Actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático

Effecctive investigative actions to identify the subject involved in the crime of computer fraud

[1] Joanna Dayan Corpus Machahua; [2] Geivi Ojeda Velásquez

[1-2] Universidad Católica de Trujillo "Benedicto XVI"

ORCID de Autora:

[1] J. Corpus (https://orcid.org/0000-0002-0753-2937)

joannadayan.01@gmail.com

[2] G. Ojeda (https://orcid.org/0000-0003-0329-7359)

geivivelasquez21@gmail.com

Fecha de recepción: 29 03 2025 Fecha de aceptación: 27 05 2025

DOI: https://doi.org/10.46363/derecho.v3i1.3

RESUMEN

El presente artículo científico pretende establecer los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático. Con el tiempo, este delito ha generado y causado aspectos significativos dentro de entidades públicas y privadas. Afectando además 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. A medida que la tecnología y los medios digitales avanzan, los criminales también adoptan técnicas cada vez más sofisticadas para cometer fraudes. Esto ha generado desafíos en términos de identificación y persecución de los responsables. Nuestra normativa legal vigente, contempla y señala actos de investigación eficaces como el allanamiento, el levantamiento del secreto de las comunicaciones, el levantamiento del secreto bancarios y las pericias. Sin embargo, se concluye en la necesidad de implementar nuevos mecanismos legales de investigación como las pruebas directas, sistemas software que identifiquen en corto tiempo las direcciones IP. Planteando además , la mejora de capacitación a los especialistas y la necesidad de realizar modificaciones dentro de la Ley N°30096 y Código Procesal Penal.

Palabras clave: Actos de investigación – sujeto – fraude informático

ABSTRACT

This scientific article aims to establish effective investigative procedures for identifying the perpetrator in the crime of computer fraud. Over time, this crime has generated and caused significant issues within public and private entities. It also affects integrity, the vulnerability of rights, and even the confidentiality of personal data, generating financial losses and increasing people's distrust of the financial system. As technology and digital media advance, criminals also adopt increasingly sophisticated techniques to commit fraud. This has generated challenges in terms of identifying and prosecuting those responsible. Our current legal regulations contemplate and outline effective investigative procedures such as search warrants, lifting of communications secrecy, lifting of banking secrecy, and forensic examinations. However, it concludes that it is necessary to implement new legal investigative mechanisms such as direct evidence and software systems that quickly identify IP addresses. It also proposes improved training for specialists and the need to make amendments to Law N°. 30096 and the Code of Criminal Procedure.

Keywords: Research acts – subject – computer fraud

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 establecer los actos de investigación para la identificación del sujeto que comete este tipo de delito. Cabe resaltar que el internet es muy favorable para la sociedad, pero a la vez es considerado un instrumento u objeto para la comisión de verdaderos delitos.

Desde la pandemia COVID -19 en el año 2020, los datos referentes a la comisión de fraudes informáticos aumentaron en grandes cantidades, donde fue mucho más visible saber que no se establecen 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.

En la ciudad de 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 y la identificación de los sujetos se vuelve problemática cuando no se obtienen actos de investigación de identificación eficaces. En el año 2021, el Ministerio Público brindó datos, referente a denuncias recibidas por el delito de fraude informático, atan solo en ese año , se recibieron 18,596 denuncias y haciendo un comparativo con el año 2020 y se obtuvo un incremento de 92,9 %. Estos datos reflejan el incremento abismal de este delito. En la misma línea, 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 excesiva demora en la entrega de información y cumplimiento de los plazos procesales , concurren a

procesos inconclusos que conllevan al archivamiento de la investigación y decisiones injustas.

1. Definición de fraude informático

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.

El fraude informático 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. Hay muchas formas comunes para cometer este tipo de delito, sobre todo con el avance que han tenido las herramientas tecnológicas, otra de las 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 fraude informático, 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.

2. Marco normativo

A. LEY N° 30096

La Ley N.º 30096 fue promulgada en el año 2013, con el objetivo de prevenir, tipificar y sancionar los delitos informáticos, es decir, los delitos cometidos mediante el uso de computadoras, redes, internet, teléfonos móviles u otras

tecnologías de la información y comunicación (TIC).
Fue creada para llenar un vacío legal frente al aumento de crímenes cibernéticos, como el hackeo, fraudes digitales, suplantaciones de identidad, entre otros.

Artículo 8-Fraude Informático
Quien, de manera intencional y sin autorización, obtenga para sí mismo o para otra persona un beneficio económico ilícito, causando perjuicio a un tercero, mediante la creación, modificación, eliminación, clonación de datos informáticos, o mediante cualquier forma de alteración o interferencia en el funcionamiento de un sistema informático, será sancionado con una pena de prisión no menor de tres ni mayor de ocho años, además de una multa de entre sesenta y ciento veinte días.

La sanción aumentará a una pena de prisión no menor de cinco ni mayor de diez años, y una multa de ochenta a ciento cuarenta días, si el perjuicio afecta fondos públicos destinados a programas sociales o asistenciales del Estado.

La Ley N.º 30096 es una herramienta clave para el sistema penal peruano en la lucha contra los delitos informáticos. Su aplicación exige coordinación entre fiscales, policías, peritos informáticos y jueces, así como colaboración de las empresas tecnológicas. A medida que la tecnología avanza, esta ley también se actualiza para seguir siendo efectiva**.**

B. ACTOS DE INVESTIGACIÓN DENTRO DEL CÓDIGO PROCESAL PENAL

Artículo 330 CPP - Inicio de la investigación preliminar
El Ministerio Público da inicio a la investigación preliminar cuando tiene conocimiento de un hecho presuntamente delictivo. En casos de fraude informático, esto puede darse por denuncia de una víctima o por reporte de una entidad bancaria o tecnológica.
Ejemplo: una persona denuncia que le han vaciado su cuenta bancaria mediante suplantación digital.

Artículo 334 CPP -Disposición de diligencias preliminares
El fiscal puede ordenar diligencias urgentes para esclarecer los hechos y determinar la identidad del autor. Esto incluye:
-Requerimiento de información a empresas tecnológicas o bancarias
-Acceso a datos de IP, cuentas digitales, etc.

Artículo 230 CPP-Levantamiento del secreto de las comunicaciones

El juez penal puede autorizar la interceptación o acceso a llamadas telefónicas, correos electrónicos, chats o mensajes en redes sociales cuando sea necesario para identificar al autor del delito o recabar pruebas.

Fundamental en delitos informáticos donde el autor se oculta tras perfiles falsos o cuentas encriptadas.

Artículo 231 CPP – Entrega de documentos y registros

Permite al fiscal requerir a empresas, bancos o particulares la entrega de documentos físicos o digitales vinculados al hecho investigado, como:

-Historial de transacciones

-Logs de acceso o navegación

-Contratos digitales o facturación electrónica

Artículo 190-A CPP - Cadena de custodia

Regula cómo se deben recolectar, conservar y presentar las evidencias digitales para asegurar su integridad.

Esto es clave para que los dispositivos incautados sean válidos como prueba en juicio.

Los artículos del Código Procesal Penal mencionados proporcionan al fiscal y a la policía herramientas jurídicas para llevar a cabo actos de investigación eficaces, legales y proporcionales para identificar al responsable de un delito de fraude informático, garantizando al mismo tiempo los derechos fundamentales.

2.1 Los verbos rectores del delito de fraude informático

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) .

2.2 Convenio de Budapest

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.

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)

3. Los sujetos en el delito de fraude informático

El personaje de mayor interés en los fraudes informáticos es el sujeto activo, este causará un perjuicio en el sujeto pasivo o víctima, la acción de solo un sujeto está descrito en el tipo penal, tratándose de este sujeto. 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. A su vez, este sujeto 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)

Sobre el sujeto pasivo, Michael (2016), 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. 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 da consecuencia de los actos para que se cometa este delito y 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).

4. Los actos de investigación para la identificación del sujeto que comete fraude informático

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.

A. **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.

B. **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.

C. Los agentes encubiertos

Con relación a este acto, 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.

D. La geolocalización

Este acto 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.

E. Las pericias

Las pericias refieren 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.

5. **El incumplimiento de los pazos procesales y entrega de información dentro de la investigación.**

La investigación preliminar se inicia desde que las autoridades toman conocimiento de un hecho delictivo y comienzan a realizar las primeras diligencias. En esta fase, y debido a la urgencia y gravedad de ciertos casos, el Ministerio Público puede requerir el levantamiento del secreto de las comunicaciones con el objetivo de identificar y ubicar geográficamente al presunto autor del delito, conforme a lo dispuesto en el artículo 230, inciso 1, del Código Procesal Penal.

Cuando las diligencias no se ejecutan con la prontitud ni mediante los mecanismos procesales adecuados, se genera un riesgo significativo para el desarrollo del proceso penal, ya que es en esta etapa donde deben recabarse los medios probatorios pertinentes que permitan atribuir la responsabilidad penal a una persona debidamente identificada. Por ello, es fundamental que el fiscal actúe utilizando medidas restrictivas de derechos, las cuales constituyen herramientas claves para obtener pruebas válidas que serán utilizadas en la etapa de juicio oral.

Una vez que el juez emite la resolución correspondiente, el fiscal debe remitir un oficio a las empresas de telecomunicaciones, acompañado de dicha resolución, solicitando de forma inmediata la entrega de información. Esto incluye la identificación de los titulares de las líneas, la geolocalización de dispositivos móviles, y el registro de las comunicaciones, las cuales deben ser proporcionadas en tiempo real, las 24 horas del día, durante los 365 días del año. Se advierte además que el incumplimiento de esta obligación podría generar responsabilidades legales

.

6. **Protecciones constitucionales de los actos de investigación.**
   Constitución Política del Perú. Art. 139 inciso 3 y 14
   Toda persona tiene derecho a un proceso justo, dentro de un plazo razonable, ante un juez imparcial.
   Las diligencias de investigación deben respetar las reglas del proceso penal y no vulnerar los derechos del imputado ni de terceros.
   El uso de medios tecnológicos para investigar (rastreo IP, geolocalización, interceptación de comunicaciones) debe contar con autorización judicial cuando se afecten derechos fundamentales.
   Artículo 2, inciso 10 de la Constitución
   Nadie puede ser objeto de interceptación telefónica, acceso a correos electrónicos o redes privadas sin una resolución judicial motivada.
   En delitos informáticos, como el fraude electrónico, donde es necesario acceder a cuentas, mensajes, llamadas o geolocalización, el levantamiento del secreto de las comunicaciones sólo puede ser autorizado por un juez (Art. 230 CPP).
   La información extraída debe ser usada exclusivamente para fines judiciales.
   Las protecciones constitucionales buscan garantizar que las medidas de investigación incluso las más intrusivas como la interceptación de datos o la geolocalización se realicen dentro del marco del respeto a los derechos fundamentales, especialmente en delitos como el fraude informático, donde las tecnologías pueden facilitar excesos si no hay control judicial.

7. **Tipos y formas comunes del fraude informático**
   A. Pishing
   Actualmente, el phishing es uno de los tipos de amenazas de fraudes informáticos más peligrosos para el desarrollo de la sociedad, ya que implica la sustracción de tus datos personales, contraseñas, tarjetas de créditos. Asimismo, no solo es un peligro para las personas naturales, también lo es para las personas jurídicas, que se han visto perjudicadas bajo esta nueva modalidad de fraude.
   Acerca del origen de la palabra phishing, Leguizamón refiere lo siguiente: El origen de la palabra phishing proviene del término fishing, que significa pescar. Se identifica con esta palabra porque la intención de esta estafa es “pescar” a usuarios (las víctimas) de internet para que revelen información susceptible. Es decir, intentan que coja el “anzuelo” y ofrezcan sus datos confidenciales.
   La forma de phishing más utilizada es el envío masivo de correos electrónicos, a las

cuentas de Gmail, Hotmail, etc. Con la finalidad de engañar a la víctima y que proporcione sus datos personales al phisher".

B. Pharming

Pharming (se pronuncia como "fárming") es un término utilizado para describir un tipo de ciberataque que redirige a los usuarios a sitios web fraudulentos o manipula sus sistemas informáticos para recopilar información delicada. El pharming se parece al phishing en que es una amenaza que engaña a los usuarios para que divulguen información privada, pero en lugar de basarse en el correo electrónico como vector de ataque, el pharming utiliza código malicioso ejecutado en el dispositivo de la víctima para redirigirla a un sitio web controlado por el atacante. Dado que el pharming ejecuta el código en el ordenador de la víctima, el atacante no depende de que el usuario objetivo haga clic en un enlace o responda a un correo electrónico. En su lugar, el código malintencionado dirige al usuario objetivo al sitio web del atacante, eliminando el paso adicional de que el usuario haga clic en un enlace.

C. Clonación de tarjetas

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.

D. Antivirus falsos

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.

METODOLOGÍA

La presente revisión sistemática es de tipo básica. (Narváez, 2023) refiriéndose a este tipo básico, determina que: “Esta se utiliza en el ámbito científico para comprender y ampliar nuestros conocimientos sobre un fenómeno o campo específico”. Llevándonos a la ampliación de nuevos conocimientos, siendo estos, hipotético, puro o primordial, y todo el análisis realizado contribuye aportes científicos los cuales van a tener la característica de confiable.

El diseño de estudio tomado en cuenta es de un artículo científico, (Barrera, 2024) determina que este diseño se entiende como un estudio científico donde se va a recolectar un universo de información hecha por investigadores a cerca de un tema o pregunta, la cual nos va a proporcionar de manera exacta e imparcial una síntesis de estudios de importancia en un solo documento, con un enfoque cualitativo.

Con respecto a la técnica que se utilizó fue la de la entrevista, la cual se recabaron datos importantes y precisos de especialistas, a fin de obtener información relevante y consistente del tema de estudio. 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).

RESULTADOS

A continuación, detallamos los resultados obtenidos a través de la aplicación de la guía de entrevista a especialistas en el tema.

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. Sin embargo, estos 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. Se obtuvieron 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. 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.

Por otro lado, la mayoría de los entrevistados concuerdan en la necesidad de promover el uso correcto del internet. Así como realizar mejoras dentro de la Ley N° 30096 – Ley de delitos informáticos y en el Código Procesal Penal , donde el proceso no se vea alargado ni interrumpido por la falta de desconocimiento de las autoridades y demora excesiva en la entrega de información, que conllevan al incumplimiento de los plazos procesales.

En la misma línea, parte de los especialistas, mencionan que el levantamiento del secreto de las comunicaciones en los casos de fraude informático influye, por el que 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. Sin embargo,

este resulta ser ineficaz cuando las empresas de telefonía influyen en el archivamiento de los casos cuando no cumplen con la óptima entrega de información dentro de los plazos procesales.

Por otra parte, los especialistas no solo mencionan las deficiencias, sino también las limitaciones entorno al fraude informático, pues están de acuerdo en la promulgación de nuevas leyes y mejoría en otras. Tanto los fiscales como jueces han afrontado dentro del proceso obstáculos para la identificación de los sujetos en el delito de fraude informático, señalando además que la falta de capacitación solo refleja la cantidad de casos impunes.

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.

En el transcurso de la recolección de datos, los entrevistados señalan la necesidad de implementar nuevos mecanismos legales para la identificación del sujeto, reforzándolos con un procedimiento, generando transformaciones y protegiendo así la información de todos. Otro mecanismo que podría ser implementado es un software que permita identificar al delincuente efectuando el hecho delictivo en tiempo real, facilitando así su identificación.

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 del estudio, que consiste en establecer los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático. 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.

En cuanto a la eficacia de la escucha telefónica es un acto de investigación idóneo 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.

Sobre la eficacia del levantamiento secreto de las comunicaciones para la identificación del sujeto en el delito de fraude informático. 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 inviables, 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 este acto de investigación 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 .

Con relación a 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.

CONCLUSIONES

Con respecto a los actos de investigación eficaces para la identificación del sujeto en el delito de fraude informático, podemos concluir que estos son el levantamiento del secreto de las comunicaciones, el levantamiento del secreto bancario, la geolocalización, las pericias y la solicitud de información a diversas instituciones que tenga relación con el sujeto investigado. 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. Para ello, ese necesario que dentro de nuestros ordenamientos legales se implementen otros actos de investigación como las pruebas directas, el uso de herramientas como VPNs (red privada virtual) e implementar un software que permita identificar al delincuente en tiempo real.

Sobre la eficacia de la escucha telefónica, 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 claves 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. Por lo que, se

necesitan modificaciones en la LEY N° 30096 y se disminuyan los plazos procesales dentro del Código Procesal Penal.

En relación al levantamiento secreto de las comunicaciones, este 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. No obstante, deben implementarse mecanismos legales que permitan su proceso célere en la obtención de información.

Para erradicar o reducir eficazmente el fraude informático en el Perú, la Ley N.° 30096 Ley de Delitos Informáticos debe ser modificada y fortalecida en cinco áreas clave: tipificación penal actualizada, mayor prevención, cooperación institucional, adaptación tecnológica y protección de víctimas vulnerables. Las penas actuales no reflejan la gravedad del impacto cuando hay muchas víctimas o se usan tecnologías avanzadas. Aumentándose la pena por el grado de afectación del fraude cuando se usa tecnología sofisticada o automatizada, también si se comete en el marco de una organización criminal o las víctimas son menores, adultos mayores o personas con discapacidad.

Incluir medidas preventivas obligatorias. La ley actual se enfoca solo en castigar, pero no previene el delito. Las mejoras serían; a) Establecer la alfabetización digital obligatoria en escuelas y campañas públicas de prevención; b) Obligar a entidades financieras, tecnológicas y de servicios digitales a tener sistemas antifraude actualizados, notificar incidentes informáticos a la Policía o Fiscalía e implementar doble autenticación para transacciones sensibles. Fortaleciendo la investigación y persecución penal.

Para finalizar, concluimos en que las autoridades involucradas en la identificación de los sujetos que cometen el delito de fraude informático afrontan grandes deficiencias. Incluidas la falta de recursos tecnológicos adecuados, la capacitación insuficiente de los fiscales en el manejo de evidencia digital y las falencias 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.

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

Barrera, E. (2024). Revisiones sistemáticas: Definición: ¿qué es una revisión sistemática? Recuperado el junio de 2024, de https://biblioguias.unav.edu/revisionessistematicas/que-es-una-revision-sistematica

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.

Código Procesal Penal [C.P.P.]. Art. 230 (29 de julio de 2004)

Constitución Política del Perú [Const] Art. 2 (29 de diciembre de 1993)

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

Dulzaides Iglesias, M. E., & Molins Gomez, A. M. (abril de 2004). Análisis documental y de información: dos componentes de un mismo proceso. *12(2)*. Recuperado el junio de 2024, de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352004000200011

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

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

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

Molinos Cóbreces, A. (2020). El fraude informático y telemático: perspectiva penal. Valladolid, España. Recuperado en 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