- LA FALTA DE ACCESO RÁPIDO A LA INFORMACIÓN DIGITAL
- USO DE TECNOLOGÍAS AVANZADAS

8. ¿Qué recomendaciones daría a las víctimas de fraude informático para protegerse y colaborar con las autoridades durante la investigación?

QUE INTERPONGAN LA DENUNCIA EN LA BREVEDAD POSIBLE PARA PRESERVAR LAS EVIDENCIAS EN LA BREVEDAD.

9. ¿Qué otros actos de investigación consideran usted útil para la identificación del sujeto activo en el delito de fraude informático en Lima Centro?

QUE EXISTA UN SOFTWARE PARA LA IDENTIFICACIÓN DE PERSONAS DONDE SE VISUALICE EL DELINCUENTE EFECTUANDO EL HECHO DELICTIVO

¡Muchas gracias por su colaboración!

Para acceder a ver todas las entrevistas, favor de seleccionar el siguiente link

https://drive.google.com/drive/folders/1HbgmZotK0BdwkkOgtpffZujpGfacuTul?usp=sharing

Anexo 2: Validación del instrumento

UCT
UNIVERSIDAD CATÓLICA DE TRUJILLO

CARTA DE PRESENTACIÓN

Lima, 24 de febrero de 2025

Estimado Mg. Yoselyn Jasmine Ulloa Fernández

Asunto: Participación en juicio de expertos para validar instrumento con enfoque cualitativo

Es grato dirigirnos a Ud. para expresarle nuestra estima personal y un cordial saludo; con respecto al ASUNTO, hacerle de conocimiento que estamos realizando el trabajo de investigación titulado: **"Actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro, 2024"**; con el fin de obtener el Título Profesional de Abogado en la Facultad de Derecho y Ciencias Jurídicas de la Universidad Católica de Trujillo Benedicto XVI.

La presente investigación tiene por finalidad, Establecer los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024: por lo que se debe realizar una entrevista, basado en un cuestionario de 09 preguntas abiertas; cuyo instrumento es la Guía de entrevista; en tal sentido, su valiosa opinión permitirá verificar si las preguntas planteadas guardan relación con el título, objetivos y categorías planteados en la investigación. Por tal motivo, deben ser validadas por expertos, como es el caso de su persona; por lo que, le invito a colaborar con mi investigación; validando en calidad de experto dicho instrumento en mención.

Seguro de su participación en calidad de experto para la validación del instrumento de evaluación, se le alcanza el instrumento, matriz de categorización que, le servirá a Ud. para hacer las apreciaciones respectivas por cada ítem del instrumento.

Agradezco su atención y disposición para cumplir con lo propuesto.

Atentamente,

.....	.....
Bach. Jhoanna Dayan Corpus Machagua	Bach. Geivi Ojeda Velasquez
DNI:71327298	DNI:76812594

X

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1 TITULO DEL TRABAJO DE INVESTIGACIÓN: Actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro, 2024
1.2 NOMBRE DEL INSTRUMENTO DE EVALUACIÓN: Guía de entrevista
1.3 INVESTIGADORES: Br Corpus Machahua Joanna Dayan Br Geivi Ojeda Velásquez

II. DATOS DEL EXPERTO

2.1 APELLIDOS Y NOMBRES: Yoselyn Jasmine Ulloa Fernàndez
2.2 ESPECIALIDAD: Maestra en Gestiòn Pùblica
2.3 LUGAR Y FECHA: Sondorillo, 04 de marzo del 2025
2.4 **CARGO E INSTITUCIÓN DONDE LABORA:** Gerente De Asesorìa Jurìdica / Municipalidad Distrital De Sondorillo

Criterios evaluados	Valoración positiva			Valoración negativa	
	MA(3)	BA (2)	A(1)	PA	NA
Calidad de redacción de los ítems			X		
Objetividad y actualidad			X		
Suficiencia e intencionalidad (el instrumento mide pertinentemente las variables, dimensiones o categorías)		X			
Congruencia y consistencia (solidez científica)			X		
Coherencia con las dimensiones, variables y categorías			X		
Estrategia metodológica		X		No aporta	

04 de marzo del 2025

Mg. Abg. Yoselyn Jasmine Ulloa Fernández

SELLO Y FIRMA DEL EXPERTO
DNI N°: 48670165

Instrucciones de Evaluación de ítems: coloque en cada casilla de valoración la letra o letras correspondientes al aspecto cualitativo que, según criterio, cumple cada ítem a medir los aspectos o dimensiones de la variable en estudio. Las valoraciones son las siguientes:

MA= Muy adecuado/ **BA**= Bastante adecuado/ **A**= Adecuado/ **PA**= Poco adecuado/ **NA**= No adecuado

UCT
UNIVERSIDAD CATÓLICA DE TRUJILLO

CARTA DE PRESENTACIÓN

Lima, 24 de febrero de 2025

Estimado Mg. Edgar Manuel Charcape Armas

Asunto: Participación en juicio de expertos para validar instrumento con enfoque cualitativo

Es grato dirigirnos a Ud. para expresarle nuestra estima personal y un cordial saludo; con respecto al ASUNTO, hacerle de conocimiento que estamos realizando el trabajo de investigación titulado: **"Actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro, 2024"**; con el fin de obtener el Título Profesional de Abogado en la Facultad de Derecho y Ciencias Jurídicas de la Universidad Católica de Trujillo Benedicto XVI.

La presente investigación tiene por finalidad, Establecer los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024: por lo que se debe realizar una entrevista, basado en un cuestionario de 09 preguntas abiertas; cuyo instrumento es la Guía de entrevista; en tal sentido, su valiosa opinión permitirá verificar si las preguntas planteadas guardan relación con el título, objetivos y categorías planteados en la investigación. Por tal motivo, deben ser validadas por expertos, como es el caso de su persona; por lo que, le invito a colaborar con mi investigación; validando en calidad de experto dicho instrumento en mención.

Seguro de su participación en calidad de experto para la validación del instrumento de evaluación, se le alcanza el instrumento, matriz de categorización que, le servirá a Ud. para hacer las apreciaciones respectivas por cada ítem del instrumento.

Agradezco su atención y disposición para cumplir con lo propuesto.

Atentamente,

.....	.....
Bach. Jhoanna Dayan Corpus Machagua	Bach. Geivi Ojeda Velasquez
DNI:71327298	DNI:76812594

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1 TITULO DEL TRABAJO DE INVESTIGACIÓN: Actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro, 2024
1.2 NOMBRE DEL INSTRUMENTO DE EVALUACIÓN: Guía de entrevista
1.3 INVESTIGADORES: Br. Corpus Machahua Joanna Dayan Br. Ojeda Velásquez Geivi

II. DATOS DEL EXPERTO

2.1 APELLIDOS Y NOMBRES: Charcape Armas Edgar Manuel
2.2 ESPECIALIDAD: Derecho Constitucional y Administrativo
2.3 LUGAR Y FECHA: Trujillo, 07 de marzo del 2025
2.4 CARGO E INSTITUCIÓN DONDE LABORA: Abogado

Criterios evaluados	Valoración positiva			Valoración negativa	
	MA(3)	BA (2)	A(1)	PA	NA
Calidad de redacción de los ítems	X				
Objetividad y actualidad	X				
Suficiencia e intencionalidad (el instrumento mide pertinentemente las variables, dimensiones o categorías)	X				
Congruencia y consistencia (solidez científica)	X				
Coherencia con las dimensiones, variables y categorías	X				
Estrategia metodológica	X			No aporta	

07 de marzo del 2025

Edgar Manuel Charcape Armas
ABOGADO
Reg. CALL. N° 9446

SELLO Y FIRMA DEL EXPERTO
DNI N°: 18210054

Instrucciones de Evaluación de ítems: coloque en cada casilla de valoración la letra o letras correspondientes al aspecto cualitativo que, según criterio, cumple cada ítem a medir los aspectos o dimensiones de la variable en estudio. Las valoraciones son las siguientes:

MA= Muy adecuado/ **BA=** Bastante adecuado/ **A=** Adecuado/ **PA=** Poco adecuado/ **NA=** No adecuado

UCT
UNIVERSIDAD CATÓLICA DE TRUJILLO

CARTA DE PRESENTACIÓN

Lima, 24 de febrero de 2025

Estimado Mg. José Velásquez García

Asunto: Participación en juicio de expertos para validar instrumento con enfoque cualitativo

Es grato dirigirnos a Ud. para expresarle nuestra estima personal y un cordial saludo; con respecto al ASUNTO, hacerle de conocimiento que estamos realizando el trabajo de investigación titulado: **"Actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro, 2024"**; con el fin de obtener el Título Profesional de Abogado en la Facultad de Derecho y Ciencias Jurídicas de la Universidad Católica de Trujillo Benedicto XVI.

La presente investigación tiene por finalidad, Establecer los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024: por lo que se debe realizar una entrevista, basado en un cuestionario de 09 preguntas abiertas; cuyo instrumento es la Guía de entrevista; en tal sentido, su valiosa opinión permitirá verificar si las preguntas planteadas guardan relación con el título, objetivos y categorías planteados en la investigación. Por tal motivo, deben ser validadas por expertos, como es el caso de su persona; por lo que, le invito a colaborar con mi investigación; validando en calidad de experto dicho instrumento en mención.

Seguro de su participación en calidad de experto para la validación del instrumento de evaluación, se le alcanza el instrumento, matriz de categorización que, le servirá a Ud. para hacer las apreciaciones respectivas por cada ítem del instrumento.

Agradezco su atención y disposición para cumplir con lo propuesto.

Atentamente,

.....	.....
Bach. Jhoanna Dayan Corpus Machagua	Bach. Geivi Ojeda Velasquez
DNI:71327298	DNI:76812594

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1 TITULO DEL TRABAJO DE INVESTIGACIÓN: Actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro, 2024
1.2 NOMBRE DEL INSTRUMENTO DE EVALUACIÓN: Guía de entrevista
1.3 INVESTIGADORES: Br Corpus Machahua Joanna Dayan Br Geivi Ojeda Velásquez

II. DATOS DEL EXPERTO

2.1 APELLIDOS Y NOMBRES: JOSE ECSI VELASQUEZ GARCIA
2.2 ESPECIALIDAD: DERECHO CONSTITUCIONAL Y ADMINISTRATIVO
2.3 LUGAR Y FECHA: 14 DE MARZO DE 2025
2.4 CARGO E INSTITUCIÓN DONDE LABORA: CONSULTOR EN DERECHO CONSTITUCIONAL

Criterios evaluados	Valoración positiva			Valoración negativa	
	MA(3)	BA (2)	A(1)	PA	NA
Calidad de redacción de los ítems	X				
Objetividad y actualidad	X				
Suficiencia e intencionalidad (el instrumento mide pertinentemente las variables, dimensiones o categorías)		X			
Congruencia y consistencia (solidez científica)		X			
Coherencia con las dimensiones, variables y categorías	X				
Estrategia metodológica	X			No aporta	

Lima, a los 14 del mes de marzo de 2025

José E. Velásquez García
ABOGADO
CASM N° 1327

SELLO Y FIRMA DEL EXPERTO
DNI N°: 48167299

Instrucciones de Evaluación de ítems: coloque en cada casilla de valoración la letra o letras correspondientes al aspecto cualitativo que, según criterio, cumple cada ítem a medir los aspectos o dimensiones de la variable en estudio. Las valoraciones son las siguientes:

MA= Muy adecuado/ **BA**= Bastante adecuado/ **A**= Adecuado/ **PA**= Poco adecuado/ **NA**= No adecuad

Anexo 3: Cuadro de categorías y sub categorías

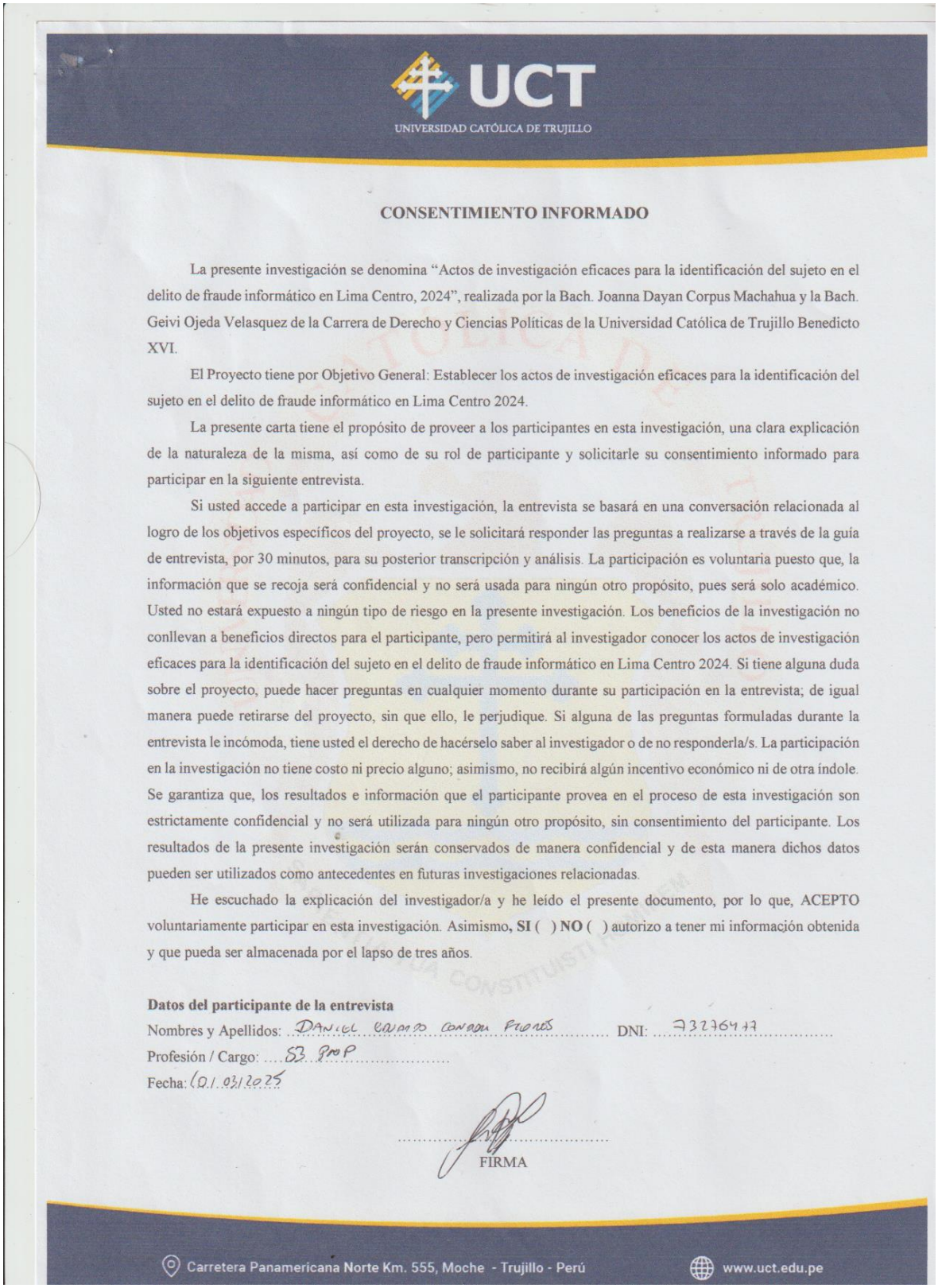
Ámbito temático	Problema de investigación	Preguntas de Investigación	Objetivos Generales	Objetivos Específicos	Categorías	Subcategorías	Preguntas a participantes
Derecho penal y sus instituciones	Actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024.	¿Cuáles son los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024?	Establecer los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro, 2024.	-Determinar si la escucha telefónica es un acto de investigación eficaz para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024. -Identificar como el levantamiento secreto de las comunicaciones es un acto de investigación eficaz para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024. - Analizar las deficiencias que afronta el Ministerio Público para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024.	Actos de investigación para la identificación del sujeto	-Actos de investigación eficaces -Identificación del sujeto en el delito de fraude informático. -La escucha telefónica. -El levantamiento del secreto de las comunicaciones.	- Para usted, ¿Cuáles son los actos de investigación eficaces para la identificación del sujeto que comete fraude informático en Lima Centro 2024? - Para usted, ¿Cuál es el principal reto que afronta usted como autoridad para identificar al responsable del fraude informático en Lima Centro? - ¿Cree usted que la escucha telefónica es una herramienta adecuada y eficaz para identificar a los autores de fraude

							informático en Lima Centro? - En cuanto a la privacidad de los usuarios, ¿cómo se determina la eficacia de la escucha telefónica en la investigación del delito de fraude informático? - ¿Qué mejoras usted considera necesarias en la legislación sobre interceptación de comunicaciones para enfrentar eficazmente el fraude informático en los próximos años? - ¿Cómo considera usted que ha influido el uso del levantamiento secreto de las comunicaciones en las investigaciones de los

							casos de fraude informático?
					Delito de fraude informático	-Principales dificultades que afrontan las autoridades -Protección jurídica y consecuencias del delito de fraude informático. - Identificación del sujeto en el delito de fraude informático.	- ¿Cuál considera usted que son las deficiencias que afronta el Ministerio Público para la identificación del sujeto activo en el delito de fraude informático en Lima Centro 2024? - ¿Qué recomendaciones daría a las víctimas de fraude informático para protegerse y colaborar con las autoridades durante la investigación? - ¿Qué otros actos de investigación consideran usted útil para la identificación del sujeto

							activo en el delito de fraude informático en Lima Centro 2024?

Anexo 4: Consentimiento informado



UCT
UNIVERSIDAD CATÓLICA DE TRUJILLO

CONSENTIMIENTO INFORMADO

La presente investigación se denomina "Actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro, 2024", realizada por la Bach. Joanna Dayan Corpus Machahua y la Bach. Geivi Ojeda Velasquez de la Carrera de Derecho y Ciencias Políticas de la Universidad Católica de Trujillo Benedicto XVI.

El Proyecto tiene por Objetivo General: Establecer los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024.

La presente carta tiene el propósito de proveer a los participantes en esta investigación, una clara explicación de la naturaleza de la misma, así como de su rol de participante y solicitarle su consentimiento informado para participar en la siguiente entrevista.

Si usted accede a participar en esta investigación, la entrevista se basará en una conversación relacionada al logro de los objetivos específicos del proyecto, se le solicitará responder las preguntas a realizarse a través de la guía de entrevista, por 30 minutos, para su posterior transcripción y análisis. La participación es voluntaria puesto que, la información que se recoja será confidencial y no será usada para ningún otro propósito, pues será solo académico. Usted no estará expuesto a ningún tipo de riesgo en la presente investigación. Los beneficios de la investigación no conllevan a beneficios directos para el participante, pero permitirá al investigador conocer los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático en Lima Centro 2024. Si tiene alguna duda sobre el proyecto, puede hacer preguntas en cualquier momento durante su participación en la entrevista; de igual manera puede retirarse del proyecto, sin que ello, le perjudique. Si alguna de las preguntas formuladas durante la entrevista le incómoda, tiene usted el derecho de hacérselo saber al investigador o de no responderla/s. La participación en la investigación no tiene costo ni precio alguno; asimismo, no recibirá algún incentivo económico ni de otra índole. Se garantiza que, los resultados e información que el participante provea en el proceso de esta investigación son estrictamente confidencial y no será utilizada para ningún otro propósito, sin consentimiento del participante. Los resultados de la presente investigación serán conservados de manera confidencial y de esta manera dichos datos pueden ser utilizados como antecedentes en futuras investigaciones relacionadas.

He escuchado la explicación del investigador/a y he leído el presente documento, por lo que, ACEPTO voluntariamente participar en esta investigación. Asimismo, **SI** ( ) **NO** ( ) autorizo a tener mi información obtenida y que pueda ser almacenada por el lapso de tres años.

Datos del participante de la entrevista

Nombres y Apellidos: DANIEL EDWARD CONDOR PUENTE DNI: 73276477

Profesión / Cargo: ABOGADO

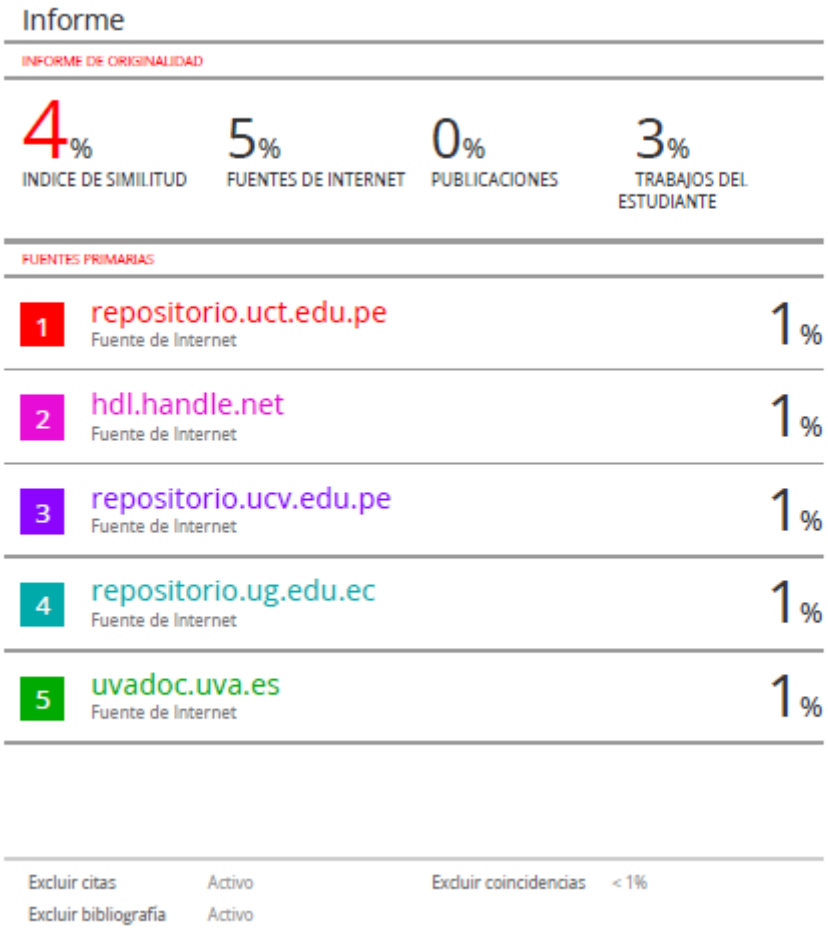
Fecha: 01/03/2025

FIRMA

Carretera Panamericana Norte Km. 555, Moche - Trujillo - Perú www.uct.edu.pe

Para acceder a ver todos los consentimientos, favor de seleccionar el siguiente link: https://drive.google.com/drive/folders/1Zctr8G1JdXpsTk6pR2iHFNiefPzvwNKv?usp=sharing

Anexo 5: Informe de turnitin



Informe

INFORME DE ORIGINALIDAD

4%	5%	0%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.uct.edu.pe Fuente de Internet	1%
2	hdl.handle.net Fuente de Internet	1%
3	repositorio.ucv.edu.pe Fuente de Internet	1%
4	repositorio.ug.edu.ec Fuente de Internet	1%
5	uvadoc.uva.es Fuente de Internet	1%

Excluir citas	Activo	Excluir coincidencias	< 1%
Excluir bibliografía	Activo		