UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Valoración de los medios probatorios de delitos informáticos en el distrito de Ventanilla, 2021

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestra en Derecho Penal y Procesal Penal

AUTORA:

Loa Pacora, Angie Melissa (orcid.org/ 0000-0002-9905-8098)

ASESOR:

Mg. Villanueva de la Cruz, Manuel Benigno (orcid.org/ 0000-0003-4797-653X)

LÍNEA DE INVESTIGACIÓN:

Derecho penal, procesal penal, sistemas de penas, causas y formas del fenómeno criminal

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía

LIMA — PERÚ

2022

Dedicatoria

A Dios, a mi madre María Elena, por su sabiduría e incondicional apoyo, por el amor y admiración que le tengo, está dedicada esta tesis a mi hija Regina, por ser el motor y motivo de mis logros, a mí amado esposo Jason por su incondicional apoyo. Gracias a mi familia porque son mi motivación, para ustedes dedico esta tesis.

Agradecimiento

Agradezco a la Universidad César Vallejo y a mi asesor por su apoyo y por brindarme su conocimiento en el desarrollo de la tesis para la obtención del grado de magister, muchas gracias por toda su dedicación.

Índice de Contenidos

Índice de tablas

Índice de figuras

Pág.

Índice de abreviaturas

Tic	Tecnologías de información y comunicación
Divindat	División de investigación de delitos de alta tecnología
R.N.	Recurso de nulidad
Cas.	Casación

Resumen

La presente investigación tuvo como objetivo: Determinar que medios probatorios son indispensables en los procesos de delitos informáticos en el distrito de Ventanilla, 2021. La metodología sigue el enfoque cualitativo, investigación de tipo básico, diseño de teoría fundamentada, para el cual se utilizó como instrumento de investigación guías de entrevista, en las cuales se entrevistaron a abogados, asistentes en función fiscal, fiscal y policías del distrito de Ventanilla.

Se concluyó que los medios probatorios se obtienen de información almacenada en dispositivos informáticos, discos rígidos, tráfico de datos, metadatos de archivos y claves de encriptación y que en el distrito de Ventanilla no se cuenta con los recursos suficientes para recabar dichos medios de prueba. En relación a la comisión del delito de hurto, se requiere de un medio físico, por ende, no se le puede tipificar dentro de los delitos informáticos, sin embargo, el delito de estafa se basa en el engaño, manipulación pudiendo ser mediante herramientas tecnológicas a fin de obtener un beneficio económico en perjuicio de otro sin embargo no está regulado como tal.

Palabras clave: cibercrimen, evidencia digital, Tecnologías de la información

Abstract

The objective of this research was to: Determine which means of proof are essential in computer crime processes in the Ventanilla dictrict of the year 2021. The methodology follows the basic qualitative approach, grounded theory design, for which it was used as an instrumento of investigation interview guides, in which lawyers, assistants in fiscal function, fiscal and policemen of the district of Ventanilla were interviewed.

It was concluded that the evidence is obtained from information stored on computer devices, hard drives, data traffic, file metadata and encryption keys. And in relation to the commission of the crime of theft a physical means is required, therefore, it can not be typified with in computer crimes, how ever, the crime of fraud is base don deception, manipulation may be through tolos technology in order to obtain an economic Benefit to the detrimento of another.

Keywords: cybercrime, digital evidence, information technology

I. INTRODUCCIÓN

La investigación analiza los criterios usados para sentenciar los delitos cibernéticos y/o informáticos en el distrito de Ventanilla, 2021. En ese contexto esta investigación aborda el análisis de sentencias, y jurisprudencias relacionadas a los delitos que requieren del uso de tecnologías de la información; la necesidad de esta investigación surge con el análisis de la obtención de medios probatorios y sus deficiencias, a fin de obtener sentencias vinculadas a delitos en los que se emplean las herramientas tecnológicas y electrónicas de información.

La Ley N° 30096 tuvo como objetivos prevenir y sancionar conductas antijuridicas que vulneren los sistemas y datos informáticos, como el patrimonio y fe pública, para los cuales el que delinque usa la tecnología para cometer actos ilícitos. Esta norma fue modificada con la Ley N° 30171 que agregó el atentado a la integridad de datos y sistemas informáticos, fraude informático, interceptación de datos informáticos, abuso de mecanismo y dispositivos informáticos, en donde el dolo es parte del ilícito penal.

A nivel internacional, varios autores coinciden con Steckman (2020), al señalar que los delitos cibernéticos corresponden al acto de infringir la ley en línea, brindando una figura penal de los delitos informáticos como un delito de resultado, porque en su ilicitud se evidencia las consecuencias de conductas humanas relacionadas a conductas típicas, como clonar, introducirse en la recepción de una señal y perturbarla, borrar, suprimir, ingresar o invadir sistemas informáticos, esta acción da como resultado causar un perjuicio económico.

A nivel nacional, Pardo (2018) resalta que los delitos informáticos se enfocan como delitos de patrimonio informáticos en modalidades de hurto, fraude y estafa, comprenden conductas dolosas, mediante dispositivos electrónicos, redes de información, es decir que son conductas típicas que solo pueden ser realizadas mediante las TICs. Estos ciberdelitos requieren de ordenadores y sistemas de información.

A nivel Local, en el distrito de Ventanilla, la conducta humana antijuridica que se realiza en el ciberespacio está relacionada a delitos que se cometen mediante el

uso de medios electrónicos y no tienen exclusivamente normas reguladoras jurídicas como tampoco un procedimiento especifico.

Granero, et, al., (2019), indica que el objeto de las diligencias de investigación tecnológicas, es el logro de pruebas electrónicas, refiriéndose como alguna información obtenida donde su punto de partida es un dispositivo electrónico o medio digital que ejerzan credibilidad respecto a un hecho, guardando una obtención correcta y licita, constituyendo así pruebas exactas, veraces y objetivas. Cuando no existe un procedimiento probatorio eficaz con los recursos que sean necesarios para el proceso penal no será solido el proceso de enjuiciamiento.

Respecto a la formulación del problema, Martinez (2014), sostiene que se debe precisar la formulación del problema en términos que también manifiesten resolubilidad, y en relación al problema de investigación deberá expresar la conexión entre dos o más variables o categorías.

El problema general de la investigación es: ¿Qué se necesita en el distrito de Ventanilla para obtener medios probatorios que ameritan ser obligatorios en los procesos relacionados a delitos informáticos?, siguiendo con el mismo orden de ideas, se plantea como problemas específicos: a) ¿Qué se necesita para continuar con la investigación preparatoria en los casos relacionados a delitos informáticos?, y b) ¿Qué relación tienen el delito de hurto y el delito de estafa en los delitos informáticos?

La justificación teórica del estudio, busca brindar información útil y mejorar la forma en que se aplica la norma sobre delitos informáticos, Asimismo con esta investigación se pretende dilucidar criterios, fundamentos, medios probatorios y una necesaria actualización para nuestros operadores de justicia al momento de imputar, y sentenciar estos delitos con la finalidad de dar una solución jurídica a estos casos.

La justificación metodológica del estudio, se basa en las averiguaciones obtenidas mediante instrumentos de investigación, que serán de utilidad para los siguientes trabajos de investigación, tal como lo señala Baena (2017), para el proceso metodológico de investigación se empleara el diseño de trabajo, recopilación de información y exposición de los resultados.

La justificación práctica de la investigación, Posada (2017) sostiene que la doctrina sobre cibercrímenes castiga las conductas que vulneran o ponen en peligro de manera ilícita la seguridad de las funciones informáticas, por ello el aporte que hará esta investigación es fruto del resultado de un análisis doctrinario y jurídico, en atención al análisis de sentencias relacionadas a los delitos informáticos y/o cibernéticos.

La justificación jurídica se basa en argumentos relacionados sobre un determinado hecho, como lo manifiesta Atienza (2016), son la base objetiva y lógica a una respuesta donde también hay diferencias de opiniones que dependen del conocimiento o ignorancia de los hechos.

En el 13° Congreso de las Naciones Unidas sobre prevención del delito y Justicia Penal (2015) se precisó, que la ciberdelincuencia recurre a las tecnologías de la información para cometer sus actividades antijurídicas, su *modus operandi* es atacar como delitos contra la confidencialidad, la integridad y disponibilidad de datos o sistemas informáticos con la finalidad de robar y estafar.

Ñaupas, et, al., (2018) Indica que los objetivos son aspiraciones que se esperan alcanzar en un periodo determinado, es decir, los objetivos son el resultado de lo que se espera alcanzar. En ese marco, el Objetivo general de la investigación es, Determinar que medios probatorios son indispensables en los procesos de delitos informáticos en el distrito de Ventanilla, 2021; como objetivos específicos se planteó: a) Determinar que se necesita en las investigaciones fiscales para procesar los casos relacionados a delitos informáticos, y b) Analizar la relación jurídica de los delitos de hurto y estafa en los delitos informáticos.

Como hipótesis general: El Ministerio público no cuenta con los recursos suficientes para acreditar los delitos informáticos en el distrito de Ventanilla, y como hipótesis especificas: a) Los conocimientos de los operadores de justicia del distrito de Ventanilla no son suficientes para imputar el delito informático, y b) El delito de hurto y estafa se pueden tipificar dentro de los delitos informáticos.

En ese contexto, el objetivo de esta investigación es Determinar que medios probatorios son indispensables en los procesos de delitos informáticos en el distrito de Ventanilla, 2021.

II. MARCO TEÓRICO

Las herramientas tecnológicas, han ayudado con un sin fin de beneficios, como programarse audiencias usando computadoras u otros medios electrónicos, que permiten relaciones de comercio, como también se ha usado para fines ilícitos como estafas mediante links, suplantación de identidad, contacto con menores de edad con fines delictivos, extorsiones y otros en perjuicio de terceros. El enfoque usado es el cualitativo, con diseño de teoría fundamentada.

Actualmente, la DIVINDAT se encarga de investigar la comisión de delitos informáticos y otros delitos donde se empleen medios informáticos. El bien jurídico es de naturaleza informática es decir “de la información y datos”, al ser un bien jurídico autónomo su vulneración da lugar a tipificar otros delitos atentatorios contra diversos intereses jurídicos, porque su comisión exige de conocimientos especializados.

A nivel internacional, Jimeno (2019), en su libro “Derecho de daños tecnológicos, ciberseguridad e insurtech” señala que, el alcance de las Tics y su trascendencia en el ámbito socioeconómico ha generado que las tecnologías de la información constituyan un pilar fundamental para la hiper conectividad, el ciberespacio alcanza consideraciones sociales y jurídicas, en el aspecto jurídico se han multiplicado las consecuencias de internet, sus fenómenos, y sus ciber riesgos como amenazas cibernéticas.

El autor concluye haciendo una diferenciación entre los términos riesgo tecnológico o informático y ciber riesgo, por tratarse de diferentes objetivos en su comisión, siendo el caso de ciber riesgos, estos se producen a consecuencia del desarrollo de las TICs, donde para su comisión se requiere de tres elementos: presencia de una acción u omisión, aprovechar una vulnerabilidad o fallo en los sistemas tecnológicos y procedimientos internos, y como resultado de estos se produzcan efectos externos que puedan causar un daño.

De la Fuente (2019), en su libro “Comunicación e imagen corporativa” narro el caso donde suplantaron la identidad del Tribunal Superior de Justicia de la Comunidad Valenciana usando como método una cuenta falsa en twitter y mediante una orden judicial, twitter cerro dicha cuenta. Cualquier persona puede crear un perfil falso con varios fines, y el más usado relacionado al robo de información de usuario para realizar fraude online son el Phising y Pharming.

Kerttunen (2020), in his book about “Routledge Hansbook of international cybersecurity” concluied “The two main problems to tackle in the región are the desproportionate focus on cybercrime legislations and the desire to increase control of the onlines space and surveillance. Actual cybersecurity concerns, the technically securing sistems, take a back seat. By focusing on control and restrictions rather tan securing systems.”

Los autores concluyen que al existir un enfoque desproporcionado en las legislaciones sobre delitos cibernéticos y el deseo de aumentar el control de lo que ocurre en el ciberespacio, dejan totalmente las restricciones que debería haber para asegurar los sistemas informáticos.

Latin America, on the other hand, the resgional emphasis has been a building technical response teams and capacity building, instead of specific treaties. By building institutional capacity, the región has been able to evolve their approach to cybersecurity issues and being les centre don cybercrime issues

América Latina se enfoca en los problemas de seguridad cibernética y así esta menos centrado en los problemas del delito cibernético.

El criminólogo e investigador privado Ferro (2020), en su libro “Cyber espionaje, Cyber estafas y Guerras informáticas El lado oscuro de Internet : la prueba digital”, resalta que los delitos que se cometen usando herramientas tecnologías no tienen una ley que regule adecuadamente las conductas que contravienen el orden jurídico en el ciberespacio, concluyendo que la ciber delincuencia corresponde a acciones humanas que se desempeñan con la ayuda de redes de comunicaciones, sistemas electrónicos e informáticos y TICs.

Steckman (2020), en su libro “Examining Internet and Technology around the world” indica que “cybercrime refers to the acto f breaking the law online. It occurs when

people decide to violate the law, usually for monetary or other personal gain. It is a fast-growing criminal industry because it can be extremely profitable and has natural, built-in barriers to being caught due to the technologies employed.

Refiriendo que el ciberdelito es el acto de infringir la ley en línea, es decir que esto ocurre cuando las personas deciden violar la ley a fin de obtener ganancias monetarias causando daños graves y representando amenazas reales en sus víctimas.

“Law enforcement agencies recognize multiple types of cibercrimen that generally fall into one of two categories: high-tech crime and cyber-enabled crime refers to either the adaptation of crimes usually committed offline to cyberspace or the inventation of new methods or means tos teal information, such as a person is identity or financial information, over the internet.

Ferro (2020), plantea que, la forma en que se concreta los ciber crímenes o delitos informáticos pertenecerían a un crimen organizado, así también se explica en el R.N N° 4727-2006 Lima, donde indica que “Dentro del delito informático se imputa la participación en grado de cómplice secundario, porque autorizo el uso de cuentas de la empresa para el desvió de dinero a cambio de un porcentaje, siendo su actuación la de guardar silencio y no denunciar el hecho ante sus superiores”.

Como antecedentes nacionales, la ciberdelincuencia se puede poner en dos categorías: delincuencia de alta tecnología que ocurre cuando el objetivo del delincuente es la interrupción o destrucción del hardware o software de una computadora, y la delincuencia cibernética la cual se refiere a la adaptación de delitos que normalmente se cometen fuera de línea al ciberespacio como robar la identidad de una persona o entidad financiera, piratería o delito cibernético para robar dinero de la cuenta o tarjetas de crédito.

Algunos procesos de delitos informáticos no han llegado hasta la etapa de juzgamiento, porque a los operadores de justicia no se les capacita de forma eficiente sobre las herramientas de las Tic, este tema también fue abordado por Mori (2019), en su tesis de maestría donde tuvo como objetivo conocer la forma en que investigan y juzgan los operadores de justicia a los delitos que requieren de tecnologías de información, encontrando la discrepancia de opiniones entre jueces

y fiscales, toda vez que en opinión de los jueces existe una carencia de instruir en herramientas tecnológicas y los fiscales no creen que exista tal ausencia, como tampoco creen que exista transgresiones a la norma porque haya una insuficiente determinación del daño causado.

Serrano (2021), recomienda redefinir los cimientos dogmáticos de los delitos informáticos, profundizando el estudio dogmático a fin de dar mayor protección a los bienes jurídicos, desde un contexto constitucional basado en una protección moderna de principios penales, orientado a la protección de la persona humana con el fin de guiar las actividades que desarrollan nuestros legisladores.

De acuerdo a Hernández (2012) la búsqueda de nuevos conocimientos se fundamenta en una teoría que sirve de partida. La investigación requiere de conceptos orientadores que guíen la investigación y sus resultados; la teoría es contrastada con el resultado teórico al contribuir a mejorar una realidad.

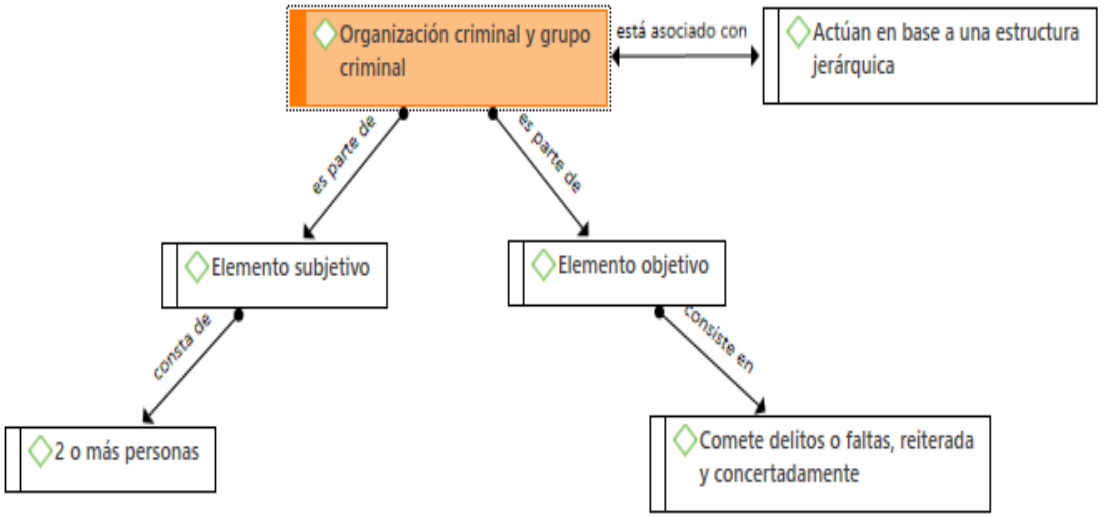
El bien jurídico que se protege como lo señala Piva, et al., (2021), en los delitos informáticos, es la protección que repercute en el bienestar de la sociedad o grupos económicos, que son vulnerados por conductas ilícitas que requieren del uso de TICs; por lo tanto, el bien jurídico protegido es la protección de la información y de los datos.

En relación a los delitos patrimoniales, Pardo (2018), en su tesis de maestría planteo como objetivos analizar dicho tratamiento jurídico penal de los delitos informáticos contra el patrimonio y sus modalidades en hurto, fraude, estafa y sabotaje informático, concluyendo que existe una deficiencia en la hermenéutica de la norma, toda vez que es inexistente una correcta sanción de los delitos informáticos que afectan el patrimonio. Asimismo, es deficiente en todas sus modalidades como hurto, fraude y sabotaje informático.

La investigación cuenta con las teorías y enfoques conceptuales de acuerdo a las categorías de delito patrimonial informático e Investigación preparatoria, en donde el R.N. N° 4727-2006 Lima, señala que el “delito informático lo constituye todo acto que permita la comisión de agravios, daños o perjuicios en contra de las personas, grupos de personas, entidades o instituciones y por lo general son ejecutados por medio del uso de computadoras mediante el mundo virtual”.

Figura 1

Organización criminal y grupo criminal



Teniendo claro lo que es un delito informático, en el R.N N° 206-2019, explica que el delito patrimonial informático corresponden a " … la comisión de delitos de contenido patrimonial mediante el uso de la tecnología informática en las cuales se obtiene el número de tarjetas bancarias a través de una réplica de página web", la conducta antijurídica es denominada como Phishing, comúnmente usado para obtener números de tarjetas y claves de seguridad.

En la Sentencia Nº 00763/2006 de España se preciso que el Hurto mediante sistemas informáticos, se configura como "… la tarjeta constituye la llave que introducida en la máquina, permite activar el mecanismo que dispensa el dinero", en ese sentido se entiende que la tarjeta de crédito o débito cumple el rol de una llave metálica, por lo tanto en el caso que la clave de la tarjeta fuera suministrada gracias a alguna maniobra de la acusada, no hubo beneficio patrimonial para la agraviada (o), porque la acción de la acusada sin conocimiento de la agraviada para sustraer dinero del cajero es el despojo de su patrimonio.

Es decir, que dicha conducta ilícita se configura como hurto agravado y no como estafa porque el delito de estafa se constituye cuando existe un nexo entre el ardid, el error y la disposición patrimonial, nexo que en este caso no se da.

Tabla 1

Tipos de actividades delictivas

Tipos de actividades delictivas		
Formas tradicionales	⇨	Fraude o falsificación
Publicación de contenido ilegales	⇨	Imágenes de abuso sexual a menor o incitación al odio racial
Delitos específicos	⇨	Ataques contra sistemas informáticos, denegación del servicio o piratería

La perspectiva criminológica del fraude informáticos es; el conjunto de conductas cuyo denominador común es el uso de las redes telemáticas como instrumentos mediante el cual se puede obtener un beneficio patrimonial ilícito derivado de un perjuicio patrimonial de un tercero o a una víctima.

Formas más conocidas del ciber fraude son: Fraude con tarjetas de crédito, Estafas piramidales, Estafas de lotería, Estafas de inversión, Ataques de scam y fraude de subastas.

En la Cas. N° 956-2017 Lambayeque se comentó sobre el expediente penal N°7061-2008 donde se concluyó que el Banco Continental no tiene responsabilidad penal dentro del delito de hurto agravado por la sustracción inconsentida de dinero de una de las cuentas bancarias de un cliente. Es decir que el banco no es responsable ni civil ni penalmente ante un robo cibernético cuando mediante boletines informativos da recomendaciones de seguridad ante fraudes por internet, es decir que cumplieron con informar sobre las medidas de seguridad que debían tener en cuenta al realizar operaciones vía internet en las páginas web del banco, el cliente debe observar el doble certificado de autenticación

En la Sentencia N°332/2020, el Tribunal Supremo de lo Penal de Madrid, en su Resolución Sts 49/2020, se precisó que la estafa dentro de los delitos informáticos corresponde al acceso de claves para realizar transferencias mediante el engaño, es decir que corresponde a la continuidad delictiva como estafa informática. Asimismo, el fraude informático está previsto como una modalidad de la estafa, y lo que se pretende proteger es el patrimonio de los ataques mediante tecnologías.

Por lo anteriormente expuesto, el tribunal de Madrid señalo que “el engaño en la estafa ya no es un elemento básico porque ha sido sustituido por artificios prohibidos, porque el acecho a patrimonios ajenos realizado mediante manipulaciones informáticas actúa con automatismo en perjuicio de un tercero, precisamente porque existe la manipulación informática y por ello no se exige el engaño personal”.

En la sentencia 1915/2019, el Tribunal Supremo de Madrid, en su Resolución Sts N° 305/2019 trata sobre la acreditación de la estafa informática, para la cual se requiere de la declaración del testigo, manifestaciones del acusado en relación a su participación en los hechos, pericia del hackeo, acreditarse el dolo (en caso el denunciado no tenga conocimiento que los depósitos a su cuenta tengan como origen procedencia ilícita).

De acuerdo a la Sentencia 23/2017 Madrid, El tipo penal de los delitos cibernéticos, se contempla las siguientes conductas: a) Se refiere a datos, programas informáticos, documentos electrónicos ajenos dañados mediante alguna acción del sujeto activo o perpetrador y b) la obstaculización o interrupción del funcionamiento de un sistema informático ajeno. Entendiéndose que el daño causado se refiere a borrar, alterar, suprimir o realizar un daño con el que sea inaccesible a datos informáticos.

En la Sentencia N° 00148/2006 la Corte suprema de justicia, se hace referencia al delito informático como un delito continuado, donde: a) En relación al fraude informático, se trata de un beneficio patrimonial para sí o para un tercero, influye en el resultado de datos de un sistema de cómputo, uso de datos falsos o indebido de datos y b) Respecto al sabotaje informático, se trata que exista un daño en los ordenadores o sus componentes.
En la prisión preventiva, se omite cuando existe delitos continuados y por ende queda firme el juicio de culpabilidad por delitos de robo agravado, falsificación de documento privado y estafa.

En el concurso ideal de delitos no se concreta cual es la pena aplicada para cada delito más grave y si este aumento o no, impidiendo conocer la penalidad por tratarse de un delito continuado.

Si bien la investigación penal tiene como objetivo descubrir la verdad sobre un hecho que fue cometido mediante pesquisas, ciencias forenses, localización, entrevistas de testigos, y diferentes técnicas de criminalística también tiene como finalidad recabar todo lo relacionado para esclarecer hechos punibles mediante las evidencias, pericias, informes, declaraciones y actuaciones que se realizan en la investigación penal, mediante el uso de instrumentos y tecnologías.

La investigación penal tiene como objetivo: a) Investigar los hechos punibles, b) Determinar si existe la comisión de un hecho punible tipificado, c) Esclarecer los hechos criminales, d) Identificar e individualizar las herramientas usadas, e) Identificar e individualizar las evidencias de la escena del crimen y otros sitios relacionados, f) Identificar al autor, participes o cómplices, g) Reconstruir los hechos punibles, h) Identificar a las víctimas, i) Garantizar la cadena de custodia de las evidencias físicas como: discos duros, grabaciones, u otros usados en la investigación.

Los elementos de la investigación penal en los delitos informáticos son las diligencias orientadas al descubrimiento o esclarecimiento del delito, que servirá como elementos de convicción como base de la investigación penal.

De acuerdo a Martín (2017) las fuentes de evidencia digital se pueden clasificar en sistemas de computacion abiertos, sistemas de comunicación y sistemas convergentes de computacion.

Para la pericia informática conocido como Análisis digital forense, tiene como objetivo averiguar lo que ocurrió durante un incidente en equipos tecnológicos, brinda apoyo teórico - científico para dar respuestas al problema tecnológico. Averigua cual fue el origen del problema, que activos fueron afectados y en qué grado.

Tabla 2

Procedimientos de investigación

Procedimiento	Sirve	Usa
Investigación criminalística	Comprueba y deja constancia de la comisión del hecho delictuoso	Inspecciones técnicas, localizar, procesar evidencia física, elabora pericias o informes técnicos
Investigación o pesquisa policial	Como proceso investigativo de campo	Localiza y entrevista testigos, indaga información, recopila y procesa, estudia modus operandi, realiza labores de inteligencia, efectúa seguimiento como registros, inspecciones, allanamientos, interceptaciones telefónicas
Pericia informativa	Reconstruir el bien jurídico informático, examina datos residuales, autentica datos y explica las características del uso aplicado a los datos y bienes informáticos	Técnicas científicas y analíticas especializadas en infraestructura tecnológica para identificar, preservar, analizar y presentar datos que sean válidos para el proceso penal

La evidencia digital es la información digitalizada que será materia de análisis por un método técnico y generará conclusiones irrefutables en lo legal, mediante la revisión de las redes sociales, discos duros, equipos de cómputo, celulares, sistemas de información, base de datos, cámaras de video etc., todas las pericias son atípicas porque no se puede determinar el tiempo real en que se logra la extracción y análisis para armar la teoría del caso.

Las pericias se pueden realizar de los análisis en dispositivos móviles, recuperación de archivos en dispositivos electrónicos, las herramientas empleadas son :Analysis video digital: Amped Five, Analysis forensic computing, Ufed 4PC: Premium, Cámaras de circuito cerrado CCTV.

La Pericia, es la habilidad para resolver con facilidad, rapidez y fluidez un problema que entra la dificultad, para su realización se necesita de un perito o experto que es una persona con amplio conocimiento y experiencia en determinada área.

En el R.N N° 1936-2019 Lima, se precisó que no basta la concurrencia de varios agentes para imputar el delito de asociación ilícita para delinquir, dado que lo que se tiene que acreditar es el dolo de los integrantes de la agrupación, en la forma y circunstancias que se exigen para ese tipo de delito, es decir de manera permanente, con relativa organización divisional, funciones de roles y con absoluto conocimiento de las finalidades del grupo para la comisión de hechos delictivos aunque aún no se hayan perpetrado.

El *modus operandi* en estos tipos de delitos de ciberdelincuencia se perpetran de dos formas, el primero es con un virus informático, en donde se utiliza una IP de otra persona ajena a todo el cibercrimen, mediante dicha IP se logran hacer transacciones de otras personas es decir que, A utiliza la IP de B, con la finalidad que mediante la IP de B se obtenga información de C, D y E, y al momento del rastreo tecnológico del delincuente se llegara a la IP de B, sin la necesidad de que B tenga conocimiento de cómo está involucrado en un delito tecnológico, y en la revista sobre Delitos informaticos (2016) la segunda forma es mediante el engaño a fin de apoderarse de un patrimonio indebido, en perjuicio de los titulares de cuentas bancarias.

Reátegui (2022) Juez del juzgado de investigacion prepatoria de la Corte Superior de Lima, en una entrevista señalo que la ley informatica es un medio para delinquir, es una ley especial, sin embargo no tiene una ley procesal tampoco fiscalias especializadas, lo que difiiculta las investigaciones y que una forma de identificar a los ciberdelincuentes, es mediante la denunciar, debe haber un agente encubierto.

III. METODOLOGÍA

Según Landeau (2008), la metodología es el conjunto de métodos que se siguen para perseguir un enfoque en particular para comprender o interpretar la realdad de un fenómeno.

La investigación es de enfoque cualitativo, de nivel básico descriptivo, porque pretende analizar el desarrollo de los casos relacionados a los delitos informáticos hasta llegar a su culminación siendo esta con la sentencia o en su archivamiento. Según Galeano (2020), los estudios cualitativos tienden a comprender la realidad social como consecuencia de un proceso previo de construcción con múltiples percepciones lógicas, por lo que el investigador cualitativo no solo obtiene la información de su investigación de conceptos, definiciones y/o clasificaciones, su análisis implica una reflexión sobre la fase anterior para avanzar en la construcción del conocimiento.

3.1 Tipo y diseño de investigación

El tipo de investigación es básico, por consiguiente se basa en el análisis de la culminación de procesos relacionados con los Delitos Informático en el Distrito de Ventanilla, 2021, para un mayor esclarecimiento, Nicomedes (2018) establece que la investigación básica comprende estudios de investigación explicativa y descriptiva, el acicate de este tipo de investigación es dar conocer que medios probatorios son necesarios para imputar el delito cibernético, que falta en nuestra legislación para que estos culminen en sentencias satisfactorias, que se necesita para que existan más sentencias por este delito, el cual se convirtió en un delito común y sin embargo no se ha superado ni 10 % de sentencias que confirmen este delito del total de denuncias relacionadas al delito informático en el distrito de Ventanilla.

Por tanto, en esta investigación se optó por la investigación básica, porque, se esperar lograr determinar los criterios que se aplican para la probanza de los delitos cibernéticos, permitirá ceñir y conceptualizar conceptos de los datos recolectados como una herramienta de información de diversos especialistas en materia penal.

En el diseño de investigación, Chávez (2016) manifiesta que una manera de clasificar el diseño de investigación, es cuando se lleva a cabo la obtención y análisis de información, y si esta es percibida en el pasado y estudiada en el presente, indica un estudio retrospectivo, correspondiendo así a una investigación descriptiva, porque la información que se utiliza es de tiempo pasado, así también lo explica Martinez (2018), cuando se refiere a la investigación descriptiva como un procedimiento para describir características de un fenómeno usando información de investigaciones previas.

El objetivo de la Teoría fundamentada según Ortiz (2020), es generar teorías en base a datos adquiridos en el proceso de la investigación, mediante procedimientos interpretativos y de decodificación. Al abordar el uso de una teoría fundamentada se reconocen elementos que deben ser considerados para su realización, siendo el procedimiento, validación de datos y teoría, los que fortalecen la interpretación de la información recolectada. Por lo tanto, la Teoría fundamentada brinda una información necesaria que responde a las categorías y sub categorías que forman parte de la investigación.

3.2 Categorías, Sub categorías y matriz de categorización

Strauss (2002), indica que una categoría representa un fenómeno, es decir, representa un problema, asunto, acontecimiento o un suceso que será definido significativamente por los entrevistados, las Sub categorías responden a preguntas sobre los fenómenos siendo estas: cuándo, dónde, por qué, quién, cómo y con qué consecuencias, explicando los conceptos de las categorías.

Tabla 3

Matriz de categoría y sub categoría

Categoría	Sub Categoría	Fuente	Técnica	Instrumento
Delito patrimonial informático	○ Hurto ○ Estafa	Abogados penalistas		
Investigación preparatoria	○ Falta de fiscalías especializadas	Expertos en informática	Entrevista	Guía de Entrevistas
	○ Falta de conocimiento en herramientas tecnológicas de información	Ingenieros de sistemas		

El Tribunal Supremo de Madrid, en su Resolución N° 49/2020, de la Sts 332/2020 preciso que la estafa dentro de los delitos informáticos corresponde a "…el engaño en la estafa ya no es un elemento básico porque ha sido sustituido por artificios prohibidos, porque el acecho o vigilancia a patrimonios ajenos realizadas mediante manipulaciones informáticas actúa con automatismo en perjuicio de un tercero, porque existe la manipulación informática y por ello no se exige el engaño personal".

Asimismo, la estafa se encuentra comprendida como una modalidad en el fraude informático, por lo que se pretende proteger es el patrimonio de los ataques mediante tecnologías.

La Tercera sala de la Corte suprema de Justicia, con su Sentencia N° 00763, expresó que el delito informático es cualquier ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel importante ya sea como medio o como fin; como medio en el caso del fraude informático, y como fin, en el sabotaje informático.

La tipificación de los delitos informáticos consiste en el resultado de la acción, es decir que se evalúa la influencia del resultado de datos de un sistema informático a través de diversas conductas y su finalidad. Para lo cual la mencionada influencia consiste en manipular información, realizar actos irregulares en un sistema, es decir en la realización de las instrucciones de un sistema.

Como medio probatorio no es necesario que el sujeto activo tenga conocimientos técnicos en informática dado que puede realizarlo cualquier persona que tenga acceso al procesamiento de datos pudiendo ser incluso de forma remota y mediante la acción de manipular programas informáticos.

3.3 Escenario de estudio

La investigación se realizará dentro del Distrito de Ventanilla en relación a delitos que requieran del uso de TICs para su comisión.

3.4 Participantes

Las personas que brindarán su colaboración con esta investigación serán el Fiscal, Asistentes en función fiscal y abogados; asimismo también se ha realizado un análisis de diversas publicaciones de autores de libros y artículos relacionados a los delitos informáticos. Finalmente, también se considerará la colaboración de la policía de Ventanilla, quienes cooperan con las fiscalías en la investigación preparatoria a fin de imputar un delito.

3.5 Técnicas e instrumentos de recolección de datos

Los instrumentos para recolectar datos son un mecanismo o dispositivo que usa el indagador para obtener información, concordando con la idea de Yuni (2006) en donde indican que instrumentos pueden ser, formularios de un cuestionario, guía de observación o guía documental de análisis de casos, videos relacionados al tema de investigación como ponencias, o charlas de magistrados exponiendo temas sobre los delitos informáticos. En base a esa línea de idea, la técnica que se ha usado para recabar información ha sido la guía documental y guía de entrevistas.

3.5.1 Técnicas

La técnica para recolección de datos usado es la Guía de entrevista a fiscales, asistentes en función fiscal, policías y abogados, asimismo también se utilizó el análisis documental como: jurisprudencias, el análisis de la Ley N° 30096, Ley N°30171, libros relacionados a los delitos informáticos y artículos de revistas jurídicas.

3.5.2 Instrumentos

Martínez (2014), sostiene que el instrumento para la recolección de datos o información debe garantizar que es lo que pretende medir ya sea en conocimientos teóricos, resolución de problemas o procedimientos, sea válido para medir las variables, a su vez que sea fiable y se fundamente con el resultado de la información recabada.

3.6 Procedimientos

Los procedimientos para recabar información o gestionar datos, son métodos, técnicas y pasos que se alinean de acuerdo a la meta que se quiere alcanzar, así también lo explica Landeau (2007), cuando indica que un procedimiento es aquel que se sigue en la investigación para lograr una meta con la finalidad de obtener un tipo particular y concreto de conocimiento, y su aplicación requiere que sea verificado y demostrado. Por lo tanto, son registros que evidenciaran con las acciones tomadas, a fin de validar los objetivos con los resultados.

El procedimiento que se usó en la presente investigación se apoya en el análisis de denuncias, imputación del delito, relación de los delitos patrimoniales informáticos con el hurto y estafa, y los procedimientos usados durante la investigación preparatoria para culminar con los procesos mediante sentencias.

También se realizará un análisis de las respuestas obtenidas de los cuestionarios que se realizarán.

3.7 Rigor científico

El rigor científico es la calidad de la información obtenida de las investigaciones haciendo que el resultado sea veraz y creíble, por lo tanto, su calidad se basa en

argumentos confiables y coherentes que puedan ser probados, es así que la principal fuente de investigación corresponde al análisis de casos de delitos informáticos cometidos en el Distrito de Ventanilla. Así también lo señala Noreña, et. al, (2012) indicando los criterios éticos que debe haber en el rigor científico mediante la interacción social y los significados que se obtienen de esta relación a fin de conocer a fondo las características de la materia de investigación.

Esta investigación cumple con los estándares de rigor científico y éticos, debido a que se precisó una problemática de la realidad jurídica para resolver conflictos relacionados a probar los delitos informáticos y porque existe una problemática social, porque son muchas las personas que han sido víctimas de hurto cibernético y estafas mediante sistemas computarizados. También porque se analizaron extractos textuales de juristas, e investigadores nacionales e internacionales.

3.8 Método de análisis de datos

El método de análisis es cualitativo, y descansa sobre supuestos, en los cuales la información será determinante para el proceso investigador. Por lo tanto, esta investigación está orientada en el Método descriptivo, porque como lo indica León (2007), la finalidad del método descriptivo es lograr una descripción del fenómeno en estudio y sea completa, reflexiva y de exigente rigor científico, a fin de aportar datos que necesitan de una interpretación, como lo son los diferentes criterios, sentencias o sucesos que motivan a que se pueda imputar el delito informático.

De acuerdo a Bernal (2006) con el método inductivo se puede tener razonamientos respecto a determinados hechos particulares como conclusiones de jurisprudencias o sentencias, su aplicación es de carácter general.

3.9 Aspectos éticos

En los aspectos éticos se visualiza los valores específicos de la investigación, Ávila (2002), señala que dentro de la investigación cualitativa donde se emplean aspectos éticos dentro de su investigación aborda principales teorías éticas y una propuesta ética como alternativa de solución, para obtener valores específicos.

Siguiendo con lo anteriormente expuesto, esta investigación se elaboró en base a las normas establecidas por la Universidad Cesar Vallejo, también se consideró la

Ley Universitaria N° 30220, la Guia de elaboracion del trabajo de investigacion y tesis para la obtencion de grados academicos y titulos profesionales, el Codigo de Etica de investigacion de la Universidad Cesar Vallejo, dentro de los aspectos internacionales se considero la normativa APA en su séptima edicion. En ese sentido tambien se ha tenido en cuenta los requisitos formales y el debido rigor cientifico que se exige cuando se indaga y se plasma sobre el analisis de los resultados del objetivo general y los objetivos especificos.

Lariguet (2019) en su libro sobre Metodología de la investigación jurídica, Manifiesta que la ética jurídica alude a numerosas problemáticas conceptuales entre sí, y la relación entre el derecho y moral, pueden corresponder a un razonamiento practico, por lo tanto la ética jurídica en la que se fundamente este trabajo de investigación deriva de lógica de principios éticos, por los siguientes fundamentos: a) Corresponden al análisis de sentencias de delitos informáticos, b) Parte de la información obtenida en la investigación son de conferencias de peritos informáticos que laboran en Perú y c) Parte de la información obtenida es de abogados expertos en delitos informáticos.

IV. RESULTADOS Y DISCUSIÓN

En relación a la aplicación de la técnica e instrumento de recolección de datos, se logró procesar información en concordancia con los objetivos planteados en la investigación. En ese sentido, los resultados que responden al objetivo general 1, Determinar ¿Qué se necesita en el distrito de Ventanilla para obtener medios probatorios que ameritan ser obligatorios en los procesos relacionados a delitos informáticos?, se formularon las siguientes interrogantes:

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

Los participantes indicaron que lo que obstaculizan las investigaciones relacionadas a delitos informáticos es la falta de persistencia del recurrente, la falta de información en las denuncias, falta de información por parte del recurrente, dado que se le cita para dar mayores declaraciones de lo sucedido y no concurre a brindar la información solicitada, falta de fiscalías especializadas, falta de coordinación entre policías y fiscalía, falta de logística y apoyo en tiempos de flagrancia, falta de inmediates, y no se tiene el debido conocimiento de la norma.

Herrera (2021), plantea que, dentro de los problemas en torno a los delitos informáticos, son el anonimato o difícil identificación de los actores, como en el caso de hackeo, utilización de datos falsos a fin de crear cuentas falsas de red social y de ese modo se engañe a su víctima para obtener una ventaja patrimonial (estafa), y en el caso de organización criminal, se dedique al tráfico de datos, desfalco en cuenta bancaria utilizando a otras personas y estas capten a otras personas que realicen las operaciones bancarias como transferencias, depósitos y retiros. Un gran obstáculo es que la ley resulta ser insuficiente para el efecto intimidatorio en el potencial delincuente, por ello se debe revisar y adecuarse según la gravedad del bien jurídico lesionado, y contemplar las formas agravadas que legitimen la sanción, en el caso de fraude informático, en donde la ley no prevé formas agravadas para integrantes de organizaciones o bandas criminales, no hay una claridad en la ley.

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

En esta pregunta existen opiniones contrarias, dado que hay respuestas que indican que la fiscalía si cuenta con las recursos necesarios para perseguir el delito porque tienen a la unidad de Divindat para investigar parte de los delitos informáticos, como también hay opiniones que indican que el hecho que la fiscalía tenga como herramienta a la unidad de Divindat como apoyo para perseguir al delito no es suficiente, porque esta unidad no se encuentra en el distrito de Ventanilla, como también se considera que la falta de conocimiento en herramientas de tecnologías de la información es un recurso menos y la falta de una fiscalía especializada con personas que tengan conocimiento en uso y herramientas tecnológicas, así como en el manejo de software que ayude en las investigaciones de delitos informáticos, es decir peritos informáticos.

Izquierdo (2021), concluyo que la ciberdelincuencia económica es un delito de alta complejidad y peligrosidad, debido al mal uso de medios informáticos, como en lo sucedido con los bonos familiares que otorgo el estado peruano en época 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 comisaria, 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 detallado 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 general 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?

Teniendo diversas opiniones respecto a esta pregunta, un grupo de participantes coincidieron que lo delitos de estafa y hurto si se encuentran dentro de los delitos informáticos porque afecta directamente al patrimonio, sin embargo otro grupo de participantes manifestaron que si bien las herramientas tecnológicas son usadas para sustraer bienes económicos, estos son un “medio” por el cual se logra los objetivos delictivo sin embargo los delitos de estafa y hurto no se encuentran dentro de los delitos informáticos.

Acosta et.al, (2020) indican que el hurto y estafa corresponden a una modalidad en la que los infractores crean y activan diferentes formas que les permitan delinquir perjudicando de manera fehaciente la privacidad e identidad de cualquier persona

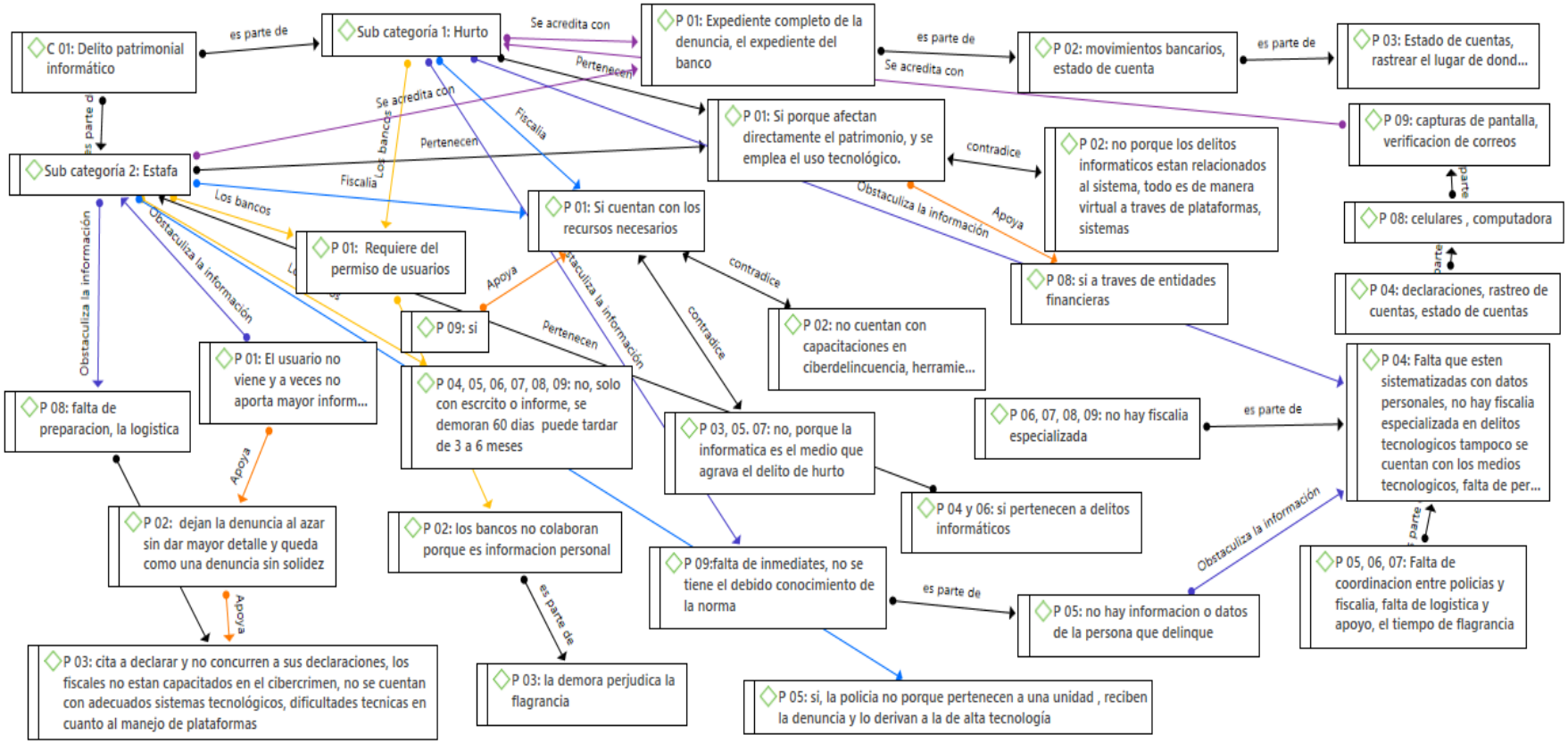
5. En su experiencia ¿Los bancos colaboran de alguna forma en las investigaciones relacionadas a los delitos informativos?

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.

Figura 2

Análisis de resultado de análisis de Categoría 1: Delito patrimonial informático



La Figura 2 explica las dos sub categorías del delito patrimonial, siendo estas el delito de estafa y hurto, para la acreditación del delito de estafa dentro de los informáticos, se necesitará del expediente completo de la denuncia y los informes del banco a fin de revisar los movimientos bancarios y rastrear de que dispositivo se hicieron los últimos movimientos.

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 la legislación penal Española, en su artículo 248.2 se consideran reos de estafa a quienes valiéndose de alguna manipulación informática consiguen transferencias no consentidas de cualquier patrimonio en perjuicio de otro, como también a quienes faciliten programas informáticos con fines destinados a la comisión de estafas finalmente también se consideran reos de estafa a quienes utilizando tarjetas de crédito o débito u otro similar realiza operaciones de cualquier cosa en perjuicio de su titular o de un tercero.

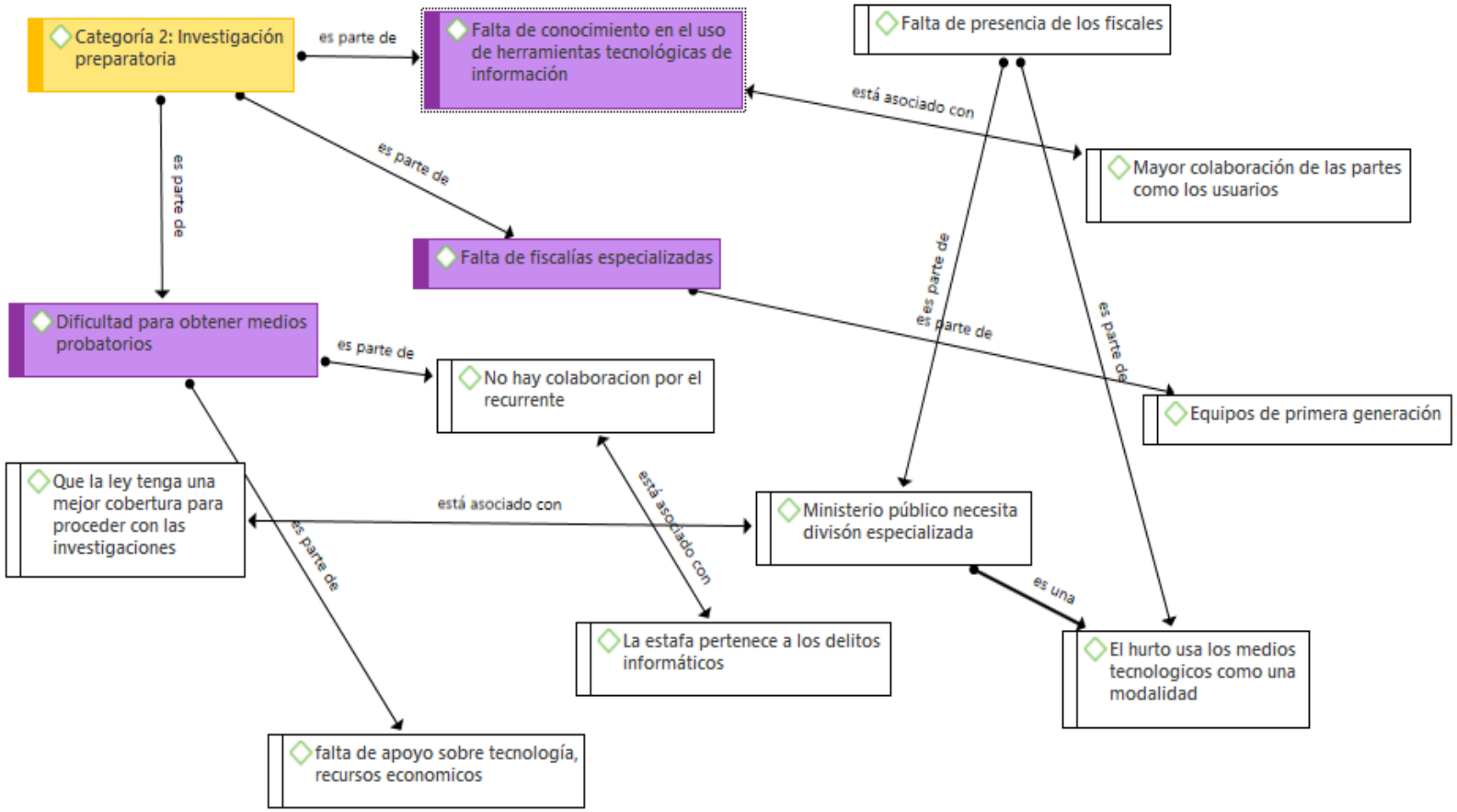
En la Ley penal venezolana, estafa es quien, a través del uso indebido de tecnologías de información, manipula sistema, manipula la data o información en ellos contenida, con la finalidad de insertar instrucciones falsas o fraudulentas, que produzcan un resultado en perjuicio ajeno.

La comisión del hurto es cuando a través del uso de Tic, acceda, manipule, intercepte, o interfiera cualquier forma un sistema o medio de comunicación para apoderarse de recursos patrimoniales económicos ajenos.

En el Art. 217 del Código Penal de Costa Rica, la Estafa informática, es cuando alguien manipula o influye en el resultado de los datos de un sistema automatizado de información, usando datos falsos o incompletos, o reprogramándolos para realizar una operación informática o artificio tecnológico, por cualquier otra acción que transgreda el procesamiento de los datos del sistema o que cause como resultado información falsa, incompleta o fraudulenta, con la cual obtenga un beneficio patrimonial o indebido para sí o para otro.

Figura 3

Análisis de resultado de Categoría 2: Investigación preparatoria



En cuanto al objetivo específico 1, Determinar que se necesita en las investigaciones fiscales para procesar los casos relacionados a delitos informáticos, se plantearon las siguientes interrogantes:

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

Mayor colaboración indagación para recopilar información, actualizarse con el uso de herramientas de las TICs, división especializada, que la ley tenga mejor cobertura para proceder con las investigaciones, equipos de primera generación y mayor acceso a la información, concientizar a la población para que no caiga en estafas de links.

Virú et.al, (2018) recomiendan, implementar sistemas de seguridad, a fin de estar más actualizados para combatir las amenazas más comunes de ataques cibernéticos, existe una deficiencia en las actuales normativas legales produciendo un estancamiento en el comercio electrónico y causando inseguridad en la población. En ese sentido Alan (2017) indica que es primordial afianzar la relación entre policías y fiscales a fin de elaborar y coordinar una estrategia de investigación que será llevada a cabo con colaboración del fiscal.

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

Falta de conocimiento de los usuarios al poner su denuncia en caso de suplantación de identidad, los usuarios no concurren a dar mayores declaraciones, no hay un seguimiento respectivo, carencia de laboratorios tecnológicos para las investigaciones descentralizadas para que se descongestione de la central, falta de equipos informáticos, los bancos demoran en los informes que pide la fiscalía pudiendo tardar más de 3 meses en algunos casos.

Dando una mayor precision Ávalos (2021) recomienda, implementar órganos de apoyo tecnicos descentralizados, equipamiento para labores de analisis forense informatico, tambien recomienda implementar una base de datos de las pericias de analisis digital forense, descentralizar el area de analisis digital forense, con la

creacion de unidades en distritos fiscales con alta demanda de casos, a fin de reducir la carga de requerimientos en Lima y agilizar los analisis forenses, asimismo tambien recomienda diseñar y desarrollar programas de capacitacion dirigido a 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 coincidieron que si hace falta capacitaciones en el uso de herramientas de las Tecnologías de información para imputar los delitos informáticos y que esto se puede observar en la cantidad de denuncias por delitos informáticos que terminan siendo archivadas.

Carrera (2021) en su tesis de maestría, concluyo que la falta de conocimiento y dominio dentro de la investigación se debe a que no se aplica bien la normativa, por lo que se debería considerar nuevos artículos que detallen específicamente sobre la ciberseguridad, asimismo indico que no existe una adecuada coordinación entre fiscalía y policía nacional del Perú que ayude a brindar mejores medidas para identificar a los autores del fraude informático.

Finalmente, en cuanto al objetivo específico 2, Determinar la relación jurídica de los delitos de hurto y estafa en los delitos informáticos., se plantearon las siguientes preguntas:

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

Las respuestas de los participantes, fue que, para la comisión del hurto, este requiere de un medio físico para su objetivo, y la herramienta tecnológica pertenece a un acceso ilícito y el hurto de una apropiación, el delito de hurto es considerado como un delito contra el patrimonio y por sus mismos entes rectores, a este no se le puede calificar dentro de un delito informático porque son un delito especial dado que es a través de sistemas. Un grupo minoritario de participantes indicaron si se le debe tipificar dentro de un delito informático.

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

Un grupo minoritario de participantes indico que si se puede tipificar el delito de estafa dentro de los delitos informáticos y el otro grupo indico que no se puede tipificar porque tienen principios diferentes para su comisión, sin embargo todos coincidieron en que se debería modificar la norma a fin de que sea más exacta en cuanto a la comisión de estafa, dado que 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, brindándole una percepción errónea de la realidad.

En el artículo 248 de la (Codigo Penal de la Legislación Española), se consideran reos de estafa “los que, sin ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan transferencia no consentida de cualquier activo patrimonial en perjuicio de otro”.

V. CONCLUSIONES

Primera: Se determino que en el distrito de Ventanilla 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 informacion de las pericias de analisis digital forense solicitadas y desarrolladas, capacitacion a fiscales y policia 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.

VI. 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 formar 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 ciber seguridad 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 u amonestación económica.

Tercera: en relación a la realidad problemática, se recomienda que en el distrito de Ventanilla 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.

Cuarta: en relación a la hipótesis, se recomienda implementar órganos de apoyo tecnicos descentralizados, laboratorios de analisis forense informatico, base de datos con informacion de las pericias de analisis digital forense solicitadas y desarrolladas, capacitar a los fiscales penales y policias encargados de recolectar la evidencia digital.

Referencias

13° Congreso de las Naciones Unidas sobre prevención del delito y Justicia Penal. (2015). Obtenido de https://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_s_V1500666.pdf

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.

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

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%20se%20pudo%20determinar,cuenta%20con%20un%20respaldo%20normativo.

CASACIÓN 956-2017 Lambayeque (CORTE SUPREMA DE JUSTICIA DE LA REPÚBLICA Sala civil transitoria 10 de Abril de 2019). Obtenido de

https://img.lpderecho.pe/wp-content/uploads/2021/08/Casacion-956-2017-Lambayeque-LP.pdf

De la fuente, C. d. (2019). *Comunicación e imagen corportiva.* Editorial Elearning S.L .

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=2ahUKEwiUndThlNT3AhUgtJUCHU6tBBMQ6AF6BAgCEAI#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

Izquierdo Estrada, F. E. (2021). *Eficacia en las investigaciones fiscales de la ciberdelincuencia económica en tiempos de pandemia*. Obtenido de https://dspace.unitru.edu.pe/handle/UNITRU/17845

Jimenez, E. N. (2017). Guía para la preparación de proyectos de servicios públicos municipales. Obtenido de https://biblio.juridicas.unam.mx/bjv/detalle-libro/1430-guia-para-la-preparacion-de-proyectos-de-servicios-publicos-municipales

Jurisprudencia, M. p.-S. (2016). Consulta destacada Jurisprudencia Agosto 2016 - Delitos informaticos.

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/

Ley N° 30171 (10 de Marzo de 2014). Obtenido de https://www.gob.pe/institucion/minsa/normas-legales/197055-30171

Ley N° 30220. (9 de Julio de 2014). Obtenido de https://cdn.www.gob.pe/uploads/document/file/105207/_30220_-_09-07-2014_10_14_18_-Nueva_Ley_Universitaria.pdf

Madrid 23/2017 (10 de Enero de 2017). Obtenido de https://vlex.es/vid/672198853

Martín, A. N. (Julio de 2017). *Manual de evidencia digital*. Obtenido de https://www.mpfn.gob.pe/Docs/0/files/manual_evidencia_digital.pdf

Martinez Mediano , C., & Galan Gonzales , A. (2014). *Técnicas e instrumentos de recogido y análisis de datos.* Uned. doi:https://books.google.com.pe/books?id=iiTHAwAAQBAJ&dq=que+son+las+tecnicas+de+recoleccion+de+datos&source=gbs_navlinks_s

Martinez, C. (2018). Investigacion Descriptica: Tipos y Caracteristicas. Obtenido de https://s9329b2fc3e54355a.jimcontent.com/download/version/1545253266/module/9548087569/name/Investigaci%C3%B3n%20Descriptiva.pdf

Maya, R. P. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. *Nuevo foro penal No. 88 enero - Junio 2017 Universidad EAFIT*, 72-112. doi:https://dialnet.unirioja.es/descarga/articulo/6074006.pdf

MORI QUIROZ, F. (2019). *Los delitos informáticos y la protección penal de la intimidad en el distrito Judicial de Lima periodo 2008 al 2012.* Obtenido de http://repositorio.unfv.edu.pe/bitstream/handle/UNFV/3519/UNFV_MORI_QUIROZ_FRANCISCO_MAESTRIA_2019%20%283%29.pdf?sequence=1&isAllowed=y

Muñoz, J. J. (2019). *Derecho de danos tecnológicos, ciberseguridad e insurtech.* Madrid: Dykinson, S.L Melendez Valdes 61- 28015 Madrid 2019.

Noreña, A., Alcaraz-Moreno, N., Rojas, J. G., & Rebolledo-Malpica, D. (2012). Aplicabilidad de los criterios de rigor y éticos en la investigación cualitativa. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1657-59972012000300006

Ñaupas Paitán, H., Valdivia Dueñas, M., Palacios Vilela , J., & Romero Delgado, H. (2018). *Metodología de la investigación, Cuantitaiva-Cualitiva y redacción de la tesis*. Bogota: U. Obtenido de https://books.google.com.pe/books?id=KzSjDwAAQBAJ&pg=PA227&dq=que+son+los+aspectos+administrativos+en+tesis&hl=es-419&sa=X&ved=2ahUKEwiV1aWpjfH3AhVKH7kGHTLiDP84ChDoAXoECAcQAg#v=onepage&q&f=false

Ortiz Sánchez, L. M. (2020). *La teoría fundamentada como método de investigación para el desarrollo de la educación contable*. Revista Vision Contable N°22, Julio-Diciembre 2020. doi:https://doi.org/10.24142/rvc.n22a3

Pardo Vargas, A. (2018). *Tratamiento jurídico penal de los delitos informaticos contra el patrimonio, Distrito Judicial de Lima 2018.* Obtenido de https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf?sequence=1&isAllowed=y

Parra Sichaca, D. P. (23 de Octubre de 2019). *Universidad Católica de Colombia*. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/23853/1/Trabajo%20Prueba%20Digital%20aprobado.pdf

Piva Torres, G., Ruiz Carrero, W., & Lattuf Rodriguez , W. (2021). *La investigación del delito en el derecho penal Español, especial referencia a la teoría del caso.* Bosh editor, Barcelona 2021. Obtenido de https://books.google.com.pe/books?id=83o6EAAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

R.N N° 1936-2019 Lima (Sala Penal Transitoria Lima 12 de Mayo de 2021).

Reátegui Sanchez James. (19 de Febrero de 2022). *Delitos informáticos poder judicial, entrevista a Juez del juzgado de investigación prepatoria de la Corte superior de Lima*. Obtenido de https://www.youtube.com/watch?v=lVKVUSYtB3c

RECURSO DE NULIDAD N.° 206-2019 Lima (Sala Penal Transitoria 23 de Enero de 2020). Obtenido de https://img.lpderecho.pe/wp-content/uploads/2020/10/RN-206-2019-Lima-LP.pdf

RN N° 4727-2006 Lima (Segunda sala penal transitoria Lima 26 de Marzo de 2008).

Roberto Granero, H., Resqui Pizarro, J., Molina Quiroga, E., Sánchez Hernández, J., & Pérez Dudiuk, G. (2019). *E-Mails, chats, WhatsApps, SMS, Facebook, filmaciones con teléfonos móviles y otras tecnologías: Validez probatoria en el proceso civil, comercial, penal y laboral.* Obtenido de

https://books.google.com.pe/books?id=Uk1OEAAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Sentencia N° 00148 (Tercera sala de la corte suprema de justicia 24 de Febrero de 2006).

Sentencia nº 00763 / 2006, 02-017140-0042-PE (Sala 3ª de la Corte Suprema de Justicia, 18 de Agosto de 2006). Obtenido de https://vlex.co.cr/vid/-498988730

Serrano, C. L. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. *Lucerna Iuris Et Investigatio de la Facultad de Derecho y Ciencia Política de la Universidad Nacional Mayor de San Marcos*. doi:https://revistasinvestigacion.unmsm.edu.pe/index.php/Lucerna/article/view/18373/16528

Steckman, L. (2020). *Examining Internet and Technology Around the World.* ABC-CLIO llc. Obtenido de https://books.google.com.pe/books?id=f14MEAAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Strauss, A., & Corbin, J. (2002). *Bases de la investigacion cualitativa, Tecnicas y procedimientos para desarrollar la teoría fundamentada.* Editorial Universidad de Antioquia. Obtenido de https://books.google.com.pe/books?id=TmgvTb4tiR8C&pg=PA160&dq=categorias+en+la+investigacion+cualitativa&hl=es-419&sa=X&ved=2ahUKEwiU57GnkL_3AhVfFLkGHb7HD-0Q6AF6BAgDEAI#v=onepage&q&f=false

STS 49/2020 (12 de Febrero de 2020). Obtenido de https://vlex.es/vid/840632447

Sts N° 305/2019, Sentencia 1915-2019 (Organo tribunañ supremo, sala de lo penal Madrir 2019).

Ferro, J. N. (2020). *Cyberesionaje, Cyberestafas y Guerras informáticas El lado oscuro de Internet : la prueba digital.* Obtenido de https://books.google.com.pe/books?id=oovKDwAAQBAJ&pg=PT378&dq=d

elitos+informaticos&hl=es-419&sa=X&ved=2ahUKEwjj9Nqvg5r3AhX5K7kGHVMUA_k4ChDoAXoECAgQAg#v=onepage&q=delitos%20informaticos&f=false

Virú, Y. R., Chirinos, H. L., & Vilchez, J. M. (s.f.). *Contratación electrónica y los delitos informáticos. En protección al consumidor*. LEX N° 28 - AÑO XIX - 2021 - II / ISSN 2313 - 1861.

Yuni, J., & Urbano, C. A. (2006). *Tecnicas para investigar: recursos metodológicos para la preparación de proyectos de investigación.* Editorial Brujas segunda edición 2006. Obtenido de https://books.google.com.pe/books?id=XWIkBfrJ9SoC&pg=PA31&dq=tecnicas+e+instrumentos+de+recoleccion+de+datos&hl=es-419&sa=X&ved=2ahUKEwj3hcfQpsH3AhVhA7kGHcNIAogQ6AF6BAgJEAI#v=onepage&q=tecnicas%20e%20instrumentos%20de%20recoleccion%20de%20datos&f=false

ANEXOS

Anexo 1. Matriz de consistencia

Título: Valoración de los medios probatorios en los Delitos Informáticos del Distrito de Ventanilla del año 2021

Problema	**Objetivo**	**Hipótesis**	**Categoría**	**Metodología**
Problema General	**Objetivo General**	**Hipótesis general**		
¿Qué se necesita en el distrito de Ventanilla para obtener medios probatorios que ameritan ser obligatorios en los procesos relacionados a delitos informáticos?	Determinar que medios probatorios son indispensables en los procesos de delitos informáticos en el distrito de Ventanilla del año 2021.	• El Ministerio público no cuenta con los recursos suficientes para acreditar los delitos informáticos en el distrito de Ventanilla	• Delito patrimonial informático • Investigación preparatoria	Enfoque: Cualitativo
Problema especifico	**Objetivo especifico**	**Hipótesis Especifica**	**Sub categoría**	Tipo de investigación: Básica
¿Qué se necesita para continuar con la investigación preparatoria en los casos relacionados a delitos informáticos?	Determinar que se necesita en las investigaciones fiscales para procesar los casos relacionados a delitos informáticos en el distrito de Ventanilla.	Los conocimientos de los operadores de justicia del distrito de Ventanilla no son suficientes para imputar el delito informático.	○ Hurto ○ Estafa	Nivel de investigación: Descriptivo
¿Qué relación tienen el delito de hurto y el delito de estafa en los delitos informáticos?	Analizar la relación jurídica de los delitos de hurto y estafa en los delitos informáticos.	El delito de hurto y estafa se pueden tipificar dentro de los delitos informáticos.	○ Falta de conocimiento en herramientas de tecnología de información ○ Falta de fiscalías especializadas	Técnica e instrumento de recolección de datos: Guía de entrevista

Anexo 2. Matriz de categorización

Problemas	Objetivos	Categoría	Sub categoría
Problema general: Determinar ¿Qué se necesita en el distrito de Ventanilla para obtener medios probatorios que ameritan ser obligatorios en los procesos relacionados a delitos informáticos?	**Objetivo general:** Determinar que medios probatorios son indispensables en los procesos de delito informáticos	Delito patrimonial informático	Hurto Estafa
Problema específico: ¿Qué se necesita para continuar con la investigación preparatoria en los casos relacionados a delitos informáticos? ¿Qué relación tiene el delito de hurto y estafa en los delitos informáticos?	**Objetivo específico:** Determinar que se necesita en las investigaciones fiscales para procesar los casos relacionados a delitos informáticos Analizar la relación jurídica de los delitos de hurto y estafa en los delitos informáticos.	Investigación preparatoria	Falta de fiscalías especializadas Falta de conocimiento en el uso de herramientas tecnológicas de información

Anexo 3. Instrumento/s de recolección de datos

Guía de entrevista

Título: Valoración de los medios probatorios en los Delitos Informáticos del Distrito de Ventanilla del año 2021

Entrevistado (a): .....

Cargo: .....

Institución: .....

Problema general: Determinar ¿Qué se necesita en el distrito de Ventanilla para obtener medios probatorios que ameritan ser obligatorios en los procesos relacionados a delitos informáticos?

Objetivo General 1: Determinar que medios probatorios son indispensables en los procesos de delitos informáticos en el distrito de Ventanilla del año 2021.

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

   _____

   _____

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

   _____

   _____

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

   _____

   _____

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

   _____

   _____

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

Problema específico: ¿Qué se necesita para continuar con la investigación preparatoria en los casos relacionados a delitos informáticos?

Objetivo específico 1: Determinar que se necesita en las investigaciones fiscales para procesar los casos relacionados a delitos informáticos en el distrito de Ventanilla

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

   _____
   _____
   _____

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

   _____
   _____
   _____
   _____
   _____

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

   _____
   _____

Problema específico: ¿Qué relación tienen el delito de hurto y el delito de estafa en los delitos informáticos?.

Objetivo específico 2: Analizar la relación jurídica de los delitos de hurto y estafa en los delitos informáticos.

9. En su experiencia ¿Cree usted que se puede tipificar el delito de hurto dentro de los delitos informático?

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

    _____
    _____
    _____
    _____
    _____

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO POR JUICIO DE EXPERTOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Categoría 1: Delito patrimonial informático	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Qué factores obstaculizan las investigaciones en los delitos informáticos?	x		x		x		
2	¿Los fiscales cuentan con los recursos necesarios para realizar investigaciones completas de los delitos informáticos?	x		x		x		
3	¿Qué medios probatorios se necesitan para acreditar los delitos informáticos?	x		x		x		
4	¿Considera que dentro de los delitos informáticos se encuentran también los delitos de estafa y hurto?	x		x		x		
5	En su experiencia ¿Los bancos colaboran de alguna forma en las investigaciones relacionadas a los delitos informativos?	x		x		x		
	Categoría 2: Investigación preparatoria	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	¿Qué medidas necesita adoptar el Ministerio Publico y Policía Nacional del Perú para aplicar la norma en relación a los delitos informáticos?	x		x		x		
7	¿Qué deficiencias cree usted que existen en las investigaciones preliminares en los casos de delitos informáticos?	x		x		x		
8	¿cree usted que faltan capacitaciones y/o actualizaciones en las herramientas de las TICs para imputar los delitos informáticos?	x		x		x		
9	En su experiencia ¿Cree usted que se puede tipificar el delito de hurto dentro de los delitos informáticos?	x		x		x		
10	En su experiencia ¿Cree usted que se puede tipificar el delito de estafa dentro de los delitos informáticos?	x		x		x		

Observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: **Araya Muñoz, Sandra Jacqueline** **RUN: 9.981.699-6**

Especialidad del validador: Jefa de Unidad Técnico Pedagógico

Santiago 08 de Julio del 2022

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante.

Anexo 4

ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO POR JUICIO DE EXPERTOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Categoría 1: Delito patrimonial informático	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Qué factores obstaculizan las investigaciones en los delitos informáticos?	x		x		x		
2	¿Los fiscales cuentan con los recursos necesarios para realizar investigaciones completas de los delitos informáticos?	x		x		x		
3	¿Qué medios probatorios se necesitan para acreditar los delitos informáticos?	x		x		x		
4	¿Considera que dentro de los delitos informáticos se encuentran también los delitos de estafa y hurto?	x		x		x		
5	En su experiencia ¿Los bancos colaboran de alguna forma en las investigaciones relacionadas a los delitos informativos?	x		x		x		
	Categoría 2: Investigación preparatoria	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	¿Qué medidas necesita adoptar el Ministerio Publico y Policía Nacional del Perú para aplicar la norma en relación a los delitos informáticos?	x		x		x		
7	¿Qué deficiencias cree usted que existen en las investigaciones preliminares en los casos de delitos informáticos?	x		x		x		
8	¿cree usted que faltan capacitaciones y/o actualizaciones en las herramientas de las TICs para imputar los delitos informáticos?	x		x		x		
9	En su experiencia ¿Cree usted que se puede tipificar el delito de hurto dentro de los delitos informáticos?	x		x		x		
10	En su experiencia ¿Cree usted que se puede tipificar el delito de estafa dentro de los delitos informáticos?	x		x		x		

Observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: Godoy Godoy, Claudia Marjorie

RUN: 12.161.025-6

Especialidad del validador: Maestría en dirección educacional

Lima 08 de Julio del 2022

Firma del Experto Informante.

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO POR JUICIO DE EXPERTOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Categoría 1: Delito patrimonial informático	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Qué factores obstaculizan las investigaciones en los delitos informáticos?	x		x		x		
2	¿Los fiscales cuentan con los recursos necesarios para realizar investigaciones completas de los delitos informáticos?	x		x		x		
3	¿Qué medios probatorios se necesitan para acreditar los delitos informáticos?	x		x		x		
4	¿Considera que dentro de los delitos informáticos se encuentran también los delitos de estafa y hurto?	x		x		x		
5	En su experiencia ¿Los bancos colaboran de alguna forma en las investigaciones relacionadas a los delitos informativos?	x		x		x		
	Categoría 2: Investigación preparatoria	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	¿Qué medidas necesita adoptar el Ministerio Publico y Policía Nacional del Perú para aplicar la norma en relación a los delitos informáticos?	x		x		x		
7	¿Qué deficiencias cree usted que existen en las investigaciones preliminares en los casos de delitos informáticos?	x		x		x		
8	¿cree usted que faltan capacitaciones y/o actualizaciones en las herramientas de las TICs para imputar los delitos informáticos?	x		x		x		
9	En su experiencia ¿Cree usted que se puede tipificar el delito de hurto dentro de los delitos informáticos?	x		x		x		
10	En su experiencia ¿Cree usted que se puede tipificar el delito de estafa dentro de los delitos informáticos?	x		x		x		

Observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: María del Carmen Sanchez Delgado

Especialidad del validador: Maestro con mención en docencia universitaria

Lima 08 de Julio del 2022

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión