UNIVERSIDAD PRIVADA SAN CARLOS

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE DERECHO

TESIS

VALORACIÓN DE MEDIOS PROBATORIOS EN DELITOS INFORMÁTICOS EN EL DEPARTAMENTO DE PUNO 2023

PRESENTADA POR:

EDY NESTOR ARCE QUENAYA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

ABOGADO

PUNO – PERÚ

2025

PLAGIARISM CHECK.ORG

3.83%

SIMILARITY OVERALL

SCANNED ON: 7 MAR 2025, 5:05 PM

Similarity report

Your text is highlighted according to the matched content in the results above.

IDENTICAL 0.79%

CHANGED TEXT 3.03%

Report #25128623

EDY NESTOR ARCE QUENAYA// VALORACIÓN DE MEDIOS PROBATORIOS EN DELITO S INFORMÁTICOS EN EL DEPARTAMENTO DE PUNO 2023 RESUMEN Valoración de Medios Probatorios en Delitos Informáticos en el Departamento de Puno 2023. El objetivo general de esta tesis fue determinar qué se necesita en el departamento de Puno para obtener medios probatorios que ameriten ser obligatorios en los procesos relacionados con delitos informáticos. La metodología empleada fue de tipo cualitativa, con un diseño no experimental de corte transversal, donde se realizaron entrevistas semiestructuradas a 5 abogados especialistas en derecho penal de la ciudad de Puno. Las conclusiones principales indican la necesidad de equipo tecnológico especializado (laboratorios forenses, peritos informáticos), una mejor coordinación interinstitucional entre la fiscalía y la Policía Nacional, la actualización en el uso de TICs, y una ley con mayor cobertura para las investigaciones. Además, se determinó que el delito de hurto requiere de un medio físico para su comisión, mientras que el delito de estafa debería considerar todo tipo de manipulación, incluyendo la informática. Palabras clave: Delitos informáticos, medios probatorios, valoración de pruebas. ABSTRACT Evaluation of Evidence in Cybercrime Cases in the Department of Puno 2023. The general objective of this thesis was to determine what is needed in the department of Puno to obtain evidentiary means that warrant being mandatory in processes related to cybercrimes. The

Yudy Roxana ALANIA LAQUI
Oficina de Repositorio Institucional

UNIVERSIDAD PRIVADA SAN CARLOS

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE DERECHO

TESIS

VALORACIÓN DE MEDIOS PROBATORIOS EN DELITOS INFORMÁTICOS EN EL DEPARTAMENTO DE PUNO 2023

PRESENTADA POR:

EDY NESTOR ARCE QUENAYA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

ABOGADO

APROBADA POR EL SIGUIENTE JURADO:

PRESIDENTE : _____
M.Sc. DENILSON MEDINA SANCHEZ

PRIMER MIEMBRO : _____
Mg. PERCY GABRIEL MAMANI PUMA

SEGUNDO MIEMBRO : _____
M.Sc. YANINA MILAGROS HUANCA EXCELMES

ASESOR DE TESIS : _____
Mg. MARTIN WILLIAM HUISA HUAHUASONCCO

Área: Ciencias Sociales.

Sub Área: Derecho.

Línea de investigación: Derecho

Puno, 14 de marzo del 2025.

DEDICATORIA

Este presente proyecto de investigación dedico a mi padres Jose y Francisca por haberme forjado y brindado su apoyo incondicional en mi formación profesional para optar el título de abogado.

A la universidad y a los docentes por los conocimientos brindados y por las enseñanzas impartidas.

EDY NESTOR ARCE QUENAYA

AGRADECIMIENTO

Primeramente agradezco profundamente a Dios todo poderoso, por haberme guiado en su camino verdadero y en la conclusión de mis estudios, gracias por darme salud, sabiduría e inteligencia para enfrentar el reto de la vida profesional.

A la universidad que nos alentó a ser buenos profesionales, a ser emprendedores, innovadores e investigadores y prestar servicio a la sociedad.

EDY NESTOR ARCE QUENAYA

ÍNDICE GENERAL

ANEXOS **44**

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE ANEXOS

RESUMEN

Valoración de Medios Probatorios en Delitos Informáticos en el Departamento de Puno 2023. El objetivo general de esta tesis fue determinar qué se necesita en el departamento de Puno para obtener medios probatorios que ameriten ser obligatorios en los procesos relacionados con delitos informáticos. La metodología empleada fue de tipo cualitativa, con un diseño no experimental de corte transversal, donde se realizaron entrevistas semiestructuradas a 5 abogados especialistas en derecho penal de la ciudad de Puno. Las conclusiones principales indican la necesidad de equipo tecnológico especializado (laboratorios forenses, peritos informáticos), una mejor coordinación interinstitucional entre la fiscalía y la Policía Nacional, la actualización en el uso de TICs, y una ley con mayor cobertura para las investigaciones. Además, se determinó que el delito de hurto requiere de un medio físico para su comisión, mientras que el delito de estafa debería considerar todo tipo de manipulación, incluyendo la informática.

Palabras clave: Delitos informáticos, Medios probatorios, Valoración de pruebas.

ABSTRACT

Evaluation of Evidence in Cybercrime Cases in the Department of Puno 2023. The general objective of this thesis was to determine what is needed in the department of Puno to obtain evidentiary means that warrant being mandatory in processes related to cybercrimes. The methodology employed was qualitative, with a non-experimental cross-sectional design, where semi-structured interviews were conducted with 5 criminal law specialists in the city of Puno. The main conclusions indicate the need for specialized technological equipment (forensic laboratories, computer experts), better inter-institutional coordination between the prosecutor's office and the National Police, updates in the use of ICTs, and a law with greater coverage for investigations. Additionally, it was determined that the crime of theft requires a physical means for its commission, while the crime of fraud should consider all types of manipulation, including digital manipulation.

Keywords: Cyber crimes, Evidentiary means, Evaluation of evidence.

INTRODUCCIÓN

La tesis titulada "Valoración de Medios Probatorios en Delitos Informáticos en el Departamento de Puno 2023" se enfoca en el análisis de los desafíos y necesidades para la correcta valoración de las pruebas digitales en el contexto de los delitos informáticos en el departamento de Puno.

La investigación reconoce que los delitos informáticos han experimentado un crecimiento exponencial a nivel mundial, facilitados por la globalización y los avances tecnológicos. Esta situación afecta a individuos, empresas y gobiernos, subrayando la necesidad de cooperación internacional para combatir estos delitos.

En el contexto peruano, la tesis señala que el país no es ajeno al aumento de los delitos informáticos, con un incremento significativo en los últimos años. A pesar de la implementación de leyes y regulaciones, persisten desafíos en la valoración y manejo de los medios probatorios en casos de cibercrimen.

A nivel local, en el departamento de Puno, la investigación destaca problemas particulares relacionados con la falta de infraestructura tecnológica adecuada y la limitada capacitación en temas cibernéticos entre los profesionales del derecho y las fuerzas del orden. Esto dificulta la recolección, preservación y valoración de los medios probatorios en delitos informáticos.

El objetivo principal de la tesis es determinar qué se necesita en el departamento de Puno para obtener medios probatorios que ameriten ser obligatorios en los procesos relacionados con delitos informáticos. Para lograr este objetivo, se plantea una metodología cualitativa con un diseño no experimental de corte transversal, utilizando entrevistas a abogados especialistas en derecho penal de la ciudad de Puno.

La tesis se estructura en cuatro capítulos:

El primer capítulo plantea el problema, destacando los antecedentes y los objetivos de la investigación.

El segundo capítulo desarrolla el marco teórico, con énfasis en la base teórica y la definición conceptual.

El tercer capítulo detalla la metodología, precisando el tipo y diseño de investigación, los instrumentos utilizados y las técnicas de recolección de datos.

El cuarto capítulo presenta la exposición y análisis de los resultados.

La investigación busca contribuir tanto al desarrollo teórico en la materia como a ofrecer soluciones prácticas que puedan ser implementadas a diferentes niveles, con un enfoque especial en la realidad del departamento de Puno.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA, ANTECEDENTES Y OBJETIVOS DE LA INVESTIGACIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA.

En la última década, los delitos informáticos han experimentado un crecimiento exponencial a nivel mundial. La globalización y el avance en las tecnologías de la información y la comunicación han permitido que los delincuentes cibernéticos operen con mayor facilidad, afectando a individuos, empresas y gobiernos. Instituciones como la Organización de las Naciones Unidas (ONU) y la INTERPOL han subrayado la necesidad de cooperación internacional para combatir este tipo de delitos. Sin embargo, una de las principales dificultades es la adecuada y uniforme valoración de los medios probatorios en diferentes jurisdicciones. Esta disparidad no sólo ralentiza los procesos judiciales, sino que también puede llevar a la impunidad de los criminales. La falta de protocolos estandarizados dificulta la cooperación entre países, lo que resalta la necesidad de investigaciones profundas en la materia para proponer soluciones que puedan ser adoptadas globalmente.

El Perú no es ajeno al aumento de los delitos informáticos. De acuerdo con el Instituto Nacional de Estadística e Informática (INEI), la incidencia de estos delitos ha aumentado significativamente en los últimos años, afectando tanto a ciudadanos comunes como a entidades públicas y privadas. La normativa peruana, si bien ha avanzado con la implementación de leyes y regulaciones para combatir estos delitos, aún enfrenta el desafío de la efectiva valoración y manejo de los medios probatorios en casos de cibercrimen. Además, existen limitaciones en la capacitación de los operadores de justicia y en la actualización tecnológica de las instituciones encargadas de la seguridad y la justicia. Este

contexto genera una necesidad urgente de desarrollar metodologías efectivas y protocolos claros que permitan una valoración justa y precisa de los medios probatorios en delitos informáticos.

El departamento de Puno, situado en el sur del Perú y caracterizado por su diversidad geográfica y cultural, enfrenta problemas particulares en relación con los delitos informáticos. La falta de infraestructura tecnológica adecuada y la limitada capacitación en temas cibernéticos entre los profesionales del derecho y fuerzas del orden empeoran la situación. Casos recientes han puesto en evidencia las dificultades para recoger, preservar y valorar los medios probatorios en delitos que, aunque cometidos en el ciberespacio, tienen un impacto directo en la comunidad local. Estos desafíos subrayan la necesidad de desarrollar estrategias específicas para la región de Puno, que consideren sus particularidades y permitan mejorar la eficacia en la lucha contra los delitos informáticos. Investigaciones centradas en la valoración de los medios probatorios en esta región pueden ofrecer importantes contribuciones para fortalecer el sistema de justicia local y mejorar la seguridad informativa de sus ciudadanos.

Este planteamiento del problema destaca la urgencia y relevancia de abordar la valoración de los medios probatorios en delitos informáticos, tanto en un contexto global como en el nacional y local. La investigación propuesta no solo busca contribuir al desarrollo teórico en la materia, sino también ofrecer soluciones prácticas que puedan ser implementadas a diferentes niveles, con un enfoque especial en la realidad del departamento de Puno.

1.1.1. PROBLEMA GENERAL

1. ¿Qué se necesita en el distrito de Puno para obtener medios probatorios que ameriten ser obligatorios en los procesos relacionados a delitos informáticos?

1.1.2. PROBLEMAS ESPECÍFICOS.

1. ¿Qué se necesita para continuar con la investigación preparatoria en los casos relacionados a delitos informáticos?
2. ¿Qué relación tienen el delito de hurto y el delito de estafa en los delitos informáticos?

1.2 ANTECEDENTES

1.2.1. INTERNACIONAL

Según Ramirez & Aguilera (2019) El trabajo está estructurado esencialmente en exámenes teóricos y prácticos de los elementos doctrinales primarios que sustentan el proceso general de creación, evolución, proyección y defensa de los delitos informáticos. Las instituciones internacionales que, desde sus inicios, buscando juntos soluciones genuinas a los grandes problemas, riesgos y amenazas que enfrenta la humanidad, se completan, con sencillez detallada, por un esquema único de referencias.

Se examinan los principales componentes doctrinales que la Comunidad Mundial considera para proporcionar un tratamiento eficaz a la delincuencia cibernética con la asistencia de organismos internacionales y el apoyo incondicional de los Estados Nacionales, así como los parámetros de referencia, la clasificación y el seguimiento internacional en la legislación de un grupo de países desarrollados y subdesarrollados.

Tomando como punto de conexión tres países de la región, también es abundante en el papel protagonista de nuestra América y su adopción de medidas en los problemas abrumadores que mueven la realidad latina de hoy, abordando sus sujetos pasivos y activos, elementos indispensables si consideramos las consecuencias que traería la proliferación de este tipo de derecho.

Peña & Bascur (2022) Tipos de delitos, sanciones y normas de procedimiento de la Ley 21.509: Delitos informáticos en Chile. Primera parte. La Ley 21.459 permitió al Estado de Chile cambiar las leyes contra la ciberdelincuencia y crear nuevas multas, directrices de procedimiento, La primera parte del análisis reglamentario, este texto ofrece una introducción al contenido de la ilicitud de este tipo de delitos y un desarrollo sistemático mediante un enfoque a los tipos penales de acceso ilícito (art. 2), fraude informático (arts. 7), recepción informática (art.6), y abuso de dispositivos (Art. 8).

Mayer (2018) Examen jurídico-criminal de los delitos cibernéticos: aspectos criminológicos En esta investigación se investigan algunos aspectos criminológicos que podrían apoyar el estudio legal-criminal de los delitos cibernéticos La investigación distingue formas y

contextos de comisión, temas y consecuencias, por lo tanto afectando el soporte lógico de un sistema informático e involucrando el uso de redes informáticas.

Cisternas & Moyano (2017) Examen y proyección de los delitos cibernéticos chilenos. El creciente desarrollo de la informática ha llevado a una multiplicación de la delincuencia informática. Este estudio examinará la situación actual de los delitos cibernéticos principalmente desde una perspectiva doctrinal con el objetivo de dar una visión sistemática del delito cibernético, examinar las técnicas legislativas utilizadas en el extranjero y en Chile para castigar estos delitos y, por último, analizar críticamente el contenido de la Ley No 19.233 relativa al delito Cibernético con el fin de exponer posibles errores en la legislación nacional sobre delitos informáticos.

Lobo et al (2023) El objetivo de la investigación era comparar la ley sobre ciberdelitos en Colombia con las que son sancionables en virtud de la legislación nacional de Perú, Chile, Alemania y España. Esto se prevé en el Convenio de Budapest contra la delincuencia cibernética. Inicialmente, se emplea un enfoque descritivo cualitativo para presentar una descripción exhaustiva del contenido y el alcance del instrumento de derecho internacional antes mencionado. Posteriormente, la clasificación y composición de los comportamientos observados en la Ley 1273 de 2009 de Colombia, que establece una nueva propiedad jurídica protegida conocida como protección de la información y los datos, y la Ley 1928 de 2018, que aprueba la Convención sobre el Ciberdelito, están conectados. Por último, la contextualización del derecho comparativo entre reglamentaciones nacionales y extranjeras depende de los países seleccionados. El avance ha permitido la identificación de varios métodos mediante los cuales los ciberdelincuentes han sido comprendidos e integrados en la legislación de estudio, así como las ventajas y desventajas de la tipografía, a fin de investigar, enjuiciar y penalizar la actividad criminal virtual.

Rivera (S.f) La rápida integración de las tecnologías informáticas hoy en Bolivia resulta en una variedad de delitos informáticos cada vez más frecuentes. No estamos lejos de lo que otras naciones están experimentando regularmente en este campo. De una manera u otra, corremos el riesgo de violar derechos muy vitales, incluyendo el derecho a la información, la

propiedad privada, el derecho de privacidad cuando manejamos computadoras, Internet, tarjetas electrónicas, chips, datos de computadora, cajeros automáticos, correo electrónico, publicidad, programas informáticos, códigos-contraseñas, etc.

Temperini (2023) Dos tipos diferentes de conclusiones se derivan de los resultados de este trabajo. Con el conocimiento de una clasificación de las naciones basada en el grado de protección penal en relación con los delitos informáticos examinados (a través de la reorganización de los datos presentados en el cuadro No 4), se pueden sacar conclusiones en el primer grupo, reconocidas desde un punto de vista cuantitativo.

Aviles (S.f) Diferentes tipos de acciones ilegales crecen como resultado del desarrollo de la informática en todas las esferas de la vida cotidiana, tanto en el trabajo como en el tiempo libre. Estas actividades se muestran de formas impensables y influyen así en un conjunto de bienes legalmente protegidos. Ser uno de los llamados "fraudes electrónicos" o "fraude informática" más frecuentes y darse cuenta de que este tipo de comportamiento goza de cierta impunidad en nuestra cultura hace que sea necesario un control adecuado.

1.2.2. NACIONAL

Mori (2019) En su tesis de maestría, buscó comprender cómo los operadores de la justicia investigan y juzgan crímenes que requieren tecnologías de la información. Descubrió la disparidad de opiniones entre jueces y fiscales, ya que los jueces creen que hay una falta de instrucción en las herramientas tecnológicas y la fiscalía no cree que haya tal ausencia, ni creen que haya violaciones de la regla porque no hay una determinación suficiente del daño causado.

Serrano (2021), Recomienda redefinir los fundamentos dogmáticos de la delincuencia cibernética, ampliando el estudio del dogmatismo para proporcionar una mayor protección a la propiedad jurídica, desde un entorno constitucional basado en una protección contemporánea de los principios penales, orientado hacia la protección de la persona humana con el objetivo de orientar las acciones de nuestros legisladores.

La protección de la información y los datos es un bien jurídico protegido ya que, como señaló

Piva et al. (2021) en el caso de la delincuencia cibernética, afecta al bienestar de la sociedad o de los grupos económicos que son susceptibles a actividades ilegales que requieren el uso de las TIC.

1.2.3. LOCAL

A nivel local no se cuenta con antecedentes relacionados al tema de investigación.

1.3 JUSTIFICACIÓN

Justificación Social.

La investigación sobre la valoración de los medios probatorios en delitos informáticos en el departamento de Puno tiene una importante justificación social. Los delitos informáticos afectan directamente a los ciudadanos, comprometiendo su seguridad y privacidad

La investigación sobre la valoración de los medios probatorios en delitos informáticos en el departamento de Puno tiene una importante justificación social. Los delitos informáticos afectan directamente a los ciudadanos, comprometiendo su seguridad y privacidad, así como sus bienes y patrimonio. Una adecuada valoración de los medios probatorios es clave para lograr condenas justas y prevenir la impunidad de estos delitos, lo que a su vez contribuye a generar un mayor sentimiento de seguridad y confianza en la población. Además, la investigación puede identificar las principales vulnerabilidades y desafíos que enfrentan las comunidades locales, permitiendo el desarrollo de estrategias y políticas públicas más efectivas para protegerlas.

Justificación Teórica

Desde el punto de vista teórico, esta investigación aportará al desarrollo del conocimiento en el campo de la valoración de pruebas digitales en el ámbito del derecho penal. Existen vacíos y dificultades conceptuales y metodológicas en torno a la valoración de este tipo de evidencias, lo que ha dificultado su aplicación efectiva en los procesos judiciales. Esta investigación permitirá analizar los enfoques existentes, identificar las principales problemáticas y proponer modelos teóricos más sólidos y adaptados a la realidad local. Esto contribuirá a fortalecer el marco teórico de la prueba digital y su aplicación en el contexto de los delitos informáticos.i

Justificación Metodológica

Desde una perspectiva metodológica, esta investigación busca desarrollar y aplicar técnicas y protocolos adecuados para la recolección, preservación y valoración de los medios probatorios en delitos informáticos. Dada la naturaleza particular de este tipo de evidencias, es necesario contar con metodologías innovadoras y adaptadas al contexto local, que permitan garantizar la autenticidad, integridad y admisibilidad de las pruebas digitales. Los hallazgos de esta investigación podrán ser empleados para mejorar los procedimientos utilizados por las instituciones encargadas de la investigación y la administración de justicia en Puno.

Justificación Normativa

En el ámbito normativo, esta investigación tiene una relevancia importante, ya que puede contribuir al fortalecimiento y la adecuación del marco legal y regulatorio relacionado con los delitos informáticos y la valoración de las pruebas digitales en el Perú, y particularmente en la región de Puno. El análisis de la normativa vigente y la identificación de vacíos o necesidades de actualización permitirán proponer mejoras a la legislación, lo que a su vez impactará positivamente en la eficacia de la persecución y sanción de estos delitos.

Importancia de la Investigación

La importancia de esta investigación radica en su potencial para mejorar la eficacia y la justicia en la persecución de los delitos informáticos en el departamento de Puno. Una adecuada valoración de los medios probatorios es fundamental para garantizar condenas justas y evitar la impunidad de estos delitos, lo que a su vez fortalecerá la confianza de la ciudadanía en el sistema de justicia. Además, los hallazgos de esta investigación podrán ser utilizados para informar el desarrollo de políticas públicas, programas de capacitación y protocolos de actuación que permitan una mejor prevención y respuesta a los delitos informáticos a nivel local y, potencialmente, a nivel nacional. En definitiva, esta investigación tiene el potencial de generar un impacto positivo en la seguridad y el bienestar de la población de Puno.

1.4 OBJETIVOS DE LA INVESTIGACIÓN

1.4.1. OBJETIVO GENERAL

1. Determinar que se necesita en el departamento de Puno, para obtener medios probatorios que ameriten ser obligatorios en los procesos relacionados a delitos informáticos.

1.4.2. OBJETIVO ESPECÍFICO

1. Determinar qué se necesita para continuar con la investigación preparatoria en los casos relacionados a delitos informáticos.
2. Determinar qué relación tienen el delito de hurto y el delito de estafa en los delitos informáticos.

CAPÍTULO II

MARCO TEÓRICO, CONCEPTUAL E HIPÓTESIS DE LA INVESTIGACIÓN

2.1 MARCO TEÓRICO

Las herramientas tecnológicas se han utilizado con fines ilegales, incluidos la vinculación de estafas, la suplantación de la identidad, el contacto con menores con fines criminales, la extorsión y otros para perjudicar a terceros. También han ayudado con beneficios interminables, como la planificación de audiencias usando computadoras u otros medios electrónicos y la facilitación de relaciones comerciales.

2.2.1. DIVINDAT

En la actualidad es responsabilidad de DIVINDAT investigar delitos informáticos y otros delitos relacionados con el uso de computadoras. Dado que el bien jurídico está relacionado con la informática, o "de la información y los datos", es un bien legal autónomo, y dado que su comisión requiere conocimientos específicos, su violación conduce a la tipificación de otros delitos como ataques contra diferentes intereses jurídicos.

Jimeno (2019), en su libro “Derecho de daños tecnológicos, ciberseguridad e insurtech” señala que, las tecnologías de la información y las comunicaciones (TIC) son ahora ampliamente utilizadas e importantes, por lo que son un componente vital en el ámbito socioeconómico. Se han convertido en un pilar básico de la hiperconectividad, donde el ciberespacio abarca esferas sociales y jurídicas. En la esfera jurídica, se han multiplicado las repercusiones de Internet, sus fenómenos y los crecientes riesgos cibernéticos, como las ciberamenazas.

Dado que sus usos en su comité difieren, el autor distingue entre el riesgo técnico o informático y el riesgo cibernético. En particular, los riesgos cibernéticos provienen del

desarrollo de las TIC y comprenden tres elementos principales: una acción o omisión, la explotación de una vulnerabilidad o fallo en los sistemas tecnológicos y procedimientos internos, y los efectos externos consecuentes que podrían causar daño.

Las cuestiones de ciberseguridad reciben la máxima prioridad en América Latina, por lo que las cuestiones relacionadas con la delincuencia cibernética reciben un enfoque bastante menor.

2.2.2. TICS

El criminólogo e investigador privado Ferro (2020), en su libro “Cyber espionaje, Ciber estafas y Guerras informáticas El lado oscuro de Internet : la prueba digital”, Considerando que la delincuencia cibernética se refiere a los actos humanos cometidos con el uso de redes de comunicaciones, sistemas electrónicos e informáticos y TIC, destaca que los delitos perpetrados con instrumentos técnicos no tienen un comportamiento suficientemente controlado por la ley que viole el orden jurídico en el ciberespacio.

Ferro (2020), sugiere que, la manifestación de los cibercrimen o delitos informáticos son parte de un crimen organizado. Esto también se detalla en el R.N N° 4727-2006 Lima, que señala que "En el delito informático se atribuye la participación en calidad de colaborador secundario, ya que permito el uso de cuentas de la empresa para el desvío de dinero a cambio de un porcentaje, siendo su comportamiento el de permanecer callado y no reportar el suceso ante sus autoridades.

2.2.3. DELITOS INFORMÁTICOS

Serrano (2021), Se recomienda que se redefinen los fundamentos dogmáticos de la delincuencia cibernética y que se siga estudiando el dogmatismo para proporcionar una mayor protección a la propiedad jurídica. Esto debe hacerse en un contexto constitucional basado en una protección moderna de los principios penales, con énfasis en la protección de la persona humana. El objetivo es orientar las actividades de nuestros legisladores.

Hernández (2012) afirma que la búsqueda de nuevos conocimientos se basa en una teoría que actúa como punto de partida. La investigación exige la orientación de las ideas que

dirigen el estudio y sus resultados; la teoría se compara con el resultado teórico por medio de ayudar a dar forma a una realidad.

La protección de la información y los datos es el bien jurídico que debe ser salvaguardado ya que Piva, et al., (2021) señala que en el caso de la ciberdelincuencia afecta al bienestar de la sociedad o de los grupos económicos, que son vulnerables a conductas ilegales que requieren el uso de las TIC; por lo tanto, la protección de información y datos es la protección del bien legal.

La investigación abarca teorías y enfoques conceptuales que están organizados según las categorías de delitos contra la propiedad relacionados con computadoras e investigación preliminar. R.N. No. 4727-2006 Lima define el delito informático como "cualquier acto que permita la comisión de delitos, daños o lesiones contra personas, grupos de personas, entidades o instituciones, y que se ejecuta típicamente mediante el uso de computadoras en el mundo virtual."

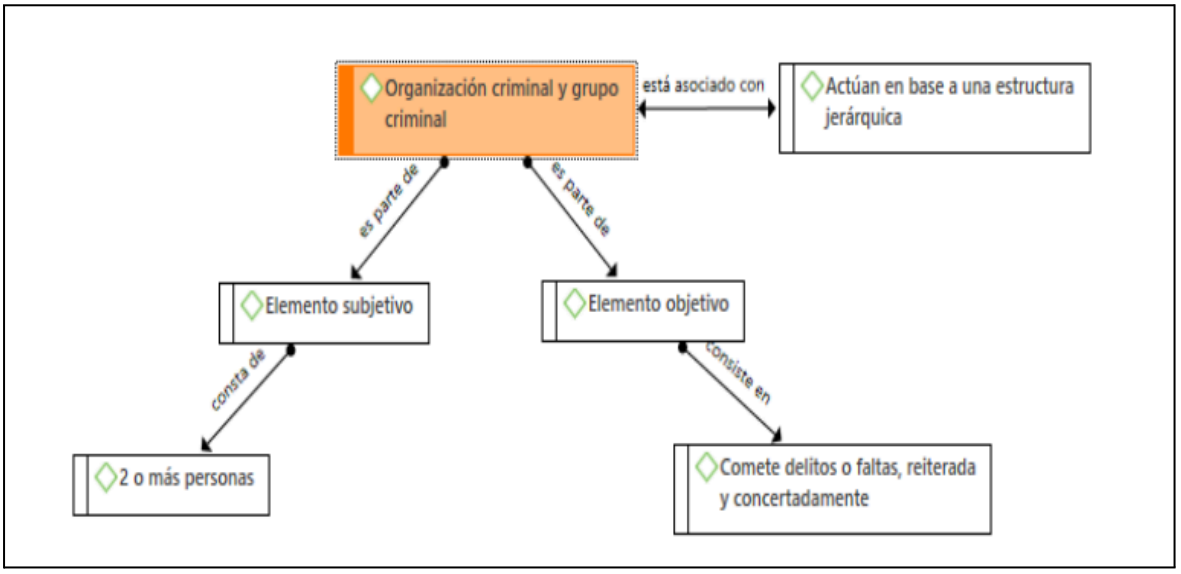

Figura 01: Organización criminal y grupo criminal

En la R.N No. 206-2019, se aclara que el delito cibernético patrimonial es "la comisión de delitos con contenido patrimonial mediante el uso de la tecnología de la información en la que se obtienen números de tarjetas bancarias a través de una réplica de una página web." Esta conducta ilícita se denomina Phishing, que se utiliza comúnmente para obtener números de tarjetas y códigos de seguridad. El robo mediante sistemas informáticos se

configura como "... la tarjeta constituye la llave que, al insertarse en la máquina, activa el mecanismo que dispensa el dinero" según lo especificado en la Sentencia No. 00763/2006 de España. En este sentido, se reconoce que la tarjeta de crédito o débito funciona como una llave metálica. En consecuencia, la víctima no recibió ningún beneficio patrimonial en caso de que el acusado proporciona el PIN de la tarjeta mediante alguna forma de manipulación. Esto se debe a que la acción del acusado de retirar dinero del cajero automático sin el conocimiento de la víctima constituye la desposesión de su propiedad.

Con respecto al número de referencia CAS 956-2017 Lambayeque, se observó en el expediente penal con el número 7061-2008 que el Banco Continental no ha sido declarado culpable de responsabilidad penal en relación con el delito de robo agravado, en particular la retirada ilegal de fondos de la cuenta bancaria de un cliente. En pocas palabras, si el banco ofrece recomendaciones de seguridad a través de boletines, no puede ser legalmente responsable de un delito cibernético. Esto implica que el banco no puede ser responsabilizado en términos civiles o penales si informa a los consumidores de las medidas de seguridad necesarias para las transacciones en línea en su sitio web y el cliente descuida el certificado de autenticación doble.

2.2. MARCO CONCEPTUAL

2.2.1. DELITO INFORMÁTICO

Se refiere a aquellas actividades delictivas que se cometen utilizando computadoras, redes o dispositivos tecnológicos. Incluye una amplia gama de acciones ilegales como el acceso no autorizado a sistemas informáticos, la manipulación de datos, el robo de información confidencial, entre otros.

2.2.2. MEDIOS PROBATORIOS

Se refiere al conjunto de instrumentos o recursos legales que permiten acreditar la existencia de un hecho o derecho en un proceso jurídico. En el contexto de delitos informáticos, incluye todo tipo de evidencia digital como registros de sistemas, correos electrónicos, archivos digitales, etc.

2.2.3. VALIDEZ DE LA PRUEBA DIGITAL

Es la aceptación de un dato o registro electrónico como prueba dentro de un procedimiento legal, basado en su autenticidad, integridad y cumplimiento de los estándares legales aplicables para su adquisición, almacenamiento y análisis.

2.2.4. ACCESO ILEGÍTIMO

Acto de ingresar sin autorización a sistemas informáticos, redes o dispositivos, con o sin la intención de causar daño o extraer información. Este acto es considerado un delito informático bajo la legislación de muchos países.

2.2.5. INTERCEPTACIÓN ILEGAL

La captura o adquisición no autorizada de transferencias de datos entre sisteas informáticos, típicamente utilizada para obtener información confidencial o propiedad intelectual sin permiso.

2.3. MARCO LEGAL Y/O JURISPRUDENCIAL

MARCO NORMATIVO

El marco normativo sobre delitos informáticos en Perú y, por extensión, en el departamento de Puno, se fundamenta en diversas disposiciones y leyes que buscan prevenir, sancionar y erradicar estos actos dentro del espacio digital. A continuación, se detallan las principales normativas aplicables:

Ley N° 30096, Ley de Delitos Informáticos,

Esta ley define y sanciona diversas conductas delictivas cometidas a través de sistemas y tecnologías de información, como el acceso ilegítimo, interceptación ilegal de comunicaciones, ataque a la integridad de datos, fraude informático, entre otros.

Decreto Legislativo N° 635, Código Penal Peruano (modificaciones pertinentes)

Integración en el Código Penal de las modificaciones relacionadas con los delitos informáticos, clasificando y describiendo las penas asociadas a cada tipo de delito computarizado.

Ley Nº 29733, Ley de Protección de Datos Personales

Protege la privacidad de los individuos respecto al tratamiento de sus datos personales en sistemas de información, tanto privados como públicos, y establece las bases para garantizar este derecho.

Decreto Supremo Nº 019-2013-JUS, Reglamento de la Ley de Protección de Datos Personales

Desarrolla y precisa los criterios para la aplicación efectiva de la Ley de Protección de Datos Personales, incluyendo procesos relacionados con la seguridad de la información.

Ley N° 28256, Ley que regula el uso de la tecnología para la transparencia en la gestión pública

Esta ley enfatiza la transparencia y acceso público a la información del Estado mediante el uso de las tecnologías de información.

Directivas emitidas por el Instituto Nacional de Estadística e Informática (INEI) y el Ministerio de Justicia y Derechos Humanos

Establecen procedimientos y protocolos para la gestión y protección de datos dentro del ámbito de la administración pública y otras entidades.

Aplicabilidad Local en Puno

A nivel de Puno, la implementación de estas leyes y regulaciones se realiza a través de las instituciones locales y regionales, como la Prefectura, la Policía Nacional del Perú (especialmente la división de delitos informáticos) y el Poder Judicial en la región. La adaptación local implica también la capacitación y el entrenamiento de funcionarios y operadores de justicia para enfrentar este tipo de delitos, a menudo con el apoyo de programas nacionales o iniciativas de cooperación técnica.

Este marco normativo está sujeto a evoluciones constantes debido a la dinámica propia de los delitos informáticos y los avances tecnológicos, lo que requiere de actualizaciones periódicas para enfrentar nuevos retos y amenazas dentro del espacio digital.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1 ZONA DE ESTUDIO

A nivel nacional

3.2. POBLACIÓN Y MUESTRA

Población

Todos los abogados que practican en el departamento de Puno y que han trabajado en casos de delitos informáticos.

Muestra

Una selección representativa de estos abogados, teniendo en cuenta factores como experiencia, especialización en derecho penal o tecnológico, y disposición para participar en el estudio.

Muestreo

Se utilizará un muestreo por conveniencia, seleccionando participantes disponibles y dispuestos a contribuir al estudio. Se considerará también el uso de muestreo intencionado para asegurar la inclusión de abogados con experiencia significativa en delitos informáticos.

3.3. TIPO Y NIVEL DE INVESTIGACIÓN.

Tipo de investigación

Cualitativa. Este enfoque se elige debido a que permite una comprensión profunda de las percepciones, opiniones y experiencias de los profesionales del derecho en Puno sobre la valoración de medios probatorios en delitos informáticos.

Nivel de investigación

Descriptivo. El estudio describe las prácticas actuales, dificultades y estrategias utilizadas por los abogados en la evaluación de evidencias digitales en casos de delito informático.

Enfoque

Es enfoque cualitativo.

3.4. DISEÑO DE INVESTIGACIÓN

El diseño de la investigación será no experimental y transversal. Se recogerán datos en un momento específico en el tiempo para analizar y describir características y variables sin manipulación de las mismas. El enfoque será principalmente descriptivo e interpretativo, utilizando análisis cualitativo para profundizar en las percepciones y experiencias de los participantes.

3.5. CATEGORÍAS-EJES DE ANÁLISIS, SUB CATEGORÍAS-SUB EJES DE ANÁLISIS

Evaluación de la Evidencia Digital:

Subcategorías:

- Autenticidad
- Integridad
- Admisibilidad

Desafíos en la Valoración de Evidencia:

Subcategorías:

- Capacitación técnica
- Limitaciones tecnológicas
- Marco legal

Impacto en la Justicia:

Subcategorías:

- Efectividad del proceso judicial
- Tiempos de resolución
- Percibida justicia en los fallos

3.6. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Técnicas

Entrevistas semiestructuradas: Permitirán obtener datos profundos y detallados sobre las percepciones y experiencias de los abogados con respecto a la valoración de evidencia digital.

Instrumento

Guía de entrevista: Un documento que incluirá preguntas abiertas diseñadas para explorar las categorías y subcategorías definidas. Las preguntas buscarán explorar cómo los abogados evalúan la evidencia digital, los desafíos que enfrentan y el impacto de estos procesos en la justicia de casos de delitos informáticos.

3.7. TÉCNICAS E INSTRUMENTOS DE ANÁLISIS Y/O INTERPRETACIÓN DE DATOS

Para el análisis de los datos recolectados se utilizó el análisis cualitativo de contenido, el cual permitió interpretar las respuestas obtenidas en las entrevistas a los abogados especialistas en derecho penal. Se aplicó una codificación temática para identificar patrones y categorías relevantes en la información obtenida.

3.8. MÉTODOS DE INVESTIGACIÓN.

El presente estudio se basa en un método de investigación cualitativo, utilizando el enfoque fenomenológico para comprender la percepción y experiencia de los abogados en la valoración de medios probatorios en delitos informáticos. Asimismo, se aplicará el método analítico-sintético para descomponer la información recolectada, identificar relaciones entre las categorías de análisis y sintetizar los hallazgos en función de los objetivos de la investigación.

3.9. DELIMITACIÓN DOCUMENTAL DE LA INVESTIGACIÓN.

La investigación se limita documentalmente a fuentes bibliográficas y normativas relacionadas con la valoración de medios probatorios en delitos informáticos. Se han utilizado entrevistas como principal fuente de información, complementadas con estudios previos, jurisprudencia relevante y normativas vigentes.

CAPÍTULO IV

EXPOSICIÓN Y ANÁLISIS DE RESULTADOS

4.1 ANÁLISIS DE RESULTADOS

El Capítulo IV, titulado "Exposición y Análisis de Resultados", presenta los hallazgos obtenidos a través de la aplicación de técnicas e instrumentos de recolección de datos, en concordancia con los objetivos planteados en la investigación.

El objetivo principal de este capítulo es analizar la información recopilada para determinar qué se necesita en el departamento de Puno para obtener medios probatorios que sean obligatorios en los procesos relacionados con delitos informáticos.

El análisis se basa en las respuestas de los participantes a las preguntas formuladas en las entrevistas, abordando temas como los factores que obstaculizan las investigaciones en delitos informáticos, la disponibilidad de recursos para los fiscales, los medios probatorios necesarios para acreditar los delitos informáticos, y la relación entre los delitos de hurto y estafa en el contexto de los delitos informáticos.

Los resultados se presentan de manera organizada, relacionando cada pregunta con los objetivos específicos de la investigación y contrastando las opiniones de los participantes con la información proporcionada por diversos autores y normativas legales. El capítulo busca proporcionar una comprensión detallada de la situación actual en el departamento de Puno en relación con la valoración de medios probatorios en delitos informáticos, identificando las principales necesidades y desafíos que enfrentan los operadores de justicia.

ANÁLISIS DE RESULTADOS

El enfoque y el instrumento de recolección de datos fueron aplicados, y la información fue procesada en alineación con los objetivos de la investigación. En este contexto, los resultados relacionados con el objetivo general 1, que es determinar los requisitos en el distrito de Puno para obtener pruebas consideradas esenciales en los procesos relacionados con el cibercrimen, llevaron a la formulación de las siguientes preguntas:

1. ¿Qué factores obstaculizan las investigaciones en los delitos informáticos?

Los sujetos de estudio destacaron que las investigaciones vinculadas a delitos informáticos se ven dificultadas por la insistencia del acusado, la insuficiencia de datos en las denuncias, la falta de información proporcionada por el acusado, dado que se le convoca para proporcionar declaraciones adicionales sobre los eventos y no se presenta para proporcionar la información requerida, la ausencia de fiscalías especializadas, la insuficiente coordinación entre las fuerzas del orden y la fiscalía, la ausencia de logística y apoyo durante los periodos de flagrancia, la falta de inmediatez, y la falta de un conocimiento adecuado de la normativa.

Herrera (2021) postula que los problemas asociados con los delitos informáticos incluyen el anonimato o la dificultad para identificar a los perpetradores. Estos problemas se manifiestan en casos de hacking, utilización de datos falsos para crear cuentas falsas en redes sociales, con el objetivo de engaño a la víctima para obtener una ventaja patrimonial (estafa). En el contexto de organizaciones delictivas, se enfocan en el tráfico de datos, el fraude en cuentas bancarias utilizando a terceros, y estas personas capturan a otras personas que realicen transacciones bancarias, como transferencias, depósitos y retiros. Un desafío significativo radica en que la legislación puede resultar inadecuada para ejercer un efecto intimidatorio sobre el potencial infractor. Por lo tanto, se requiere una revisión y adaptación en función de la severidad del bien jurídico perjudicado, y contemplar medidas agravadas que legitimen la sanción. En el caso del fraude informático, donde la legislación no contempla sanciones agravadas para los miembros de organizaciones o bandas delictivas, existe una falta de claridad en la legislación.

2.¿Los fiscales cuentan con los recursos necesarios para realizar investigaciones completas de los delitos informáticos?

La respuesta a esta interrogante presenta posturas divergentes, dado que existen respuestas que sostienen que la fiscalía posee los recursos necesarios para investigar el delito gracias a la presencia de la unidad de Divindat. Sin embargo, también existen posturas que sostienen que la utilización de la unidad de Divindat como herramienta para la persecución del delito no es suficiente, dado que dicha unidad no se ubica en el distrito de Puno. Asimismo, se postula que la insuficiencia de conocimientos en herramientas de tecnologías de la información representa un recurso insuficiente, y la ausencia de una fiscalía especializada con individuos con habilidades en el uso y gestión de herramientas tecnológicas, así como en el manejo de software, resulta un obstáculo.

Izquierdo (2021) llegó a la conclusión de que la ciberdelincuencia económica constituye un delito de elevada complejidad y riesgo, atribuible al uso indebido de tecnologías informáticas, tal como se evidenció en el caso de los bonos familiares proporcionados por el estado peruano durante el período de la pandemia sanitaria.

3.¿Qué medios probatorios se necesitan para acreditar los delitos informáticos?

Englobando las respuestas de los participantes, indicaron que se necesita de un expediente completo de la comisaría, queja en el banco por las transferencias realizadas sin consentimiento del agraviado, expediente del banco, declaración del agraviado, movimientos bancarios, estados de cuenta, capturas de pantalla, equipos tecnológicos, verificación de correos electrónicos.

Alan (2017) indica que la obtención de información, como los elementos de prueba en una investigación criminal, exige que los investigadores encargados, preserven, analicen y presenten la evidencia digital garantizando la autenticidad e integridad presentada por el fiscal en el juicio oral.

- La evidencia digital puede encontrarse almacenada en dispositivos informáticos, por ejemplo, memoria RAM, discos rígidos, tráfico de datos, por ello se ha clasificado en tres grupos la evidencia digital: a) Sistemas de computación abiertos, computadoras

personales y sus servidores, b) Sistemas de comunicación, compuestos de las redes de telecomunicaciones, comunicación inalámbrica e internet y c) Sistemas convergentes de computación, teléfonos celulares inteligentes, asistentes personales digitales, tarjetas inteligentes.

Por lo que la información que se necesita como medios de pruebas son obtenidos de programas almacenados, mensajes de datos transmitidos usando el sistema informático, tarjetas de memoria, USB, discos portátiles, historial de navegación de internet, chats de internet, listas de registros, fotografías en distintos formatos de archivos, archivo de imágenes, documentos, archivos de texto, metadatos de archivos, claves de memoria, claves de encriptación, Sistemas de posicionamiento global, video filmadoras, localizador, cámaras de seguridad, listado de llamadas, mensajes recibidos y enviados, páginas de internet visitadas por el agraviado, datos de localización geográfica, aplicaciones de software, mensajes de correos.

Toda incautación de dispositivos de almacenamientos externos deberá estar específicamente detallada en la orden de allanamiento expedida por el juez a pedido del fiscal. Como posibles evidencias físicas pueden ser documentos impresos, impresiones dactilares, ADN, a fin de vincular al usuario con el dispositivo digital incautado

Respecto al aseguramiento de la escena del delito, esta será llevada a cabo por policías judiciales que cuenten con conocimiento técnico avanzado en el manejo de evidencia digital. Una forma de poner una barrera de protección es mediante Direwire, Ethernet.

En cuanto al objetivo específico 2

¿Qué relación tiene el delito de hurto y estafa en los delitos informáticos?, se plantearon las siguientes preguntas:

4. ¿Considera que dentro de los delitos informáticos se encuentran también los delitos de estafa y hurto?

En respuesta a la interrogante planteada, un conjunto de participantes concordó en que los delitos de estafa y hurto se clasifican dentro de los delitos informáticos debido a su impacto directo en el patrimonio. No obstante, otro conjunto de participantes expresó que, aunque las

herramientas tecnológicas se emplean para la extracción de bienes económicos, estas constituyen un "instrumento" para alcanzar los objetivos delictivos, los delitos de estafa y hurto no se categorizan dentro de los delitos informáticos.

Acosta et al. (2020) postulan que los delitos de hurto y estafa se caracterizan por la creación y activación de diversas estrategias que facilitan el delito, comprometiendo de forma efectiva la privacidad e identidad de cualquier individuo.

5. En su experiencia ¿Los bancos colaboran de alguna forma en las investigaciones relacionadas a los delitos informáticos?

Solo cuando se solicita el levantamiento del secreto bancario, cuando el usuario da su autorización para un informe de sus cuentas bancarias, la demora de la información solicitada a los bancos perjudica la flagrancia.

Matos (2022), propuso como una acción complementaria, establecer un convenio entre la entidad bancaria, el Ministerio Público y la Policía Nacional del Perú para facilitar información inmediata al usuario y señala dentro de sus conclusiones que no existe una buena articulación entre las entidades bancarias, PNP y Ministerio público.

Sin embargo, por la acreditación del delito de hurto dentro de los informáticos no es posible, dado que, si bien no existe una figura jurídica como hurto informático, para este delito se requiere de un medio físico para su comisión, aunque en países como Venezuela, Costa Rica, y en España si este esta figura jurídica al considerar hurto informático a la forma en que logra despojar del patrimonio a una persona jurídica o natural, sin la necesidad de emplear un medio tecnológico.

Parra (2019), señala que el proceso judicial se debe fortalecer con garantías procesales para la prueba digital, las fuentes de prueba son las herramientas que el juez utiliza para verificar hechos facticos, los medios de prueba es parte de, como testigos, documentos, conocimiento técnico del perito. La valoración probatoria en la evidencia digital debe cumplir con los requisitos intrínsecos de la prueba como la utilidad, conducencia y pertinencia.

Las IOCE, el digital forensic research workshop, se establecen lineamientos internacionales para recabar evidencia en medios electrónicos.

En el artículo 248.2 de la legislación penal española, se definen como reos de estafa a aquellos individuos que, mediante alguna manipulación informática, obtienen transferencias no autorizadas de cualquier patrimonio en detrimento de otro, así como a aquellos que proporcionan programas informáticos con el propósito de realizar operaciones de cualquier tipo en detrimento de su titular o de un tercero.

En el marco jurídico venezolano, la estafa se define como la manipulación de sistemas y la manipulación de la información contenida en ellos, con el objetivo de introducir instrucciones falsas o fraudulentas que resulten en un resultado en perjuicio de terceros.

La comisión del hurto ocurre cuando, mediante el empleo de tecnologías de la información y la comunicación (TIC), se accede, manipula, intercepta o interfiere de cualquier manera en un sistema o medio de comunicación con la finalidad de apropiarse de recursos patrimoniales económicos ajenos.

En el Artículo 217 del Código Penal de Costa Rica, la Estafa Informática se define como cuando un individuo manipula o afecta el resultado de los datos de un sistema automatizado de información, empleando datos falsos o incompletos, o programándolos para llevar a cabo una operación informática o artificio tecnológico, o por cualquier otra acción que transgredan el procesamiento de los datos del sistema o que resulten en información falsa, incompleta o fraudulenta, con el objetivo de obtener un beneficio patrimonial o indebido para sí mismo o para terceros.

6. ¿Qué medidas necesita adoptar el Ministerio Público y la Policía Nacional del Perú para aplicar la norma en relación a los delitos informáticos?

Es fundamental promover una mayor colaboración y cooperación en el proceso de indagación con el fin de recopilar información precisa y detallada. Es imprescindible mantenerse actualizado y familiarizado con el uso de las herramientas tecnológicas de las TICs, así como contar con una división especializada en el área de investigación. Es necesario que la legislación existente brinde una cobertura más amplia y efectiva para facilitar y agilizar los procedimientos investigativos. Asimismo, se requiere contar con equipos de última generación que permitan un acceso más rápido y eficiente a la

información relevante. Es importante concientizar a la población sobre los riesgos de caer en estafas a través de enlaces fraudulentos.

Virú y sus colegas (2018) sugieren encarecidamente la necesidad de establecer y poner en marcha sistemas de seguridad avanzados y eficaces, con el objetivo de mantenerse al día y preparados para hacer frente a las cada vez más frecuentes y sofisticadas amenazas de ciberataques. Es evidente que la falta de actualización y adaptación de las normativas legales vigentes está generando un estancamiento preocupante en el desarrollo del comercio electrónico, lo cual a su vez está contribuyendo a aumentar los niveles de inseguridad y desconfianza en la población en general. En ese sentido, Alan (2017) destaca la importancia fundamental de consolidar y fortalecer la colaboración y comunicación entre los cuerpos policiales y los representantes del Ministerio Público, con el propósito de establecer y ejecutar de manera conjunta una estrategia integral de investigación, la cual se llevará a cabo mediante una estrecha colaboración y coordinación entre ambas partes.

7. ¿Qué deficiencias cree usted que existen en las investigaciones preliminares en los casos de delitos informáticos?

La falta de conocimiento por parte de los usuarios al momento de presentar su denuncia por suplantación de identidad es evidente. Muchas veces, los usuarios no brindan detalles adicionales que podrían ser de gran ayuda para las autoridades encargadas de la investigación. Además, la falta de un seguimiento adecuado por parte de las autoridades contribuye a la impunidad en estos casos. Es preocupante la carencia de laboratorios tecnológicos especializados para llevar a cabo investigaciones descentralizadas. Esta situación dificulta el proceso de descongestión de la central de denuncias, lo que a su vez afecta la eficacia de las investigaciones. Otro aspecto a considerar es la escasez de equipos informáticos adecuados para llevar a cabo las investigaciones de forma eficiente. La falta de recursos tecnológicos adecuados limita la capacidad de las autoridades para rastrear y recopilar pruebas de manera oportuna. Adicionalmente, la demora por parte de los bancos en la entrega de informes solicitados por la fiscalía es un problema recurrente. En algunos

casos, esta demora puede extenderse por más de tres meses, lo que ralentiza significativamente el avance de las investigaciones y la impartición de justicia.

Dando una mayor precisión y profundidad en sus recomendaciones, Ávalos (2021) sugiere la implementación de órganos de apoyo técnicos descentralizados, el suministro de equipamiento especializado para labores de análisis forense informático. Además, propone la creación de una base de datos integral que contenga las pericias de análisis digital forense, así como la descentralización del área de análisis digital forense mediante la creación de unidades en distritos fiscales con una alta demanda de casos. Todo esto con el objetivo de disminuir la carga de requerimientos en Lima y agilizar los procesos de análisis forenses. Asimismo, se destaca la importancia de diseñar y ejecutar programas de capacitación extensos y detallados dirigidos al personal administrativo, peritos forenses y fiscales penales.

8. ¿Cree usted que faltan capacitaciones y/o actualizaciones en las herramientas de las TICs para imputar los delitos informáticos?

Todos los participantes en la reunión estuvieron de acuerdo en que es necesario brindar capacitaciones especializadas en el manejo de herramientas de las Tecnologías de la Información para investigar los delitos informáticos. Esto se refleja claramente en el aumento de denuncias por delitos informáticos que lamentablemente acaban archivadas debido a la falta de conocimiento técnico en la materia.

En su investigación de posgrado realizada en el año 2021, Carrera llegó a la conclusión de que la carencia de conocimientos y competencias en el ámbito de la investigación se origina en la incorrecta aplicación de la normativa vigente, por lo cual sería pertinente considerar la incorporación de nuevos apartados que abordan de manera detallada el tema de la ciberseguridad. Asimismo, señaló que la falta de una adecuada coordinación entre la fiscalía y la policía nacional del Perú obstaculiza la implementación de medidas efectivas para la identificación de los responsables de los delitos informáticos.

9. En su experiencia ¿Cree usted que se puede tipificar el hurto informático?

Las respuestas proporcionadas por los participantes indicaron que, según la comisión del hurto, este delito necesita de un medio físico para alcanzar su propósito, y el uso de una herramienta tecnológica implica un acceso no autorizado y la apropiación indebida de bienes. El hurto se clasifica como un delito contra el patrimonio y, según las autoridades competentes, no puede ser catalogado como un delito informático debido a su naturaleza especial, ya que se lleva a cabo a través de sistemas informáticos. Un reducido grupo minoritario de participantes expresaron su opinión sobre si se les debería considerar como parte de un delito informático o no.

10. En su experiencia ¿Cree usted que se puede tipificar el delito de estafa dentro de los delitos informáticos?

Un grupo minoritario de participantes indicó que, en su opinión, sí se puede tipificar el delito de estafa dentro de los delitos informáticos, mientras que el otro grupo sostuvo que no se puede tipificar debido a que poseen principios diferentes para su comisión. No obstante, todos estuvieron de acuerdo en que sería conveniente modificar la normativa con el objetivo de que sea más precisa en lo que respecta a la comisión de estafa. Consideran que, si bien se han llevado a cabo estafas a través de herramientas tecnológicas, estas cumplen con la finalidad del "delito de estafa" al lograr engañar a un usuario y proporcionarle una percepción errónea de la realidad.

En el artículo 248 del Código Penal de la Legislación Española, se establece que serán considerados como autores de estafa aquellos individuos que, sin tener intención de obtener beneficio económico y recurriendo a algún tipo de engaño informático o artimaña similar, logren la transferencia de activos patrimoniales sin el consentimiento de la persona perjudicada.

DISCUSIÓN

En las conclusiones, se determinó, en consonancia con el objetivo general de la investigación, la necesidad de equipos tecnológicos, laboratorios forenses informáticos, peritos informáticos, policías y fiscales con conocimiento en evidencia digital para obtener medios probatorios. Esto se alinea con los antecedentes que señalan la falta de capacitación

en herramientas tecnológicas como un obstáculo significativo en las investigaciones. Respecto al primer objetivo específico, se concluyó que en las investigaciones preliminares se requiere una mejor coordinación entre fiscalía y policía nacional, actualización en el uso de TICs, una división especializada en delitos informáticos, mejor cobertura legal, equipos de primera generación, mayor presencia del recurrente, laboratorios tecnológicos, una base de datos con información de las pericias forenses digitales, y capacitación. Esto refuerza la idea planteada por Mori (2019) sobre la disparidad de opiniones entre jueces y fiscales respecto a la capacitación en herramientas tecnológicas. En cuanto al segundo objetivo específico, la investigación determinó que el hurto requiere un medio físico para su comisión, mientras que las herramientas tecnológicas pertenecen a un acceso ilícito. Respecto al delito de estafa, se concluyó que debería incluir todo tipo de manipulación, incluyendo la informática, para engañar y obtener un beneficio económico, tal como se indica en el código penal de la legislación española. Esto se relaciona con los antecedentes que mencionan que los delitos de estafa y hurto sí se encuentran dentro de los delitos informáticos porque afectan directamente al patrimonio.

CONCLUSIONES

Primera: Se determinó que se necesitan equipos tecnológicos, laboratorios forenses informáticos, peritos informáticos, policías y fiscales con conocimiento en evidencia digital a fin de obtener medios probatorios como los que se encuentran almacenados en dispositivos informáticos y sus análogos.

Segunda: Se determinó que en las investigaciones preliminares se necesitan una mejor coordinación entre fiscalía y policía nacional del Perú, mayor colaboración en la indagación para recopilar información, el Ministerio público necesita actualizarse con el uso de herramientas de las TICs, también necesita de una división especializada en delitos informáticos, y que la ley tenga mejor cobertura para proceder con las investigaciones, un procedimiento específico, equipos de primera generación, mayor presencia del recurrente cuando se le solicita, laboratorios tecnológicos, base de datos con información de las pericias de análisis digital forense solicitadas y desarrolladas, capacitación a fiscales y policía nacional del Perú, y capacitaciones en el uso de herramientas de las Tics.

Tercera: La comisión del hurto, requiere de un medio físico para su objetivo, y las herramientas tecnológicas pertenecen a un acceso ilícito, en cuanto al delito de estafa el cual consiste en engañar, también debería consistir en todo tipo de manipulación pudiendo ser esta también informática u otro artificio semejante a fin de engañar y tener un beneficio económico, como también lo indica en el código penal de la legislación española.

RECOMENDACIONES

Primera: Capacitar y evaluar los conocimientos tanto de la Policía nacional como del Ministerio Público en función a delitos informáticos, asimismo que se analice una futura modificatoria a la Ley N° 30096 a fin que sea más exacta en cuanto a su aplicación relacionada al delito de estafa y la nuevas formas de delinquir mediante herramientas tecnológicas en donde también se consideren los tiempos en flagrancia a fin de que la ley tenga mejor cobertura para proceder con las investigaciones.

Segunda: en relación al instrumento, se recomienda Implementar sistemas de ciberseguridad como Direwire, Ethernet, concientizar a la población para que no caiga en estafas de links, e indicar un plazo de rendir informes o lo solicitado a las entidades bancarias bajo apercibimiento de una multa y amonestación económica

Tercera: en relación a la realidad problemática, se recomienda que en el distrito de Puno los fiscales y policía nacional cuenten con herramientas tecnológicas para perseguir el delito, estén capacitados en la aplicación de la norma, y en el manual de evidencia digital del cual no tienen conocimiento. Mejor apoyo y coordinación en las investigaciones preliminares dado que estas se obstaculizan debido a la falta de persistencia del recurrente, falta de información en las denuncias, falta de fiscalías especializadas, falta de logística y apoyo en flagrancia.

BIBLIOGRAFÍA

Acosta, M., Benavides, M., & Garcia, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. Revista Venezolana de Gerencia, vol. 25, núm. 89, 2020.

Aviles Avalos, G. E. *Necesidad de ampliar la penalización de los delitos informáticos en Bolivia referentes a estafa electrónica* (Doctoral dissertation).

Atienza Rodríguez, Manuel. (2016). Un tratado sobre la justificación jurídica. (P. Grández Castro, Ed.) Palestra Editores S.A.C. Obtenido de https://books.google.com.pe/books?id=46HNDwAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Ávalos Rivera, Z. (2021). Ciberdelincuencia: Pautas para una investigación fiscal especializada. Perú: Ministerio público - Informe de análisis N° 04.

Ávila, M. G. (2002). Ética y formación universitaria. Obtenido de https://rieoei.org/historico/documentos/rie29a04.htm

Bascur, G., & Peña, R. (2022). Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459. Primera parte. *Revista de Estudios de la Justicia*, *37*, 1-38.

Baena Paz, G. (2017). Metodología de la investigación (tercera edición ed.). Grupo editorial Patria . Obtenido de http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/metodologia%20de%20la%20investigacion.pdf

Carrera Peña, I. d. (2021). Deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021. Obtenido de https://repositorio.ucv.edu.pe/handle/20.500.12692/71492#:~:text=Como%20resultado

Cisternas Hernández, E. A., & Moyano Montecino, J. (2017). *Analisis y proyeccion de los delitos informaticos en Chile* (Doctoral dissertation, Universidad de Talca (Chile). Escuela de

Derecho).%20se%20pudo%20determinar,cuenta%20con%20un%20respaldo%20nor mativo.

Eneken Tikk, M. K. (2020). Routledge Handbook of International Cybersecurity. Routledge

Española, L. (s.f.). Ley Orgánica 10/1995 Código Penal. Obtenido de https://confilegal.com/20170710-codigo-penal-espanol-actualizado/

Galeano, M. (2020). Diseño de proyectos en la investigación cualitativa. Universidad Eafit. Obtenido de https://books.google.com.pe/books?id=Xkb78OSRMI8C&dq=enfoque+cualitativo&source=gbs_navlinks_s

Hernández León, R., & Coello Gonzáles , S. (2012). El proceso de investigación cientifica. La Habana: Editorial Universitaria. Obtenido de https://books.google.com.pe/books?id=tX71DwAAQBAJ&pg=PA19&dq=las+teor%C3%ADas+gu%C3%ADan+los+procesos+de+investigaci%C3%B3n&hl=es-419&sa=X&ved=2ahUKEwiUndThlNT3AhUgtJUCHU6tBBMQ6AF6BAgCEA I#v=onepage&q&f=false

Herrera, E. Z. (17 de Mayo de 2021). Delitos informáticos: ¿nuevas formas de criminalidad? Obtenido de https://www.deleyes.pe/articulos/delitos-informaticos-nuevas-formas-decriminalidad.

Landeau, R. (2007). Elaboración de trabajos de investigacion. Editorial Alfa 2007. Obtenido de https://books.google.com.pe/books?id=M_N1CzTB2D4C&printsec=frontcover&dq=aspectos+administrativos+en+tesis&hl=es-419&sa=X&ved=2ahUKEwjMroyQjPH3AhVvrpUCHbcKBksQ6AF6BAgDEAI #v=onepage&q&f=false

Lariguet, G. (2019). Metodología de la investigación jurídica. Editorial Brujas 2019. Obtenido de https://books.google.com.pe/books?id=J8SWDwAAQBAJ&dq=teorias+de+investigacion+en+el+derecho&source=gbs_navlinks_s

León, I. H., & Garrido, J. T. (2007). Paradigmas y métodos de investigación en tiempos de cambio. Los libros de El Nacional, colección Minerva, Editorial CEC, SA (2007).

Obtenido de https://books.google.com.pe/books?id=pTHLXXMa90sC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Ley N° 30096 (22 de Octubre de 2013). Diario el Peruano. Obtenido de Ley de delitos informáticos: https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

Lobo, M. M., Gil, S. V. H., & Aguirre, A. M. G. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. *Revista de ciencias sociales*, *29*(2), 356-372.

Mayer Lux, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Ius et Praxis*, *24*(1), 159-206.

Rivera, N. E. E. Los delitos informáticos en Bolivia. Una propuesta para la implementación de un juzgado de informática.

Temperini, M. G. I. (2013). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. In *1er. Congreso Nacional de Ingeniería Informática/Sistemas de Información*.

ANEXOS

Anexo 01: Matriz de Consistencia

TÍTULO	PROBLEMA	OBJETIVOS	CATEGORÍAS	METODOLOGÍA Y DISEÑO
VALORACIÓN DE MEDIOS PROBATORIOS EN DELITOS INFORMÁTICOS EN EL DEPARTAMENTO DE PUNO 2023	**GENERAL** ¿Qué se necesita en el distrito de puno para obtener medios probatorios que ameriten ser obligatorios en los procesos relacionados a delitos informáticos?	**GENERAL** Determinar que se necesita en el departamento de Puno, para obtener medios probatorios que ameriten ser obligatorios en los procesos relacionados a delitos informáticos.	Medios Probatorios	**TIPO O MODELO DE INVESTIGACIÓN** Cualitativo
	ESPECÍFICO ¿Qué se necesita para continuar con la investigación preparatoria en los casos relacionados a delitos informáticos? ¿Qué relación tienen el delito de hurto y el delito de estafa en los delitos informáticos?	**ESPECÍFICO** Determinar qué se necesita para continuar con la investigación preparatoria en los casos relacionados a delitos informáticos. Determinar qué relación tienen el delito de hurto y el delito de estafa en los delitos informáticos.	**INDEPENDIENTE** Delitos Informaticos	**METODOLOGÍA O ENFOQUE DE INVESTIGACIÓN**

Anexo 02: Instrumento

Tema	Resultados Clave
Obstáculos en Investigaciones	Falta de persistencia del recurrente y de información en las denuncias. Falta de fiscalías especializadas y coordinación entre policías y fiscalía. Falta de logística y apoyo en tiempos de flagrancia, así como de conocimiento de la norma. Anonimato de los actores en delitos como el hackeo y uso de datos falsos para estafas. Insuficiencia de la ley para intimidar a los delincuentes y falta de claridad en las formas agravadas del fraude informático.
Recursos de los Fiscales	Opiniones divididas sobre si la fiscalía cuenta con los recursos necesarios. La unidad de Divindat no es suficiente y no está presente en todos los distritos. Falta de conocimiento en herramientas de tecnologías de la información y peritos informáticos. Necesidad de una fiscalía especializada con personal capacitado en tecnologías y software para investigaciones.
Medios Probatorios Necesarios	Expediente completo de la comisaría y del banco. Declaración del agraviado, movimientos bancarios y estados de cuenta. Capturas de pantalla, equipos tecnológicos y verificación de correos electrónicos. Evidencia digital almacenada en dispositivos informáticos, como memoria RAM, discos rígidos y tráfico de datos. Información obtenida de programas almacenados, mensajes de datos, tarjetas de memoria, historial de navegación, chats, fotografías, etc..
Hurto y Estafa en Delitos Informáticos	Opiniones divididas sobre si la estafa y el hurto se encuentran dentro de los delitos informáticos. Algunos consideran que las herramientas tecnológicas son un "medio" para lograr los objetivos delictivos, pero no son delitos informáticos en sí mismos. Otros coinciden en que sí se encuentran dentro de los delitos informáticos porque afectan directamente al patrimonio.
Colaboración de los Bancos	La colaboración se limita al levantamiento del secreto bancario o la autorización del usuario. La demora en la entrega de información por parte de los bancos perjudica la flagrancia. Falta de articulación

	entre entidades bancarias, la Policía Nacional y el Ministerio Público.
Medidas Necesarias	Mayor colaboración en la indagación y actualización en el uso de TICs. División especializada, mejor cobertura legal y equipos de primera generación. Concientización a la población sobre estafas en links.
Deficiencias en Investigaciones Preliminares	Falta de conocimiento de los usuarios al denunciar suplantación de identidad. Los usuarios no dan mayores declaraciones y no hay seguimiento respectivo. Carencia de laboratorios tecnológicos descentralizados y falta de equipos informáticos. Demora de los bancos en los informes solicitados por la fiscalía.
Capacitación en TICs	Todos los participantes coinciden en la falta de capacitación en el uso de herramientas de las TICs para imputar delitos informáticos. Muchas denuncias por delitos informáticos terminan siendo archivadas por esta razón. Falta de conocimiento y dominio en la investigación debido a la mala aplicación de la normativa.
Tipificación del Hurto Informático	Para la comisión del hurto, se requiere un medio físico, mientras que las herramientas tecnológicas pertenecen a un acceso ilícito. El delito de hurto es contra el patrimonio y no se le puede calificar dentro de un delito informático porque son un delito especial a través de sistemas. Algunos participantes indican que sí se debería tipificar dentro de un delito informático.
Tipificación de la Estafa en Delitos Informáticos	Opiniones divididas sobre si se puede tipificar el delito de estafa dentro de los delitos informáticos. Todos coinciden en que se debería modificar la norma para que sea más exacta en cuanto a la comisión de estafa. Si bien se ha logrado estafas mediante herramientas tecnológicas, estas cumplen con la finalidad del "delito de estafa" porque se logra engañar a un usuario.

Anexo 03: Resumen de respuestas codificadas

Pregunta de investigación	Hallazgos principales
¿Qué obstáculos afectan la investigación de delitos informáticos?	Falta de persistencia del denunciante, ausencia de fiscalías especializadas, falta de coordinación entre la fiscalía y la PNP, carencia de equipos tecnológicos.
¿Los fiscales cuentan con recursos suficientes para investigar estos delitos?	Opiniones divididas: algunos creen que sí, debido a la existencia de DIVINDAT, mientras que otros afirman que falta personal capacitado y herramientas tecnológicas adecuadas.
¿Qué medios probatorios son necesarios en los delitos informáticos?	Registros de bancos, capturas de pantalla, correos electrónicos, historial de navegación, metadatos, dispositivos digitales, registros de llamadas.
¿Qué relación existe entre el delito de hurto y la estafa en el ámbito digital?	Mientras que el hurto requiere de un medio físico, la estafa puede valerse de herramientas digitales para engañar a las víctimas. En algunos países el "hurto informático" ya está tipificado.
¿Cómo colaboran los bancos en las investigaciones?	Solo responden cuando hay una orden judicial, pero demoran en entregar la información, lo que dificulta la flagrancia. Se recomienda un convenio entre el Ministerio Público, la PNP y los bancos.
¿Qué deficiencias existen en las investigaciones preliminares?	Falta de seguimiento en denuncias, demora en la obtención de pruebas digitales, ausencia de laboratorios forenses descentralizados, desconocimiento de herramientas TIC por parte de fiscales y policías.
¿Se necesita capacitación en TIC para mejorar la persecución de delitos informáticos?	Sí, todos los participantes coincidieron en que es fundamental la capacitación en herramientas digitales para fiscales y policías.