UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Delitos informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestra en Derecho Penal y Procesal Penal

AUTORA:

Anicama Arones, Yessica Angelica (orcid.org/0009-0006-4863-7731)

ASESORES:

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

Mg. Perez Gonzales, Wilmer Lino (orcid.org/0000-0002-9414-128X)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal, Procesal Penal, Sistema de Penas, Causas y Formas de Fenómeno Criminal

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía

LIMA - PERÚ

2023

DEDICATORIA

La presente investigación está dedicada a Dios por darme la fortaleza necesaria durante todo este tiempo y especialmente a mi madre expresarle mi profunda gratitud por su apoyo constante e incondicional, por sus sabios consejos, su gran ejemplo de vida, perseverancia y dedicación que ha sido mi base e inspiración, que me permite seguir para cumplir con mis objetivos. Dedicado con todo mi amor y gratitud.

AGRADECIMIENTO

Expreso mi agradecimiento y reconocimiento a las instituciones que han mostrado su apoyo incondicional y contribución en la elaboración de la presente investigación, a la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, y a la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), quienes ha sido pieza fundamental como participantes que generosamente compartieron su tiempo y conocimientos para hacer posible la investigación. Así mismo a los profesionales que han contribuido con sus conocimientos en la ejecución de la investigación, a mi docente asesor quien ha brindado valiosos comentarios y sugerencia durante la investigación, a todos mis más sinceros agradecimientos.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La investigación tuvo como objetivo general: Analizar los delitos informáticos perpetrados por medio de la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022, la metodología de la investigación fue de enfoque cualitativo, de tipo básica y de diseño fenomenológico, porque se basa en estudios experimentales reales, se contó con 13 participantes entre fiscalía, DIVINDAT y abogados. Como técnica se empleó la entrevista y como instrumento la guía de entrevista validada por expertos. De acuerdo a los resultados los delitos informáticos permiten establecer una relación directa con la criminalidad económica, causando un perjuicio a las víctimas. Se concluyó que los delitos informáticos, puede vincularse directamente la propiedad, tienen impacto en los sistemas informáticos y en la economía; se deben implementar nuevas políticas públicas, haciendo uso de las nuevas tecnologías para hacer un frente, ante el incremento de delitos informáticos en los últimos años, conforme los datos obtenidos de las instituciones públicas del Estado. Finalmente se recomienda evaluar la expansión de las Fiscalizas Especializadas en Ciberdelincuencia a nivel nacional, en cuanto al Poder Judicial, evaluar la implementación de juzgados especializados en delitos cibernéticos con personal debidamente capacitado para desempeñarse en casos y delitos cometidos utilizando los medios tecnológicos.

Palabras clave: Delitos informáticos, tratamiento judicial, tratamiento fiscal, ministerio público, poder judicial.

ABSTRACT

The general objective of the research was: To analyze computer crimes perpetrated through cybercrime with the use of new technologies in Lima Centro 2022, the research methodology was qualitative, basic and phenomenological design, because it is based on real experimental studies, there were 13 participants including the prosecution, DIVINDAT and lawyers. The interview was used as a technique and the interview guide validated by experts as an instrument. According to the results, computer crimes allow establishing a direct relationship with economic crime, causing harm to the victims. It was concluded that computer crimes, property can be directly linked, have an impact on computer systems and the economy; New public policies must be implemented, making use of new technologies to deal with the increase in computer crimes in recent years, according to data obtained from public institutions of the State. Finally, it is recommended to evaluate the expansion of Specialized Cybercrime Prosecutors at the national level, in terms of the Judiciary, to evaluate the implementation of courts specialized in cybercrime with duly trained personnel to work in cases and crimes committed using technological means.

Keywords: Cybercrime, court treatment, tax treatment, public ministry, power of attorney.

I. INTRODUCCIÓN

La tecnología informática, es una herramienta de mayor alcance en la sociedad, estando que a través de estas plataformas (internet) conectan entre sí. Sin embargo, esta herramienta está siendo utilizada de manera incorrecta, estando que el crimen organizado se incrementó debido a los cambios de vida propiciado por la Pandemia Covid-19, que nos conllevó a manejar las plataformas digitales, que trajo consigo muchos beneficios, pero que también abrió un espacio para el incremento de los delitos cibernéticos cuyo accionar ha desbordado las fronteras.

En el contexto internacional, el perfeccionamiento de la tecnología y su uso, se ven reflejados en actos ilegales y delictivos. El surgimiento de nuevos tipos delictivos y nuevas formas de cometer delitos tradicionales determina que cada vez más bienes jurídicos protegidos por el derecho penal puedan verse comprometidos por quienes aprovechan los avances científicos para delinquir (Fernández, 2018). Según la Asamblea General de la UNESCO (2019), la puerta está abierta a los ciberdelincuentes con avances tecnológicos, que producen expansión del nivel y la diversidad de delitos.

El delito cibernético va en aumento, destruye economías y medios de vida de las personas y comete actividades ilegales. Es por eso que las organizaciones están luchando para detener esta práctica y mantenerse a salvo. Fernández (2018) dijo que en Europa se encuentra el más alto índice de ciberdelincuentes, que tienen su sede en Europa, siendo Estados Unidos el país más afectado por los piratas informáticos. Los piratas informáticos rusos son personas tecnológicas que buscan nuevas formas para burlar la seguridad tecnológica.

En el ámbito nacional, Pardo (2018), refirió que en las investigaciones que guardan relación con este tipo de delitos, advierte que no existe un mecanismo idóneo, toda vez que no se cuenta con los medios tecnológicos para llevar a cabo las pericias que corresponde para cada caso en concreto. Por ende, en el año 2021, fue creada la “Fiscalía Especializada en Ciberdelincuencia de Lima Centro con Resolución de la Fiscalía de la Nación Nº 843-2021- MP-FN, del 08 de junio del 2021, modificada con Resolución Nº 848- 2021-MP-FN, con

la intención de brindar a la colectividad una asistencia eficaz y eficiente en la obtención de una buena gestión de justicia para que no haya vulneración de sus derechos por esta nueva modalidad delictivita que hacen mal uso de la tecnología.

En ese contexto, estos delitos, tienen un mayor alcance, tales como fraude, robo, chantaje, falsificación entre otros y su principal modo de operación se viene dando con el uso de la implementación de nuevos métodos tecnológicos “internet y redes” que a través de los programas o aplicaciones permiten grandes beneficios en la vida del ser humano pero que también puede ser contraproducente al existir personas inescrupulosas denominadas delincuentes cibernéticos, que se valen del uso de la tecnología para afectar la seguridad, integridad y bienestar de la ciudadanía.

Bajo ese panorama, la investigación trazó la formulación del problema; que tuvo como problema general: ¿Cuáles son los delitos informáticos perpetrados por medio de la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022?; así mismo se planteó los siguientes problemas específicos: P.E.1. ¿Cuáles son los delitos más comunes y de mayor alcance dentro de los delitos informáticos y la ciberdelincuencia?; P.E.2. ¿Cuáles son los mecanismos jurídicos para Implementar la Ley 30096 en los Delitos Informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022?; P.E.3. ¿Existe un procedimiento fiscal y judicial que se adopta en los delitos informáticos y la ciberdelincuencia?

Asimismo, encuentra su justificación toda vez que se trata de poner en claro un problema que ha ido creciendo a un ritmo acelerado en los últimos años, causando daños económicos a la sociedad. En cuanto a su justificación teórica, encuentra su justificación en el ordenamiento jurídico democrático, ya que el ser humano es el fin supremo establecido por nuestra constitución política peruana, por ello es importante que se garanticen los derechos reconocidos, así como los relacionados con los sistemas informáticos. Por tanto, la investigación aportará la información recabada para conocer las razones del aumento de los delitos informáticos y ciberdelincuentes con el fin de mantener la prevención y tomar medidas eficaces frente al problema.

En cuanto a la justificación práctica, será de utilidad siempre que se pretenda hacer valer nuevos mecanismos informáticos que protejan la seguridad jurídica. En cuanto a la justificación metodológica, la investigación ha recopilado información bibliográfica relevante para su análisis y clasificación, ya que los resultados de este estudio son útiles a nivel metodológico y permitirán que este estudio sea utilizado por otros interesados en ampliar su contenido. En la justificación social, se fundamenta en el aporte a la sociedad, que es la principal parte victimizada, para que sepa prevenir este tipo de delitos, y el fundamento jurídico final radica en la determinación de la Ley N° 30096, “Ley de Delitos Informáticos” y sus reformas para prevenir Delitos informáticos y ciberdelitos que van en incremento.

En este contexto, los delitos informáticos se han desarrollado de manera alarmante y ha traspasado fronteras, hoy el mundo vive en la era digital y con ello el mundo de internet, y los delincuentes se benefician de este cambio digital y del uso de las tecnologías en los ataques para atacar a las víctimas y causan daño y por ende se tiene grandes consecuencias económicas para lograr los fines previstos.

Para abordar el tema, se planteó el objetivo general: Analizar los delitos informáticos perpetrados por medio de la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022; y objetivos específicos: O.E.1. Analizar los delitos más comunes y de mayor alcance dentro de los delitos informáticos y la ciberdelincuencia; O.E.2. Determinar los Mecanismos Jurídicos para Implementar la Ley 30096 en los Delitos Informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022; O.E.3. Analizar el procedimiento fiscal y judicial que se adopta en los delitos informáticos y la ciberdelincuencia.

II. MARCO TEÓRICO

De acuerdo al tema de investigación, en el contexto internacional se tiene a Rodríguez (2020), se tiene una aproximación *"phishing"* que es una técnica que permite acceder a las cuentas o datos bancarios, siendo uno de los métodos más comunes para cometer delitos basados en el engaño con el fin de inducir al error a la víctima y causar un daño económico. Es por ello que el "Consejo de la Unión Europea", ha realizado operaciones con la finalidad de que estas acciones sean tipificadas como delitos, ya que el propósito de lucro y fraude informático se realiza por medio de la tecnología y se realiza mediante envío sin autorización, que se le denomina "la defraudación económica" como parte del manejo de la informática. Esta técnica, lo hace un agente llamado porteador que se encarga de procesar y transferir el dinero generado por el fraude informático, por lo que el tribunal considera que se trata de una manipulación de *hardware* y *software* que se calcula para obtener datos.

En México, Vences (2019), señala que la informática actualmente es importante para el desarrollo de los individuos, pero debe conocerse sus alcances y las consecuencias, puesto que la cobertura puede provocar ser víctima de los delitos cibernéticos. Asimismo, refiere que la informática es una de las ciencias con mayor desarrollo y evolución en la actualidad, pues su implementación ha cambiado la vida del ser humano, sin embargo, también ha traído consigo la realización de conductas de carácter ilícito e ilegal como lo son el delito cibernético, que afectan a muchas personas que hagan uso de las tecnologías con el simple hecho de conectarse a internet.

En Colombia, Ospina y Sanabria (2020), refiere que los delitos informáticos, se presenta diversas amenazas cibernéticas que fue en aumento a razón de la pandemia, es por ello que el autor plantea promover políticas sólidas de seguridad para salvaguardar la información de los ciudadanos y organizaciones, y que debe verse reflejado en las nuevas leyes de uso de software, el perfeccionamiento de denuncias y las sanciones de los delitos informáticos ante un nuevo cambio.

En Argentina, Horianski (2021), sobre los delitos informáticos, refiere que no se entienden porque no hay bienes jurídicos protegidos por la ley y en un

principio era imposible castigar los ciberdelitos, pero a medida que avanza la tecnología aparecen nuevas formas y es necesaria una nueva normativa para proteger a la ciudadanía frente a los ataques de los ciberdelitos, bajo la delincuencia informática.

Ecuador, Saraguro (2021), sobre la ciberdelincuencia, señala que es importante invertir, prepararse para fortalecer la investigación sobre los métodos de detección de relaciones que provocan delitos informáticos, también es importante capacitar y preparar a expertos en este campo para que intervengan como especialistas con el fin de lograr el máximo éxito y obtener los mejores resultados.

En Colombia, Valencia (2020), concluyó que se tiene que comprender la nueva realidad de cómo opera la ciberdelincuencia, ya que este delito computarizado es a través de medios electrónicos, y aunque ya no estando en pandemia se sigue produciendo; teniendo como resultados que la sociedad y el ser humano crece de la mano de la tecnología por lo que las normativas penales deben adecuar sus estándares a la realidad social.

En el ámbito nacional, se tiene a Canelo (2022), concluyó que, a raíz de la pandemia, se determinó que el fraude informático fue el principal delito cometido, aumentando los niveles de mercadeo electrónico y compras a través de aplicaciones y tiendas en línea. Desde otro ángulo, se determinó que las investigaciones de estos delitos fueron archivadas por falta de pruebas o por la imposibilidad de identificar al autor material del hecho delictivo. Esta investigación ha contribuido con aportes, para que tanto los juzgados como los fiscales especializados en ciberdelincuencia puedan generar cambios y que este tipo de delitos no queden impunes.

Sotomayor (2022), sobre el delito informático, precisó que en la investigación fiscal, se desnaturaliza y termina siendo formalizado como hurto agravado; por ende, debe buscarse incentivar para crear fiscalías especializadas en ciberdelincuencia y su calificación para que las denuncias sean evaluadas por profesionales altamente capacitados y entrenados para este tipo de investigaciones.

Carrera (2021), enfatizó que la falta de actualización de la norma, la implementación de áreas de investigación con equipos de alta tecnología que brinden métodos efectivos para la identificación del autor del hecho delictivo, y la falta de instrucción de los agentes involucrados en la investigación, son un blanco accesible para perpetrar los delitos informáticos.

Chilcon (2021), llega a la conclusión que, en el Perú, el nivel alcanzado por el cibercrimen afecta significativamente a la seguridad nacional, su estructura informática, la protección de data y sus fines; dicha investigación tiene aporte en que es conveniente desarrollar nuevas políticas de control de información.

Huamán (2020), afirma que la suscripción del “Convenio de Budapest”, hacer caer la balanza sobre el procedimiento de los delitos informáticos y el desarrollo de la ley de delitos informáticos en el Perú y que el problema actual causado por los delitos informáticos es cada vez mayor debido a el acceso y uso de diversas herramientas tecnológicas.

Gómez (2020), refiere que, dada la complejidad y especificidad de los delitos informáticos, su tratamiento jurídico requiere una adaptación constante de las normativas legales existentes. De este modo, el sistema jurídico se enfrenta al reto de establecer mecanismos vigorosos para la aprensión, investigación y sanción de este tipo de conductas.

Condori y Rufino (2020), concluyo que el fraude informático genera daños negativos, debido a que, en la mayoría de los asuntos de averiguación en la fiscalía, no es posible identificar al autor fraudulento del hecho ilícito. Siendo de recomendación que los administradores de justifica forjen esfuerzos con solidaridad y cooperación interinstitucional a fin de planificar y establecer oportunamente los lineamientos y protocolos a la par de la tecnológica, a fin de tener mayores alcances y posibilidades para enfrentar de manera más efectiva el ciberdelito.

Por otro lado, en relación a las teorías y los enfoques conceptuales donde se enmarca la investigación, se tiene como primera categoría “los delitos informáticos”, de la cual cabe indicar que es un término ampliamente utilizado para describir acciones que implican el uso de la información y la tecnología, así como el quebrantamiento de un bien jurídico, ya que parece que la mayoría

de estos delitos vulneran el derecho informático de forma delictiva y, por tanto infringiendo la ley porque con el desarrollo de la ciencia, cada día aparecen nuevos métodos para vulnerar la tecnología (Bayardo & Hermoza, M. M. (2019)

En derecho penal, el número de delitos de información es definido como un concepto amplio y complejo, ya que incluye no solo el derecho civil, sino también el derecho penal. Asimismo, se pueden definir como aquellos actos ilegales que se ejecutan manipulando la tecnología de la información y las comunicaciones. Estos actos pueden involucrar el acceso a sistemas informáticos, la manipulación de datos, el robo de información personal o financiera, el fraude y muchas otras formas de actividad delictiva, que se relacione o tenga relación con datos o procedimientos de ejecución, que afectan los componentes electrónicos y el procesamiento” (Dass, 2019).

El cibercrimen, es una actividad ilícita que vulnera la seguridad de la información y el resguardo de los derechos humanos básicos a través del tratamiento no autorizado de la información, lo que se refleja en diversos incidentes de delincuencia electrónica. Por tanto, los delitos informáticos pueden definirse como la utilización habitual, ilícita y demostrablemente delictiva de medios de información, con o sin finalidad. Frente a esta figura se promulgo la Ley 30171, que modifica la Ley 30096, que busca adecuarse al Convenio de Budapest, con la finalidad de garantizar el goce del derecho a la libertad y desarrollo, para hacerle frente a la ciberdelincuencia (Santisteban & Andrade, 2019).

Hay diferentes delitos informáticos y en la opinión de Camacho Losa citado por Acurio, afirma que el único límite que existe es una combinación de factores "La falta de imaginación del autor, su habilidad técnica y el control existente del sistema informático". En la ciberdelincuencia, los bienes jurídicos protegidos se entienden de manera amplia, donde se expone información (base de datos) de manera general y se afectan bienes jurídicos. La información debe ser un producto consistente en una base de datos o un proceso informático automatizado para ser incluida como propiedad jurídica protegida debido al valor económico de la información.

Por otro lado, el delito de estafa informática también incide en la enorme legitimidad que otorga a otros ciberdelitos conocidos como "oportunidades informáticas". Este recurso es especialmente importante porque la mayoría de estos delitos utilizan Internet como lugar de comisión (Mayer y Oliver, 2020).

La Corte Suprema, por su parte, ha señalado en diversas sentencias que las lesiones psíquicas que afectan la integridad de la personalidad de una persona y los diversos tratos inhumanos que atentan y destruyen la integridad de una persona son derechos humanos internacionalmente reconocidos. También muestra la importancia del gobierno como ente regulador y provoca la protección de la integridad personal con el fin de desarrollar diferentes estrategias para combatir estos delitos.

De la información proporcionada por DIVINDAT, se resalta que, respecto a las denuncias recibidas, se tiene por acceso ilícito, suplantación de identidad y delitos informáticos contra la intimidad y el secreto de comunicaciones, puesto que durante el año 2020 recibieron 4168 denuncias, en lo que corresponde al año 2021 se tiene 5620 denuncias, en el año 2022, 4010 y respecto al 2023, se tiene 1816 denuncias en lo que va de la mitad del año.

Con relación a la segunda categoría "tratamiento de la actuación fiscal", el sistema penal regula la investigación previa a la formalización de la investigación, el cual exige que el fiscal que previamente dirigió la investigación adopte medidas eficaces para determinar si la supuesta actividad ilícita es o no delictiva. Sin el correcto procedimiento de investigación, no se puede formalizar la investigación ni iniciar acción penal en contra del responsable de la comisión del delito informático (Coronado y Segura, 2018).

Núñez y Carhuancho (2017), refieren que la investigación fiscal no solo se desenvuelve en base a escenarios teóricos, sino que también se desarrollan en sociedades donde coexisten muchas relaciones humanas que son titulares de derechos, y delimitan claramente sus límites para evitar la vulneración de los derechos.

El Ministerio Público antes de establecer los hechos, realiza una investigación de los hechos alegados para probar la existencia de un delito y para este

propósito puede tomar una posición para determinar los hechos, ejercer la debida diligencia y lo más importante tratar de verificar lo que se ha hecho a través de investigaciones, rastros, tipo de delitos y determinar si existen delitos (Sánchez, Fernández y Díaz, 2021).

Estos factores han llevado al Ministerio Público, a cumplir con su mandato constitucional de establecer un grupo de trabajo especial para combatir este tipo de delitos, proteger los derechos de las personas, llevar a los perpetradores ante la justicia y, por lo tanto, poner fin a la delincuencia negra, legalmente obligada a hacerlo. Este tipo de actividad ilegal no ha sido debidamente considerada por las autoridades delegadas de la persecución e indagación.

La Fiscal Superior de los Fiscales de Delitos Cibernéticos, Aurora Castillo Fuerman (Coordinadora de la Unidad de Delitos Cibernéticos del Ministerio Público), manifestó en una entrevista que se realiza una capacitación continua a los fiscales a fin de que tengan especialización para el tratamiento de estos delitos y obtener excelentes efectos considerables en la lucha contra el cibercrimen (Avalos, 2020)

Respecto de la tercera categoría “Tratamiento Judicial”, Villavicencio (2021), señala que, el Poder Judicial, que administra justicia, está obligado a hacer cumplir la ley, a pesar de su lento ritmo de cambio. Las organizaciones del crimen organizado, por otro lado, tienden a adoptar nuevas tendencias rápidamente y se benefician enormemente de ellas. Lo mismo ocurre con la ineficiencia del sistema judicial, que no se puede solucionar únicamente con medios tecnológicos. En cambio, urge dotar de más recursos materiales y humanos, lo que sin duda eliminará algunas de las barreras que, a la hora de resolver los problemas judiciales, los problemas de hoy tienen el mismo peso que los del pasado.

Asimismo, conforme a los estados procesales de los delitos informáticos, estos pueden encontrarse archivados, en curso, sobreseída, terminada anticipadamente, juicio oral o con sentencia. Se descubre que los motivos del archivo se deben a la falta de cooperación de los afectados, la dificultad para localizar a los infractores y la desarticulación de las instituciones públicas y

privadas (Ministerio Público Fiscalía de la Nación, 2021).

Para Elías Puelles, la falta de fiscales y policías con experiencia en informática y ciberdelincuencia es otra señal de estancamiento procesal. También señaló el experto que solo existen dos unidades policiales de la DIVINDAT, lo que sustenta la afirmación de que los operadores carecen de los conocimientos necesarios para solicitar información a las redes sociales, sitios web o hosting donde se guarda la información de los usuarios. En estos casos, hay 150 efectivos en Lima y 23 en Arequipa, pero solo 70 de ellos son especialistas en ciberdelincuencia, según el Diagnóstico Multisectorial sobre Ciberdelincuencia (2020). Por lo tanto, debido al aumento en el número de víctimas, no hay suficientes especialistas para investigar, lo que indica un claro vacío en el manejo de las denuncias.

De la información proporcionada por la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro respecto a los delitos informáticos y la ciberdelincuencia, se tiene que en el periodo comprendido del 15 junio a 2022, se ha tenido un total de 5063 casos archivados, 3 casos concluidos por principio de oportunidad, 42 casos concluidos por terminación anticipada, 2 casos en etapa de juicio oral y 44 con sentencia. Como puede ver en estos números, las denuncias por delitos cibernéticos están creciendo exponencialmente; sin embargo, terminan siendo archivadas por la dificultad de encontrar a los autores del delito y esto se debe por no contar con una cobertura más amplia en tecnología. Los problemas se concentran en la etapa preliminar, y al no contar con los suficientes elementos para continuar con la investigación, se concluye con el archivamiento de la investigación.

Finalmente, de la información brindada por la Presidencia de la Corte Superior de Justicia de Lima, mediante Proveído N°1370-2023-SG-CSJLI-PJ, del periodo comprendido en el año 2020 al 2022 por delitos informáticos y ciberdelincuencia en Lima centro, se tiene 111 casos archivados y 141 casos sentenciados. (Corte Superior de Justicia de Lima 2023).

III. METODOLOGÍA:

3.1. Tipo y diseño de investigación

3.1.1. Enfoque de investigación: Tuvo un enfoque cualitativo, porque su propósito es recopilar y resumir toda la información posible relacionada con nuestro tema y comparar la información con la respuesta del experto (Arias, 2020).

3.1.2. Tipo de investigación: Es de tipo básica, porque busca ampliar la información, con el objetivo de incrementar conocimientos respecto al tema de investigación, ya que se utiliza para recopilar datos de modo que se puedan generar nuevos datos. Porque es un conocimiento que será de utilidad para futuras investigaciones. (Baena, 2017).

3.1.3. Diseño de investigación: Fue fenomenológico en cuanto se basa en estudios experimentales reales, ven los acontecimientos desde la fijación del sujeto; este diseño se base en el análisis y discusión de las invenciones de temas específicos y sobre todo encuentran, a través de la teoría de los métodos analíticos, distinguir limitaciones a los mismos (Fuster, 2019).

3.2. Categorías, Subcategorías y matriz de categorización

Estaban relacionadas con el tema de investigación lo que ayudó a desarrollar el marco teórico y producto de ello surgió la posibilidad de plasmar una matriz de consistencia (Quevedo, 2017).

La categorización, es una parte esencial del análisis e interpretación de los resultados, por ende, se trazó categorías y sub categorizas para dicho alcance.

Tabla 1

Categorías y subcategorías

Categoría	Subcategorías

Delitos informáticos	• Delitos informáticos establecidos en la Ley 30096 • Causas del incremento de los delitos informáticos • Bien jurídico protegido
Tratamiento Fiscal	• Evaluación de los hechos • Elementos de convicción
Tratamiento Judicial	• Estado procesal de los delitos informáticos • Motivo de archivamiento

3.3. Escenario de estudio

Es fundamental para las preguntas descritas en la introducción de toda investigación, ya que sus recomendaciones se reflejarán a lo largo de la disertación, así lo ha señalado (Arias, 2020).

La investigación se realizó en Lima Centro y se aplicó los instrumentos de recolección de datos a la fiscalía y División de Investigación de Delitos de Alta Tecnología (DIVINDAT).

La Fiscalía o el Ministerio Público, considerado un organismo autónomo del Estado, que representa los intereses de la sociedad y tiene como objetivo que se cumpla con la Ley y garantizar la justicia en el estado de derecho.

Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, especializada en tratar los delitos informáticos.

La División de Investigación de Alta Tecnología (DIVINDAT), se encarga de los aspectos técnicos y operativos que se relacionen con los delitos informáticos y todo lo que versa entorno a la tecnología de la información.

3.4. Participantes

Es la población que se indaga para recolectar los datos (Hernández y Mendoza, 2018). Los participantes fueron los que laboran en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, agentes policiales de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), y abogados especialistas en derecho penal y procesal penal.

Tabla 2

Participantes:

Código	Nombres y Apellidos	Cargo
P1	**Jonathan Cirilo Portillo Vela**	Fiscal Provincial
P2	**Angélica Lorena Pérez Ascencio**	Fiscal Adjunta Provincial
P3	**Jesús Pedro Ojeda Valdiviezo**	Fiscal Adjunto Provincial
P4	**Jessica Pamela Cajo Rodas**	Asistente en Función Fiscal
P5	**Raúl Víctor Caparachin Runachagua**	Asistente en Función Fiscal
P6	**Elizabeth Brigitte Melgar Ferreyra**	Asistente Administrativo
P7	**Kimberly Dakini Madueño Oscorima**	Asistente Administrativo
P8	**Walter Ismael Díaz Rufasto**	Capitán PNP Investigador
P9	**Edwin Ríos Crisosotmo**	Sub Oficial Superior PNP
P10	**Paul William Sabrera Álvarez**	S1 PNP
P11	**Julia Elisa Redhead Meza**	SS PNP
P12	**Claudia Maricela Díaz Gómez**	Abogado
P13	**Percy Alfredo Tapia Rodríguez**	Abogado

3.5. Técnicas e instrumentos de recolección de datos

Permite a los investigadores recopilar toda la información necesaria relacionada con su tema, utilizando teorías, libros, artículos académicos, documentos, documentos, etc. que contribuyen a la producción de datos importantes. Según el tipo de investigación, puede que no sea posible omitir una entrevista o un cuestionario. (Quevedo, 2017).

Se utilizó una técnica de entrevista con una guía de entrevista que sirvió como herramienta para la recopilación de información. La guía de entrevista contenía

15 preguntas relevantes y se adaptó a las subcategorías, categorías y temas de investigación.

- Técnica: La entrevista, mediante la comunicación que se establece directamente entre los investigadores y los colaboradores de la investigación.
- Instrumento: La guía de entrevista, este es un documento escrito por el entrevistador para guiar la entrevista y contiene una lista de preguntas que se harán durante la entrevista.

3.6. Procedimiento

En cuanto al procedimiento, cabe señalar (Arias, 2020), que involucra el uso de diferentes métodos para la obtención de los resultados. La investigación cualitativa requiere el uso de diferentes estrategias. Por lo tanto, el procedimiento verificó diversas fuentes primarias, realizó entrevistas a 13 participantes de la fiscalía, la DIVINDAT y abogados, y realizó verificaciones bibliográficas como fuentes secundarias. Tiene reputación y repositorios de universidades licenciadas por la SUNEDU.

Para aplicar el instrumento, se solicitó autorización al Ministerio Público de la Nación - Unidad Fiscal Especializada en Ciberdelincuencia y al Departamento de la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú, mediante una carta de presentación, la misma que tuvo la debida autorización mediante documentación otorgando la fecha y periodo para la debida aplicación, así mismo mediante una hoja de ruta se visitó a cada una de las entidades antes mencionadas para la aplicación del instrumento y a los abogados especialistas en la materia; la aplicación se realizó de manera directa presencial, y finalmente con la guía de entrevista, se obtuvo los datos.

3.7. Rigor científico

Es equivalente al valor y confiablidad de la investigación cualitativa, la misma que ha sido certificada por 03 jueces expertos (Tabla 3), se elaboró de forma objetiva bajo los siguientes discernimientos que dan la eficacia de rigor científico: la credibilidad, es una actividad proporcionada por expertos a los investigadores que identifican las categorías, las entrevistas y las tablas de

análisis de documentos como ideales y, por lo tanto, apropiados para usar en el presente estudio porque se recolectaron los datos correctos sin alterarlos. (Tamayo, 2002). Asimismo, la confiabilidad, los diferentes estándares de los investigadores se basan en la evidencia, sin sesgos ni prejuicios, y esto se demuestra al aceptar una de las posiciones propuestas o si nos oponemos a la posición inicialmente establecida, lo que a su vez nos permite observar la propia situación de discusión que suscita la autora. Análisis de investigación (Viorato y Reyes, 2019). Finalmente, la dependibilidad autenticar la aplicación donde también hay evidencia de diferentes posiciones para ayudar en la investigación. (Arias, 2020).

Tabla 3

Expertos validadores:

Nombres y Apellidos	Institución / Centro de Labores	Cargo	Grado
Roció Rosario Gines Aliaga	Poder Judicial / Corte Superior de Justicia de Lima Este	Magistrada de Juzgado Unipersonal	Maestra en Derecho Penal
Javier Enrique Reyna de la Cruz	Universidad Nacional del Santa	Docente Universitario	Maestro en Derecho Penal y Ciencias Criminológicas
Lucery Yameli Paz Ortega	Poder Judicial / Corte Superior de Justicia de Ica	Especialista Judicial de Juzgado	Maestra en Derecho Penal y Procesal Penal

3.8. Método de análisis de datos

Describe e instaura los datos disponibles que se recolectaron en función a las preguntas de la investigación y ser interpretados. (Narkhede, 2020). La información utilizada, fue a través del proceso de sistematización toda vez que contrasta las respuestas obtenidas a partir del punto de vista por los expertos y que luego ha sido interpretada por diferentes perspectivas de los intervinientes, por lo que se aplicó el método descriptivo para analizar los datos e identificar los aspectos importantes del estudio.

La información ha sido procesada a través del *software (*Atlas ti v.23). Es una herramienta tecnológica y técnica diseñada para brindar apoyo en investigaciones cualitativas, facilitando la organización, análisis e interpretación de datos. Este programa permite gestionar y estructurar grandes volúmenes de información en diversos formatos digitales. Además, posibilita el contraste y la comparación de datos, optimizando así el tiempo dedicado a la investigación y potenciando el trabajo colaborativo mediante elementos de análisis y herramientas para equipos de trabajo.

3.9. Aspectos éticos

La investigación estuvo diseñada bajo mecanismos establecidos por la Universidad Cesar Vallejo, cuyo contenido es auténtico y ha sido viabilizadas por el asesor. Asimismo, sigue los lineamientos establecidos en la Norma APA en su séptima edición. Asimismo, se rige por los principios éticos: principio de autonomía, los participantes han mostrado su consentimiento para la participación de la presente investigación; el principio de beneficencia, mediante la presente investigación se ha realizado en beneficios de la población y el Estado como agraviados frente al delito materia de investigación, mediante la cual los participantes también obtienen un beneficio con el estudio realizado; el principio de no maleficiencia, la investigación realizada bajo *primum non nocere,* es decir “lo primero es no hacer daño”; se realizó un análisis previo, no se ha dañado a ninguna persona y se ha respetado la integridad de los participantes; el principio de justicia, en la investigación el trato ha sido de forma igualitaria para todos los participantes. De esa forma respetando y cumpliendo con los principios ético con la finalidad de realizar un buen desarrollo y obtener un mejor resultado.

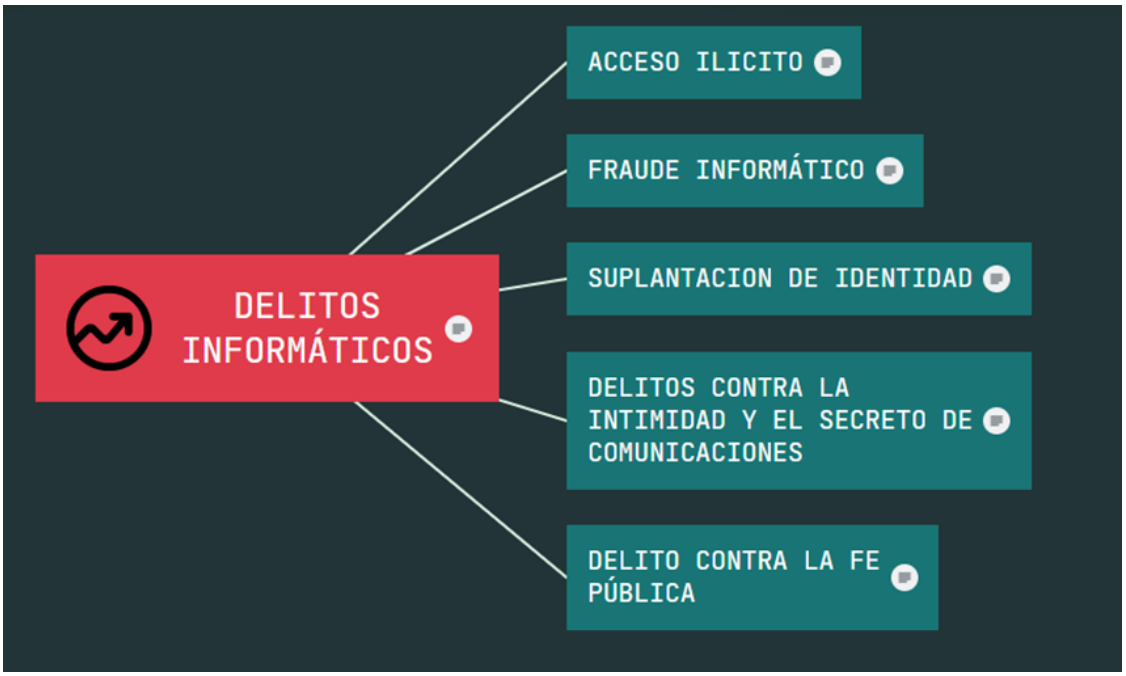
IV. RESULTADOS Y DISCUSIÓN

4.1. Descripción y análisis de resultados

Según lo expuesto en el estudio, se llevó la obtención de los resultados, que se obtuvo de acuerdo con el instrumento que se utilizó para recolectar los datos, el cual fue el uso de la guía de entrevista; para ello a fin de procesar los resultados, se utilizó el software Atlas ti v.23, que permitió establecer la relación entre las categorías y subcategorías conforme al siguiente detalle:

Figura 1

Categoría 1: Delitos Informáticos

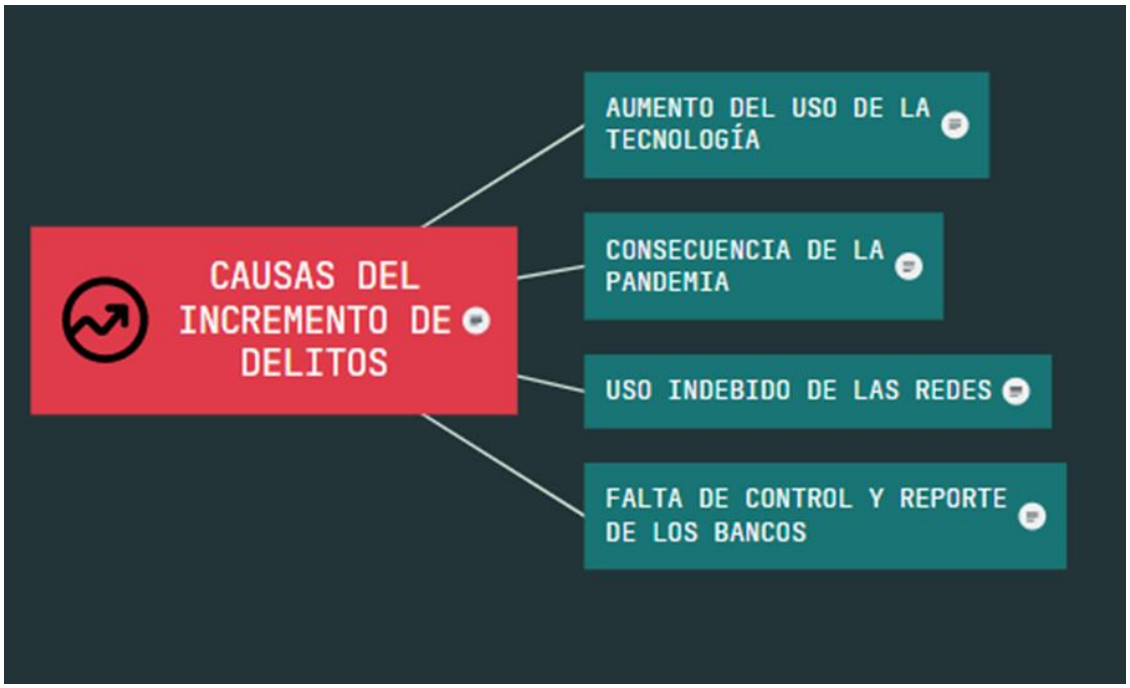


La figura 1, corresponde a la categoría 1, delitos informáticos, se da a conocer que el instrumento aplicado cuenta seis preguntas que ayudaron a obtener información sobre esta categoría. Los códigos que se visualizan, son el resultado de la agrupación de las respuestas que dieron los participantes, quienes coinciden que los delitos informáticos con mayor incidencia es el "acceso ilícito" cuya conducta típica es acceder sin autorización a una base de datos y el bien jurídico protegido es privacidad, "la suplantación de identidad", que se refiere al uso de las tecnologías de la información o la comunicación para hacerse pasar por alguien, causando daño material o psíquico (Artículo 9

de la Ley N° 30096), también se tiene “fraude informático”, que según Libano Manzur (2007), que abarca una amplia gama de actividades delictivas, como el robo de datos personales, “delitos contra la fe pública” que comprende la suplantación de identidad de una persona y se genera un perjuicio material o moral. En definitiva, estos delitos señalados precedentemente, son perpetrados a través de medios electrónicos.

Figura 2

Sub categoría: Causas del Incremento de Delitos Informáticos



La figura 2, corresponde a la subcategoría incremento de los delitos establecidos en la figura 1, en base a la respuesta de los participantes, quienes coincidieron que la causa del incremento de estos delitos, se dio por la pandemia ya que implemento con un mayor alcance los medios tecnológicos para generar facilidades a las personas para que no tengan que ir a una entidad bancaria y lo puedan hacer de manera virtual a través de las plataformas implementadas, sin embargo esta implementación, también ha sido una oportunidad para los delincuentes quienes se fueron adaptando de manera espontánea a las nuevas tecnologías para identificar los puntos vulnerables para cometer sus actos delictivos. Bajo esa perspectiva, mientras más avances tecnológicos se vayan creando, esto significa que la comisión de delitos se va

perfeccionando ya que guardan una relación muy estrecha, ya que crean nuevos métodos para cruzar la línea de seguridad que tiene cada plataforma digital.

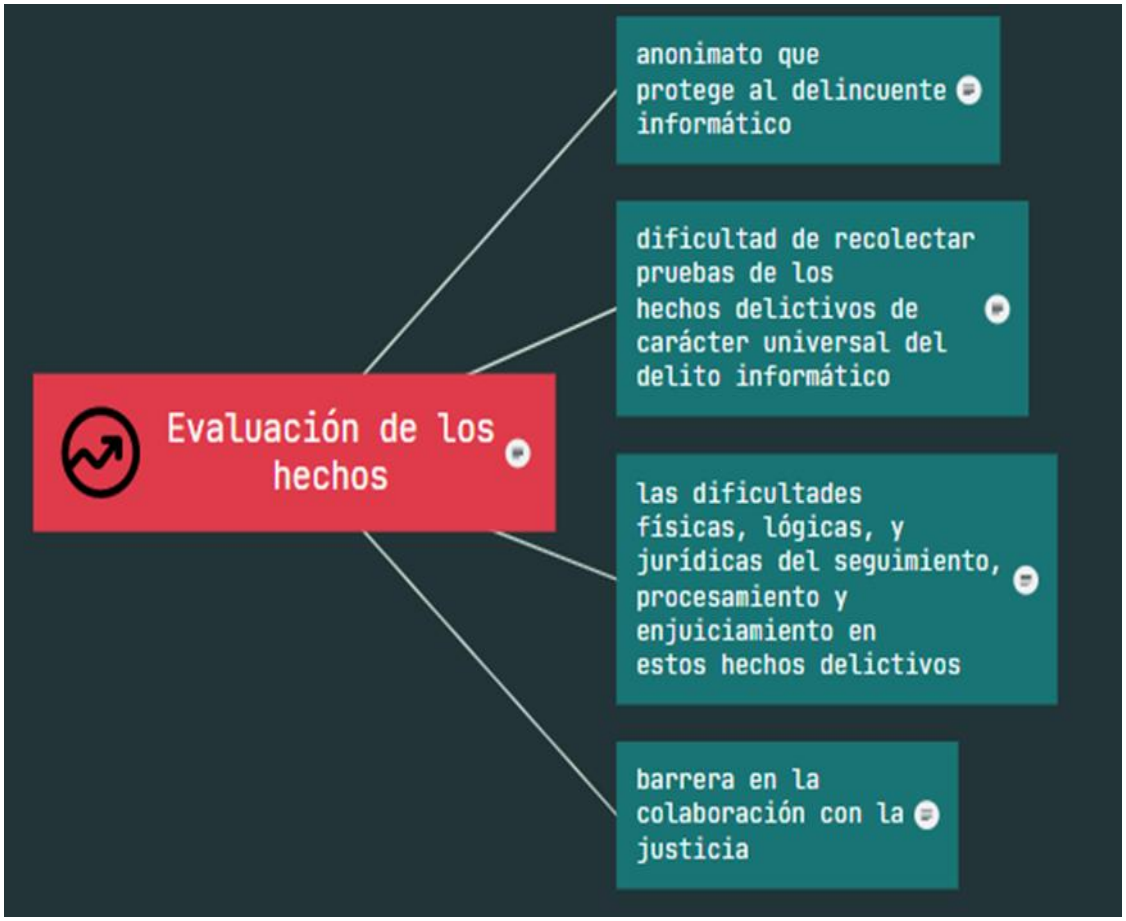
Figura 3

Sub categoría: Bien Jurídico Protegido

La figura 3 comprende a la sub categoría bien jurídico protegido y que de acuerdo a la agrupación de la respuesta de los participantes se tiene que, frente a este tipo de delitos, resulta varios derechos legales que se pueden ver violentados, incluidos la propiedad, la indemnidad sexual, la privacidad y los datos personales. Además, estos delitos, pandémicos o no, afectan los derechos legales a la información. Algunos delitos informáticos afectan a los derechos previstos en el derecho penal. Cabe aclarar que el delito informático, por su propia naturaleza, es un delito compuesto en cuanto compromete bienes jurídicos como información privilegiada, cuentas bancarias, tarjetas de crédito y correo electrónico. Finalmente, a nivel individual considero que ante ello se puede perder valiosa información personal, al contar con un respaldo como un antivirus que es un mecanismo de protección. En efecto, estos delitos con mayor incidencia han tomado fuerza sobre aquellas personas que no se informan sobre estas modalidades, caso contrario estarían a la vanguardia.

Figura 4

Categoría 2: Tratamiento fiscal



La figura 4, corresponde al desmembramiento de la categoría 2 para abordar el tratamiento fiscal que comprende la sub categoría evaluación de hechos que realiza el fiscal durante la investigación y que según la agrupación de las respuestas de los participantes, este, se ve envuelta en una serie de dificultades, ya que dentro de la calificación fiscal involucra una serie de diligencias para obtener evidencias digitales las cuales son difíciles de conseguir, y al no existir las herramientas adecuadas para poder conseguir los elementos suficientes debido a complejidad; las investigaciones deben ser derivadas a la DIVINDAT, por contar con los implementos necesarios para canalizar las investigaciones ordenadas por el Fiscal.

Asimismo, para la evaluación de los hechos, se accede al secreto de comunicaciones, que el código procesal penal, determina, que, para llevar a cabo esta tarea, primero se debe contar con un mandato del juez, ya que no

estaría acorde al marco legal, sin embargo, esta situación procesal de alguna u otra manera genera un retraso y dificultad para la atención oportuna de estos delitos.

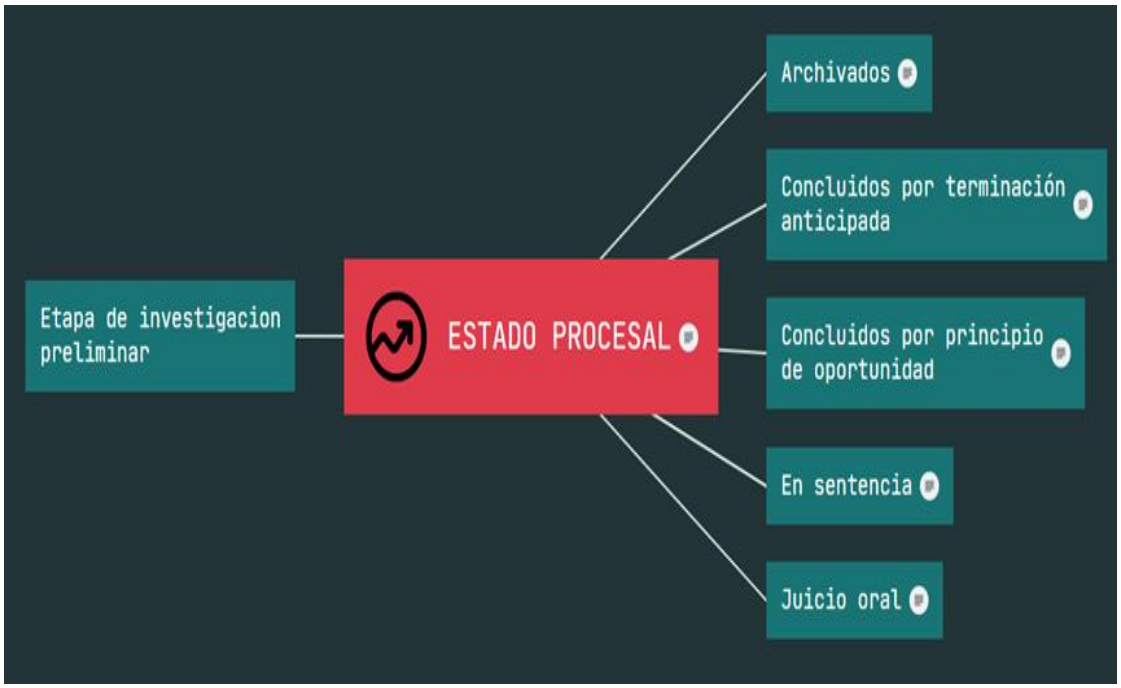
Figura 5

Sub categoría: Elementos de convicción

La figura 5, corresponde a la sub categoría elementos de convicción que juega un rol muy importante durante la investigación y que han sido generados del procesamiento de las respuestas de los participantes, quienes refirieron que a razón de la Pandemia, los delitos informáticos, se incrementaron en un alto índice, sin embargo por diversas limitaciones y particularidad en el tratamiento de estos, por el anonimato de los perpetradores y el hecho de que los perpetradores pueden estar realizando ataques en cualquier parte del país, muchos casos se terminan archivando debido a la falta de elementos de convicción.

Figura 6

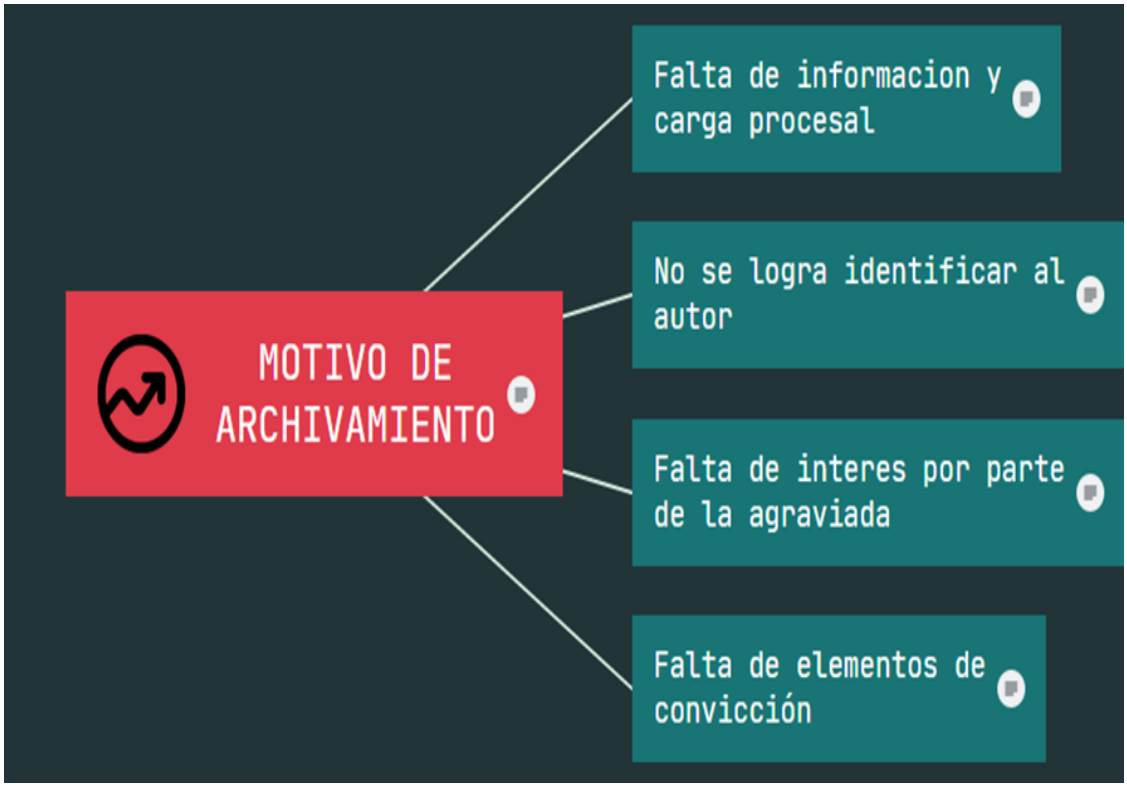
Categoría 3 Tratamiento judicial



La figura 6, corresponde a la desmembración de la categoría 3, y se da a conocer que el instrumento aplicado cuenta cuatro preguntas que ayudaron a obtener información sobre esta sub categoría que corresponde al estado procesal de los delitos, los entrevistados coincidieron que como tales delitos son elusivos, no hay recursos suficientes para investigar o recopilar pruebas suficientes; además, algunos encuestados agregaron que muchos de los casos están archivados por la falta de pruebas, la investigación pericial insuficiente y la falta de formación de los expertos técnicos. Se tiene casos pendientes de audiencia oral, pero son muy pocos según lo indicado por la Fiscalía Especializada en Ciberdelincuencia durante el periodo 2022, solamente han llegado 2 casos hasta esta etapa, mientras los otros han concluido mediante el principio de oportunidad o terminación anticipada y solamente 44 casos tienen sentencia.

Figura 7

Sub categoría: Motivo de archivamiento



La figura 7, corresponde a la sub categoría motivos de archivamiento de la categoría 3, donde los fundamentos considerados por los entrevistados para que se genere el archivamiento de las investigaciones de delitos informáticos, son la falta de individualización del sujeto, no es justiciable penalmente, hechos atípicos y acción penal privada además de la carga procesal y falta de interés de la agraviada.

Si bien es cierto que la adhesión al Convenio de Budapest supuso un paso importante en la lucha contra la ciberdelincuencia, no supuso cambios demostrativos en la forma en que se investigan y persiguen los delitos informáticos. Sin embargo, la solidez del compromiso del Perú con este tratado ha concedido que la cooperación internacional identifique a los delincuentes informáticos en los países que se han adherido a este tratado internacional (Tenorio 2018). También se reconoció que no existen restricciones legales para la presentación de cargos durante la investigación preliminar, pero la naturaleza de este tipo de delitos tiene otros factores que afectan la conducción de la investigación.

Figura 8

Nube de Palabras

Figura 8, es una red o nueve de palabras, que contiene las palabras más recurrentes que utilizaron los participantes en sus respuestas y la forma de diseño y procesamiento ha sido generado en el software Atlas. ti v.23, dentro de las cuales se visualizan las palabras más resaltantes: delitos, informáticos, participante, fraude, información, investigación, suplantación, ciberdelincuencia, redes, comunicaciones, seguridad, entre otras que forman parte de la investigación.

4.2. Discusión

De acuerdo a los resultados logrados y los trabajos previos, se procedió a realizar la discusión.

Respecto al objetivo general: Analizar los delitos informáticos perpetrados por medio de la ciberdelincuencia con el uso de las nuevas tecnologías en Lima

Centro 2022; se tiene que para la Ley N°30096 citado en la tesis de Carlos Reyes; el fraude se comete mediante el uso de herramientas informáticas que les otorgan a ellos mismos o a un tercero que genera una ventaja ilícita y dañan explícitamente a una persona al manipular el funcionamiento de un sistema informático. (Reyes, 2020, p. 27).

Del lado de Villavicencio citado en su trabajo de Elías Chávez; la describe como aquella conducta que intenta engañar y violar los sistemas en los dispositivos electrónicos, violando su seguridad, ya sea en computadoras, portátiles, sistemas de almacenamiento de datos. (Chávez, 2018, p. 43)

Los delitos informáticos tuvieron sus inicios en el año 1991, y en razón a ello se promulgo la Ley 30096 que fue introducido para especializarse en este tipo de ciberdelincuencia, centrándose en el avance y la inversión en la formación de profesionales del derecho con el único objetivo de lidiar con la ciberdelincuencia que encierra a todo tipo de delincuencia que se relaciona con el uso de la tecnología de información y comunicación.

Al respecto Tenesaca y Cedeño (2021) concluyeron que estos delitos, se ejecutan por medios tecnológicos que ha sido una cobertura amplia para el incremento de los delitos informáticos como el fraude, a razón de que ahora forma parte de la dinámica social y la necesidad de hacer uso de los medios informáticos. Es así que, se analizó los tipos de delitos informáticos más comunes que son perpetrados a través de los medios tecnológicos y que ha crecido considerablemente por la pandemia.

En ese contexto cabe señalar que, del análisis de los delitos señalados en la norma precedente, se tiene que estos engloban un conjunto de acciones ilícitas relacionados en el ciberespacio y que tienen como fin, apoderarse de los sistemas informáticos para así acceder al espacio donde se almacén los datos personales de las personas y perpetrar la comisión de un hecho delictivo, sin embargo por su naturaleza se vuelve una problemática ya que la forma en como ocurren los hechos, dificultan la apropiada ubicación e identificación el autor.

Respecto a los objetivos específicos:

O.E.1. Analizar los delitos más comunes y de mayor alcance dentro de los

delitos informáticos y la ciberdelincuencia. El derecho y la sociedad siempre ha estado en constante cambio, por lo que las normas siempre se van adecuando a las necesidades de la sociedad, aunque hoy en día el derecho penal no tiene una amplia doctrina respecto a los delitos informáticos debido a que la actividad criminal dentro de su desarrollo comprende una diversidad de acciones que son difícil de establecer en una sola definición.

Como menciona Camacho citado en el libro del Dr. Santiago Acurio del Pino; existe una variedad de engaños, manipulaciones, codicia, fraude, venganza, en todas las fases de la actividad humana. Debido a esto, con el aumento de la tecnología, surgen el fraude, el robo, el espionaje, el sabotaje e incluso el homicidio. (Acuario del Pino, S/F, p. 7).

Por otro lado, según Quijano M. (2021), los delitos con mayor incidencia son el fraude informático, suplantación de identidad, que han sido contrastados por el reporte dado por el Misterio Publico y su aplicación de instrumento de recolección de datos. Frente a ello, acuerdo a los resultados obtenidos, también se tiene que los delitos más comunes son el acceso ilícito, suplantación de identidad, fraude informático, delitos contra la fe pública y que se dan a través del ingreso o utilización indebida a la base de datos de las personas, el trasfondo de información y la falta de protección por las entidades bancarias. Asimismo, de acuerdo al reporte proporcionado por el Misterio Publico, sobre las denuncias registras por la División de Alta Tecnología, estas coinciden con los resultados.

Teniendo esta incidencia, el Perú cuenta con un gran marco normativo, sin embargo, no es suficiente para contrarrestar la ciberdelincuencia; ya que su implementación en el sistema jurídico no es del todo completa en cuanto aplicación de mecanismo para imputar este tipo de delitos. En resumen, dado que estas formas de delito pueden causar averías, es necesario iniciar una adecuada difusión para prevenirlos. Es cierto que la solución a este problema es compleja, ya que la tecnología está en constante evolución y no permanece estática. Sin embargo, se deben encontrar soluciones para evitar que los delincuentes eludan el castigo, ya que los métodos para cometerlos evolucionan a medida que surgen nuevas formas de fraude. Si bien muchos

bancos han tratado de mejorar la protección de sus plataformas digitales, persiste un factor social que tiene un gran impacto como es la falta de conocimientos informáticos, ya que si bien esto es una ventaja en la realización de las actividades cotidianas, también puede causar daños, pues la informática delictiva demuestra que el robo de información genera inseguridad.

También es importante recordar la clasificación que se ha hecho en relación con los delitos de lesión y la peligrosidad abstracta de tales delitos. El primero se considera una infracción consecutiva; es decir, violan el derecho protegido, mientras que quien amenaza con cometer un delito amenaza el objeto del derecho protegido. Finalmente, una encuesta muestra que muchos funcionarios encargados que hacen cumplir la ley, están de acuerdo en que investigar los delitos informáticos de es extremadamente complejo, especialmente cuando se trata de enjuiciar a los involucrados. Por esta razón, es necesario brindar a los jueces, abogados, fiscales y público en general una capacitación actualizada y difundir adecuadamente la información sobre el delito cibernético.

O.E.2. Determinar los mecanismos Jurídicos para Implementar la Ley 30096 en los Delitos Informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022; se conoce que los delitos informáticos, es bien sabido que estos irán en aumento ya que van de la mano con la tecnología, por lo que resulta un reto que el sistema jurídico implemente estrategia de prevención y sanción en beneficio de la sociedad, ya que según el investigador Saraguro (2021), es de gran necesidad e importancia reforzar este tipo de investigaciones, y para ello debe utilizarse la tecnología adecuada para determinar la causa y efecto del ciberdelito. Asimismo, debe capacitarse a los profesionales para lograr una mayor efectividad y obtener un eficaz resultado, y lo que es más importante, utilizar tecnología que permita investigar y no archivar el proceso. La Ley 30096 y sus modificaciones han tenido un considerable avance en relación con la investigación de delitos informáticos, ya que esto ha permitido la creación de nuevas fiscalías especializadas para tratar este tipo de delitos que son complejos por sus particularidades.

Según Ramos (2020), menciona que el Perú tiene una amplia gama de leyes, sin embargo, no son adecuadas para combatir la delincuencia cibernética, ya

que su aplicación en el sistema jurídico ha sido deficiente en cuanto a la implementación de mecanismos para imputar los delitos. Se menciona que varios países miembros del convenio han modificado sus leyes para reflejar la realidad social de cada uno de ellos, ya que la presencia de diferencias puede llevar a la imputación de delitos penales. De manera similar, el Perú no ha anticipado este evidente vacío hasta el momento, ya que la elaboración de la Ley N°30096, que la falta de información sobre los límites de los delitos informáticos impide conocer cómo manejar situaciones específicas. Finalmente, es importante destacar la importancia de establecer medidas para reforzar la protección informática, con el fin de garantizar la seguridad del usuario cuando se encuentra en Internet. En síntesis, se puede decir que la aplicación de la ley de delitos no ha sido tan efectiva como se preceptúa por lo que resulta necesario su modificación teniendo en cuenta que el uso de la tecnología ha sobrepasado las barreras de protección.

O.E.3. Analizar el procedimiento fiscal y judicial que se adopta en los delitos informáticos y la ciberdelincuencia. Cuando se trata de los procedimientos fiscales y legales aplicables a los delitos informáticos y los delitos cibernéticos, es imperativo que los administradores de justicia, estén preparados para manejar de manera efectiva la responsabilidad civil en los tribunales penales, tal como manejan la responsabilidad penal. Sin embargo, la protección no es efectiva, estando que el problema no se aborda directamente en el marco del ciberdelito; considerando la legislación general, que no contempla en un acto jurídico especial los aspectos contrarios a la violación de la privacidad de una persona, lo que conduce a una insuficiente sanción.

Rodríguez (2020), refiere que, frente a esta actuación, se tiene una gran dificultad para obtener información de elementos electrónicos, como la dirección IP y la clave de teléfono bloqueado, no contar con peritos informáticos en el Ministerio Público para acelerar el proceso de investigación y, en muchos casos, si se trata de provincias, estas tienen que remitirlas en la ciudad de Lima para recién procesar la información. También cabe resaltar que se tiene como obstáculo para el proceso de enjuiciamiento de delitos informáticos, que muchos casos no se logran identificar al autor, especialmente debido a la falta

de recursos para la contratación de personal especializado, logística, etc.

Se tiene coincidencia con Ramos (2020) que esto se refiere al hecho de que la recopilación de pruebas es difícil ya que muchos fiscales provinciales carecen de equipos modernos para identificar al perpetrador. La Policía Nacional del Perú carece de capacitación en técnicas y habilidades de investigación especializadas, lo que dificulta la prevención del delito en el Perú. Por ende resulta importante implementar mecanismos para sancionar conductas típicas del ordenamiento jurídico, ya que este requisito es la base de su ineficacia.

Por ende, el estado procesal de los delitos informáticos es que son archivados y una de las razones principales es la falta de pruebas concretas que permitan tener los suficientes elementos de convicción, falta de identificación del perpetrador y capacitación adecuados del personal, lo que puede provocar daños. Es así que el investigador Saraguro (2021), concluyó que es de gran importancia invertir en herramientas de trabajo idóneo para el tratamiento de estos delitos, además de capacitar al personal que lidera este tipo de investigaciones.

V. CONCLUSIONES

Primera: En razón al objetivo general, un presupuesto especial para delitos informáticos, puede vincularse directamente contra la propiedad, y que también incluye tipos de delitos que tienen un impacto significativo en los sistemas informáticos e incluso en la economía del país. Para combatir los delitos informáticos y cibernéticos, debemos solicitar a los países que firmen nuevos acuerdos internacionales que contengan nuevas herramientas a medida que el modus operandi criminal y las pandillas evolucionan; en nuestro país se deben implementar nuevas políticas pública, haciendo uso de las nuevas tecnologías para hacer un frente, ante el incremento de delitos informáticos en los últimos años, conforme los datos obtenidos de las instituciones públicas del Estado Peruano.

Segunda: En razón al primer objetivo específico, se concluye que los delitos más comunes de acuerdo a los resultados y la información proporcionada por la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, especializada en tratar los delitos informáticos y la División de Investigación de Alta Tecnología (DIVINDAT); son el acceso ilícito, suplantación de identidad, fraude informático, delitos contra la fe pública, los cuales han sido corroborados con los resultados de las guías de entrevistas aplicadas a los participantes.

Tercera: En razón al segundo objetivo específico, la aplicación de la Ley N° 30096, y sus modificaciones, han logrado avances significativos en las investigaciones relacionadas con delitos informáticos, esta a su vez han permitido la creación de nuevas fiscalías especializadas que dirigen y califican las investigaciones de manera focalizada con el fin de obtener pruebas y establecer si existen delitos de esta índole.

Cuarta: En razón al tercer objetivo específico, se concluye que las autoridades judiciales tienen una buena preparación para juzgar efectivamente la responsabilidad civil en los tribunales penales, así como lo hacen con la responsabilidad penal. Sin embargo, la falta de

cooperación interinstitucional, escases de pruebas o elementos de convicción; los casos terminan archivándose en su mayoría según fuente de la fiscalía especializada en ciberdelincuencia de Lima Centro, en su defecto muy pocos logran llegar al juicio oral o tener una sentencia condenatoria y que se ha podido contrastar con la información proporcionada por la Corte Superior de Justicia de Lima, en comparación con la cantidad de denuncias registradas estando a la información proporcionada por la DIVINDAT.

VI. RECOMENDACIONES

Primera: Se recomienda, establecer disposiciones que permitan la rápida conservación de los datos almacenados en los sistemas informáticos, además de la actualización de la Ley N° 30096, a fin de que se tome cuenta el dinamismo y avance tecnológico, la participación activa del público a través del uso de las redes sociales y la negociación a través de plataformas de internet y las nuevas tecnologías.

Segunda: En cuanto al método empleado en la ejecución de la investigación, fue a través del proceso de sistematización toda vez que contrasta las respuestas obtenidas a partir del punto de vista por los expertos y que luego fue interpretada por los diferentes puntos de vista de los implicados, y finalmente se aplicó el método descriptivo para el análisis de datos e identificar los aspectos importantes del estudio a través del software Atlas ti v.23, por lo que se recomienda que esta aplicación sea de constante utilización ya que facilita el procesamiento de la información con inteligencia artificial.

Tercera: En cuanto al instrumento de recolección de datos, se ha empleado la guía de entrevista; se recomienda ser utilizado para cuyas investigaciones que tengan un enfoque cualitativo, tomando en cuenta los objetivos de la investigación y sus respetivas categorías, ya que con ello se realiza el análisis de la información recopilada para el posterior procesamiento de los datos y obtención de los resultados. Dicho instrumento ha sido aplicado a los participantes: personal fiscal de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, agentes policiales de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), y abogados especialistas en derecho penal y procesal penal, en Lima Centro, estando que es nuestro escenario y territorio de la presente investigación.

Cuarta: Se ha evidenciado el incremento de delitos informáticos, por lo que, teniendo como modelo al Distrito Fiscal Lima Central, se recomienda evaluar la expansión de las fiscalías corporativas enfocadas en delitos cibernéticos y con el tiempo, crear otras jurisdicciones fiscales

en función de la necesidad, la demanda, la mayor frecuencia de denuncias de delitos cibernéticos y otros criterios. En cuanto al Poder Judicial, evaluar la implementación de un subsistema de justicia de delitos cibernéticos con personal debidamente capacitado para conocer casos de delitos cibernéticos y otros delitos cometidos utilizando los medios tecnológicos, para que sean equiparados de la misma forma, poniendo un frente ante estos tipos de delitos novedosos que se van incrementando a diario y transformando la criminalidad cibernética, proponiendo nuevos temas de investigación al respecto.

Quinta: Esta investigación ha puesto de relieve la importancia de abordar los delitos informáticos y la ciberdelincuencia en el contexto de las nuevas tecnologías y la lucha contra estos delitos requiere un enfoque integral que involucre la colaboración entre el Estado y la sociedad, los mismo que deben trabajar juntos para compartir información sobre amenazas, desarrollar soluciones conjuntas y promover prácticas de seguridad efectivas.

Sexta: Se recomienda la prevención y la protección de datos, ambos son elementos clave en la lucha contra los delitos informáticos, y se deben promover mejores prácticas de seguridad cibernética para minimizar los riesgos y salvar la información personal y confidencial que se tenga en la red denominada internet; es fundamental que los individuos y las organizaciones comprendan los riesgos asociados con las nuevas tecnologías y adopten medidas para protegerse, como el uso de contraseñas seguras, la actualización regular de software y la capacitación en técnicas de protección frente a los ciberataques.

REFERENCIAS:

Acurio, S (2023) *Cybercrime. Accessed April 8*. Recovered from: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Arias Gonzales, J. (2020). *Scientific research techniques and instruments*. Recovered from: http://bit.ly/2YFtw2Y

Avalos Rivera, Z. (2020). Informe de análisis n°04 ciberdelincuencia: pautas para una investigación fiscal especializada. Recuperado de https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA.

Azcorra, P. y López, V. (2016). Investigación cualitativa en subjetividad. Psicoperspectivas. https://www.redalyc.org/pdf/1710/171043532001.pdf

Baena, G., (2017). Metodología de la investigación: Serie integral por competencias. 3^a ed. México: Grupo Editorial Patria. ISBN 9786077447481. Disponible en: http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_ Abuso/Artículos/metodologia%20de%20la%20investigacion.pdf.

Bayardo, S. & Hermoza, M. (2019). Los delitos informáticos y su tipificación en la legislación penal ecuatoriana. Ecuador: Risti.

Canelo, J.P. (2022). *Delitos informáticos perpetrados a través de las redes sociales y su tratamiento judicial en el Ministerio Público.* (Tesis de pregrado, Universidad César Vallejo). Repositorio Institucional UCV. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/95324/Canelo_PJP-SD.pdf?sequence=1&isAllowed=y

Carrera, P.I (2021). *Deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021.* Tesis de posgrado, Universidad César Vallejo. Recuperado de: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/71492/Carrera_PIDR-SD.pdf?sequence=1&isAllowed=y

Chilcon, S.M. (2019). *El Cibercrimen en el Perú y su Incidencia en la Seguridad Nacional.* Tesis de postgrado, Centro de Altos Estudios Nacionales.

Repositorio Renati SUNEDU. https://renati.sunedu.gob.pe/bitstream/sunedu/393223/1/CHILCON%20TESIS%20DOCTORADO%202019.pdf

Corte Superior de Justicia de Lima (2023), Presidencia de la Corte Superior de Justicia de Lima, mediante Proveído N°1370-2023-SG-CSJLI-PJ, Información sobre casos por delitos informáticos y ciberdelincuencia en la CSJ de Lima, del periodo comprendido en el año 2020 al 2022 - Lima Centro.

Coronado. R. y Segura, L. (2018). La actuación del representante del ministerio público frente al levantamiento del secreto de las comunicaciones (tesis licenciatura). Universidad Señor de Sipán: Perú. Disponible en: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/6051/Coronado%20Tarrillo%20%26%20Segura%20Samillan.pdf?sequence=1&isAllowed=y

Código Penal (CP). 15 de mayo de 1871 (Alemania). Traducido por Claudia López Días. Disponible en: https://perso.unifr.ch/derechopenal/assets/files/legislacion/l_20080616_02.pdf

Condori Ccori, R. (2020). “Implicancias Jurídicas del Fraude Informático y la Protección Penal del Delito Contra el Patrimonio Distrito Fiscal de Lima Norte 2020". Lima: Universidad Cesar Vallejo. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/63158

CONAPOC (2020). Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia en el Perú. Primera edición digital. Lima: MINJUS. Disponible en: https://cdn.www.gob.pe/uploads/document/file/1487798/01%20Diagno%CC%81stico%20Situacional%20Multisectorial%20sobre%20la%20Ciberdelincuenci a%20en%20el%20Peru%CC%81%20%281%29.pdf.pdf

Convenio de Budapest (2019), Convenio sobre la Ciberdelincuencia.

Congreso de la República del Perú. (2013, 21 de octubre). *Ley N° 30096. Ley de delitos informáticos.* El Diario Oficial "El Peruano" https://busquedas.elperuano.pe/normaslegales/ley-de-delitosinformaticos-ley-n-30096-1003117-1/

Dass T. (2019) Comentario a la Ley de delitos informáticos Ley Nº 30096.

División de Investigación de Delitos de Alta Tecnología DIVINDAT (2023, Junio), Información de denuncias recibidas, se tiene por acceso ilícito, suplantación de identidad y delitos informáticos contra la intimidad y el secreto de comunicaciones 2020-2023.

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

Elías Puelles (2021) Derecho penal y cibercrimen. Lima: Idemsa.

Fernández Díaz, C. (2018). La amenaza de las nuevas tecnologías en los negocios: el ciber espionaje empresarial. Revista de Derecho UNED, Madrid, N. º 23, 17- 57. ISSN: 18869912. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6855253

Fiscalía Superior de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, Información sobre casos por delitos informáticos y ciberdelincuencia en el periodo comprendido del año 2020 al 2022.

Gómez Vásquez, J. C. (2020). *El tratamiento jurídico penal por parte del fiscal en los delitos informáticos contra el patrimonio*, distrito judicial de Lima Norte 2019. Lima, Perú. https://t.ly/9zb0

Hancco, E. (2017) "*La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096"-Perú.*

Hernández, R. y Mendoza, C., (2018). Metodología de investigación: Las turas cuantitativa, cualitativa y mixta. México: Mc Graw Interamericana Editores. ISBN 9781456260965

Hernández - Sampieri, R., & Mendoza Torres, C. P. (2018). *Metodología de la investigación*. Las rutas cuantitativa, cualitativa y mixta. México: Mc Graw Hill.

Hernández, S., y Duana, D. (2020). Técnicas e instrumentos de recolección de datos. Boletín Científico De Las Ciencias Económico Administrativas Del ICEA (17), https://doi.org/10.29057/icea.v9i17.6019

Hernández Sampieri, R. & Fernández Collado, C., & Baptista Lucio, P. (2014). *Investigation methodology* (sixth edition). México: Mc Graw Hill Education.

Horianski, J.E, (2021), *La protección penal ante el avance tecnológico y la delincuencia cibernética, "Dado el carácter transnacional ¿es suficiente la normativa penal existente para impedir el avance de la ciberdelincuencia? "Trabajo final de Graduación, Universidad Siglo 21"*. Recuperado de: https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/14687/HORIANSKI%20JORGE.pdf?sequence=1&isAllowed=y

Huamán, C.M. (2020). *Los Delitos Informáticos en Perú y la Suscripción del Convenio de Budapes.* Tesis de pregrado, Universidad Andina del Cusco. Recuperado de: https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/4116/Marleny_Tesis_bachiller_2020.pdf?sequence=1&isAllowed=y

Ley N° 30096. Ley del Delito Informático (22 de octubre de 2013) Diario Obtenida de: https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-leyn-30096-1003117-1/.

Ley N° 27806 "Transparencia y Acceso a la Información Pública", Proveído N° 001370-2023-SG-CSJLI-PJ (EXPEDIENTE 026438-2023-TDA-SG).

Mayer, L. (2018). El delito de fraude informático: concepto y delimitación. Recuperado de: https://doi.org/10.5354/0719-2584.2020.57149

Ministerio Público Fiscalía de la Nación. (Febrero de 2021). *Informe de Análisis N 04 Ciberdelincuencia en el Perú: Pautas para una investigación Fiscal Especializada. Obtenido de Oficina de Análisis Estratégico contra la Criminalidad*: https://t.ly/2VPS

Narkhede, S. (2020). Understanding Descriptive Statistics. In: Towards data science. Available in: https://towardsdatascience.com/understandingdescriptive-statistics-c9c2b0641291.

Nuñez, F., Carhuancho, B. (2020). Cyber crime in times of Covid-19: Violation of constitutional rights? LUMEN, Revista de la Facultad de Derecho de la UniversidadFemenina del Sagrado Corazón. https://www.aulavirtualusmp.pe/ojs/index.php/VJ/article/download/

United Nations Office on Drugs and Crime (2020) *cybercrime. Recovered from: https://www.unodc.org/e4j/es/cybercrime/module-1/keyissues/cybercrime-in-brief.html*

Ospina, M. & Sanabria, P. (2020). *Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia*, Universidad Militar Nueva Grada, recuperado de https://bit.ly/3h1lU3q

Peña, A. (2016). *Derecho Penal y Procesal Penal*. VII Edición. Lima, Perú.

Quevedo González, J. (2017). *Investigación y prueba del ciberdelito* (Tesis doctoral) Universidad de Barcelona.

Rodríguez García. (2020). *Una aproximación al delito de estafa en sus modalidades clásica e informática: De la estafa tradicional a las nuevas modalidades como el Phishing*. Recuperado de http://hdl.handle.net/2183/27015

Technological Dictionary. New technologies (2023). *Recuperado de: https://muytecnologicos.com/diccionario-tecnologico/nuevas-tecnologias*

Tenorio, J. (2018). *Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia.* Academia Diplomática del Perú "Javier Pérez de Cuéllar". Disponible en: http://repositorio.adp.edu.pe/handle/ADP/71.

Tomayo, M. (2002). *El proceso de la Investigación Científica*. Recuperado de http://evirtual.uaslp.mx/ENF/220/Biblioteca/Tamayo%20TamayoEl%20proceso%20de%20la%20investigaci%C3%B3n%20cient%C3%ADfic a20 02.pd

Saraguro, O.A. (2021). *La debilidad del proceso investigativo de los delitos informáticos.* Trabajo de Investigación, Universidad Técnica del Norte. Repositorio Institucional UTN. http://repositorio.utn.edu.ec/bitstream/123456789/11747/2/PG%20933%20TRABAJO%20GRADO.pdf

Sánchez, M., Fernández & M., Díaz, J. (2021). *Técnicas e instrumentos de recolección de información: análisis y procesamiento realizado por el investigador cualitativo*. Revista Científica Uisrael, Vol. 8, No. 1. E-ISSN: 2631-2786.

Santisteban, A., Ocares, L. & Andrade, L. (2020). Analysis of National Cybersecurity Strategies. International Journal of Advanced Computer Science and Applications, vol. 11, (12), 711-779. https://thesai.org/Downloads/Volume11No12/Paper_88-Analysis_of_National_Cybersecurity_Strategies.pdf

Schettini, P. & Cortazzo, I. (2015). *Análisis de datos cualitativos en la investigación social: Procedimientos y herramientas para la interpretación de la información cualitativa.* Editorial de la Universidad de la Plata. ISBN: 978-950-34-1231-2.

Sotomayor, R.G. (2022). *La Calificación Fiscal en los Delitos Informáticos en el Distrito Fiscal de Lima Centro, 2019 - 2020.* "tesis de maestría, Universidad César Vallejo". Repositorio Institucional UCV. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/95834/Sotomayor_RGB-SD.pdf?sequence=4&isAllowed=y

Valencia Gómez, M. O., Espejo Pérez, M. M., & Cano Ramírez, P. A. (ABRIL de 2020). Los delitos informáticos virtuales en redes sociales y las medidas que ha tomado el Estado colombiano para garantizar la protección integral de los ciudadanos al año 2019. EDUCACIÓN INCLUSIÓN Y DERECHO, PRIMERA, 231. COLOMBIA. Obtenido de https://t.ly/HuFl

Vences, S.O. (2019). *Penalización de los Delitos Informáticos.* [Tesis de posgrado, Universidad Autónoma del Estado de Morelos]. Repositorio RIAA. UAEM. http://riaa.uaem.mx/xmlui/bitstream/handle/20.500.12055/2675/VESONS

06T.pdf?sequence=1&isAllowed=y

Villavicencio T. (2021) Delitos Informáticos-Cibercrimen. Pág. 284.304. Recuperado de: file://D/:/Usuarios/pjudicial/Downloads/13630-54269-1-PB%20(1).pdf

ANEXO 1. MATRIZ DE CONSISTENCIA

<table>
<tr><td colspan="6">Título: Delitos informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022.</td></tr>
<tr><td colspan="2">Problemas</td><td colspan="2">Objetivos</td><td colspan="2">Categorías y sub categorías</td></tr>
<tr><td colspan="2">Problema General:</td><td colspan="2">Objetivo General:</td><td colspan="2">Categoría 1: DELITOS INFORMÁTICOS</td></tr>
<tr><td colspan="2" rowspan="2">¿Cuáles son los delitos informáticos perpetrados por medio de la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022?</td><td colspan="2" rowspan="2">Analizar los delitos informáticos perpetrados por medio de la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022.</td><td>Sub categorías</td><td>Ítems / Instrumento</td></tr>
<tr><td>• Delitos informáticos establecidos en la Ley 30096
• Causas del incremento de los delitos informáticos
• Bien jurídico protegido</td><td>1-6 / GUIA DE ENTREVISTA</td></tr>
<tr><td colspan="2" rowspan="2">Problemas Específicos</td><td colspan="2" rowspan="2">Objetivos Específicos</td><td colspan="2">Categoría 2: TRATAMIENTO FISCAL</td></tr>
<tr><td>• Evaluación de los hechos
• Elementos de convicción</td><td>7-11 / GUIA DE ENTREVISTA</td></tr>
<tr><td colspan="2">¿Cuáles son los delitos más comunes y de mayor alcance dentro de los delitos informáticos y la ciberdelincuencia?</td><td colspan="2">Analizar los delitos más comunes y de mayor alcance dentro de los delitos informáticos y la ciberdelincuencia.</td><td colspan="2">Categoría 3: TRATAMIENTO JUDICIAL</td></tr>
<tr><td colspan="2">¿Cuáles son los mecanismos jurídicos para Implementar la Ley 30096 en los Delitos Informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022?</td><td colspan="2">Determinar los Mecanismos Jurídicos para Implementar la Ley 30096 en los Delitos Informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022.</td><td>Sub categorías</td><td>Ítems / Instrumento</td></tr>
<tr><td colspan="2">¿Existe un procedimiento fiscal y judicial que se adopta en los delitos informáticos y la ciberdelincuencia?</td><td colspan="2">Analizar el procedimiento fiscal y judicial que se adopta en los delitos informáticos y la ciberdelincuencia.</td><td>• Estado procesal de los delitos informáticos
• Motivo de archivamiento</td><td>12-15 / GUIA DE ENTREVISTA</td></tr>
<tr><td>Diseño de investigación:</td><td colspan="2">Escenario de estudio y Participantes:</td><td>Técnicas e instrumentos:</td><td>Rigor científico:</td><td>Método de análisis de datos:</td></tr>
<tr><td>Enfoque: CUALITATIVO
Tipo: BASICA
Diseño: DESCRIPTIVO</td><td colspan="2">• Escenario: Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro y División de Investigación de Delitos de Alta Tecnología (DIVINDAT). – en Lima Centro.
• Participantes: Personal fiscal, agentes policiales y abogados especialistas en derecho penal y procesal penal.</td><td>• Técnica: Entrevista
• Instrumento: Guía de Entrevista.</td><td>Validez y confidencialidad: Ficha de Validación de Expertos</td><td>• Método: Descriptivo
• Software: Atlas ti v.23</td></tr>
</table>

ANEXO N°02

TABLA DE CATEGORIZACIÓN APRIORÍSTICA

Título: Delitos informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022.

Categoría de estudio	Definición conceptual	Subcategoría	Códigos
DELITOS INFORMÁTICOS	En nuestro Código Penal, en su artículo 207-A, define los delitos informáticos como actos que hacen mal uso o ingresan a una base de datos, red informática o cualquier parte de la misma, para crear, ejecutar o modificar un circuito o similar, o destruir, interferir, acceder o copiar contenido existente.	• Delitos informáticos establecidos en la Ley 30096 • Causas del incremento de los delitos informáticos • Bien jurídico protegido	• Delitos Informáticos • Incremento de Delitos Informáticos • Fraude Informático • Suplantación de Identidad
TRATAMIENTO FISCAL	Existe un estudio de hecho que es objeto de la denuncia que conduce a la prueba de la existencia del delito o de su inexistencia, por esa posición adicional que puede tomar la fiscalía para encontrar la verdad, antes de que esto suceda, el fiscal examina los hechos, promete ser cuidadoso, y lo principal es que trata de averiguar qué tipo de delito se comete para seguir el proceso de investigación, y finalmente pretende averiguar cuál es el delito (Sánchez, Fernández y Díaz, 2021).	• Evaluación de los hechos • Elementos de convicción	• Denuncias • Calificación Fiscal • Elementos de Convicción • Hechos
TRATAMIENTO JUDICIAL	El Tratamiento Judicial según los estados procesales de los delitos informáticos se pueden encontrar archivadas, en proceso, sobreseimiento, sentencia, Terminación anticipada. Encontramos también los motivos de archivamiento por la falta de colaboración de la parte afectada, en la falta de información y falta de pericias. (Ministerio Público Fiscalía de la Nación, 2021)	• Estado procesal de los delitos informáticos • Motivo de archivamiento	• Proceso Judicial • Sentenciados • Archivados

ANEXO N°03

INSTRUMENTO DE RECOLECCIÓN DE DATOS

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POST GRADO

GUÍA DE ENTREVISTA:

Delitos Informáticos y La Ciberdelincuencia con el Uso de las Nuevas Tecnologías en Lima Centro 2022

ENTREVISTADO: **(Nombre Completo)**	
BREVE RESUMEN CURRICULAR: **(Centro de Labores – Función que desempeña)**	
FECHA DE ENTREVISTA:	

INDICACIONES: La presente entrevista responde a la realización de un trabajo investigativa, por medio del cual se le pide responder objetivamente a las preguntas planteadas. Donde esta información será utilizada para fines académicos.

Objetivo General: Analizar los delitos informáticos perpetrados por medio de la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022.

- **CATEGORÍA 1: DELITOS INFORMÁTICOS:**

1. **¿Cuáles son los delitos informáticos perpetrados en el capítulo II de la Ley N°30096?**
   .....
   .....
   .....
   .....
2. **¿En cuánto ha sido el incremento de los delitos informáticos en los últimos años?**
   .....
   .....
   .....
   .....
3. **¿Cuáles son las causas del incremento de los delitos informáticos y la ciberdelincuencia?**
   .....
   .....
   .....
   .....
4. **¿A qué se debe la existencia de una deficiente investigación fiscal con relación a los delitos informáticos? Explique.**
   .....
   .....
   .....
   .....

5. ¿Cuáles son los casos de delitos informáticos y ciberdelincuencia más comunes en el Lima Centro?

.....
.....
.....
.....

6. ¿Considera que quiénes desconocen el uso de las nuevas tecnologías: aplicaciones y/o redes sociales, son más propensas a ser víctimas de la ciberdelincuencia? ¿Por qué?

SI	NO

.....
.....
.....
.....

- **CATEGORÍA 2: TRATAMIENTO FISCAL:**

7. Dentro de su experiencia ¿Qué tanto influye la calificación fiscal en la tramitación de investigaciones relacionadas a delitos informáticos?

.....
.....
.....
.....

8. ¿La deficiente investigación fiscal se debe a los diferentes vacíos legales y escasez de normativa en relación a la criminalidad informática? ¿Por qué?

SI	NO

.....
.....
.....
.....

9. ¿Cuáles son las principales diligencias que se realizan a nivel fiscal y policial que ayudan a determinar directamente la comisión de los delitos informáticos?

.....
.....
.....
.....

10. Desde su perspectiva ¿desde la aplicación de la Ley N°30096 y su modificatoria ha ayudado a mejorar el nivel de calificación de las denuncias por la presunta comisión de delitos informáticos?

.....
.....
.....
.....

11. Desde su experiencia ¿Qué tan negativo fue el impacto de calificar denuncias por delitos informáticos hasta antes de la aplicación de la Ley N° 30096?

.....
.....
.....
.....

- **CATEGORÍA 3: TRATAMIENTO JUDICIAL:**

12. **¿Considera que la Ley N°30096 tiene vacíos legales que imposibilitan la sanción de los delitos informáticos? ¿Por qué?**

SI	NO

.....
.....
.....
.....

13. **¿Cuál cree que es la principal razón para que la mayoría de los casos de delitos informáticos sean archivados?**

.....
.....
.....
.....

14. **¿Cuáles son los motivos de archivamiento o sobreseimiento de las denuncias por delito informático?**

.....
.....
.....
.....

15. **Desde su experiencia ¿considera usted que el tratamiento que le da el Estado, a través de las instituciones que operan en el sistema de justicia, en relación a los delitos informáticos es el correcto o tiene deficiencias?**

.....
.....
.....
.....

ANEXO N°04 JUICIO DE EXPERTOS

UNIVERSIDAD CÉSAR VALLEJO

1. **Datos generales**

Nombre del juez:	**GINES ALIAGA, ROCIO ROSARIO**
Grado profesional:	Maestría (X) Doctor ( )
Área de formación académica:	Clínica ( ) Social (X) Educativa ( ) Organizacional ( )
Áreas de experiencia profesional:	Área Penal
Institución donde labora:	Poder Judicial – Corte Superior de Justicia de Lima Este
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	Trabajo(s) psicométricos realizados Título del estudio realizado.

2. **Propósito de la evaluación:**
Validar el contenido del instrumento, por juicio de expertos.

3. **Datos Complementarios:**

Nombre de la Prueba:	Delitos informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022.
Autor (a):	Anicama Arones, Yessica Angelica
Objetivo:	Determinar la causa del incremento de los delitos informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022
Año:	2023
Ámbito de aplicación:	Lima Centro
Niveles o rango:	Alto nivel, moderado nivel, bajo nivel, no cumple con el criterio
Cantidad de ítems:	12 ítems
Tiempo de aplicación:	1 hora

4. **Presentación de instrucciones para el juez:**
A continuación, a usted le presento el cuestionario elaborado por Anicama Arones, Yessica Angelica en el año 2023 de acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de

		acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente.

4: Alto nivel
3: Moderado nivel
2: Bajo Nivel
1: No cumple con el criterio

CATEGORÍA 01: DELITOS INFORMÁTICOS

Definición de la categoría: En nuestro Código Penal, en su artículo 207-A, define los delitos informáticos como actos que hacen mal uso o ingresan a una base de datos, red informática o cualquier parte de la misma, para crear, ejecutar o modificar un circuito o similar, o destruir, interferir, acceder o copiar contenido existente. si se trata de una base de datos, será sancionado con prisión de hasta dos años o servicio público de 52 a 140 días.

Subcategoría 1: Delitos contra datos y sistemas informáticos. Delitos informáticos contra la indemnidad y libertad sexual. Delitos informáticos contra la intimidad y el secreto de las comunicaciones. Delitos informáticos contra el patrimonio. Delitos informativos contra la fe pública. Evaluación de los hechos.

CATEGORÍA 02: TRATAMIENTO FISCAL

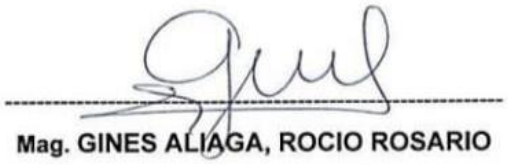
Existe un estudio de hecho que es objeto de la denuncia que conduce a la prueba de la existencia del delito o de su inexistencia, por esa posición adicional que puede tomar la fiscalía para encontrar la verdad, antes de que esto suceda. el fiscal examina los hechos, promete ser cuidadoso, y lo principal es que trata de averiguar qué tipo de delito se comete para seguir el proceso de investigación, y finalmente pretende averiguar cuál es el delito (Sánchez, Fernández y Díaz, 2021).

Subcategoría 2: Situación jurídica/Elementos subjetivos
La aplicación temporal o vigencia temporal de la ley penal constituye el conjunto de principios o reglas que tratan de conflicto entre diferentes leyes penales en el tiempo en relación a un hecho imputado. En relación a los elementos subjetivos en este tipo de delitos devienen en aquellas características que la denoten como tal, por ello debe de apreciarse que la acción delictiva sea dolosa para que no incurra en nulidad y a futuro se puedan plantear excepciones para librar de responsabilidad penal al investigado. (Calle, 2020).

CATEGORÍA 03: TRATAMIENTO JUDICIAL:

El Tratamiento Judicial según los estados procesales de los delitos informáticos se pueden encontrar archivadas, en proceso, sobreseimiento, sentencia, Terminación anticipada. Encontramos también los motivos de archivamiento por la falta de colaboración de la parte afectada, en la falta de información y falta de pericias. (Ministerio Público Fiscalía de la Nación, 2021)

Subcategoría 3: Estado procesal de los delitos informáticos / Motivo de archivamiento.
Hace referencia a la situación en la que se encuentra el proceso y las causas que conllevan a su archivamiento.



Mag. GINES ALIAGA, ROCIO ROSARIO

DNI N° 21136727

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO DE GUÍA DE ENTREVISTA.

Nº	CATEGORÍAS / INTERROGANTES	CLARIDAD				COHERENCIA				RELEVANCIA				SUGERENCIAS
		Alto nivel 4	Moderado nivel 3	Bajo nivel 2	No cumple 1	Alto nivel 4	Moderado nivel 3	Bajo nivel 2	No cumple 1	Alto nivel 4	Moderado nivel 3	Bajo nivel 2	No cumple 1	
CATEGORIA 1: DELITOS INFORMÁTICOS														
1	¿Cuáles son los delitos informáticos perpetrados en el capítulo II de la Ley N°30096?	X				X				X				
2	¿En cuánto ha sido el incremento de los delitos informáticos en los últimos años?	X				X				X				
3	¿Cuáles son las causas del incremento de los delitos informáticos y la ciberdelincuencia?	X				X				X				
4	¿A qué se debe la existencia de una deficiente investigación fiscal con relación a los delitos informáticos? Explique	X				X				X				
5	¿Cuáles son los casos de delitos informáticos y ciberdelincuencia más comunes en el Lima Centro?	X				X				X				
6	¿Considera que quiénes desconocen el uso de las nuevas tecnologías: aplicaciones y/o redes sociales, son más propensas a ser víctimas de la ciberdelincuencia? SI / NO ¿Por qué?	X				X				X				
CATEGORIA 2: TRATAMIENTO FISCAL														
7	Dentro de su experiencia ¿Qué tanto influye la calificación fiscal en la tramitación de investigaciones relacionadas a delitos informáticos?	X				X				X				
8	¿La deficiente investigación fiscal se debe a los diferentes vacíos legales y escasez de normativa en relación a la criminalidad informática? SI / NO ¿Por qué?	X				X				X				
9	¿Cuáles son las principales diligencias que se realizan a nivel fiscal y policial que ayudan a determinar directamente la comisión de los delitos informáticos?	X				X				X				

10	Desde su perspectiva ¿desde la aplicación de la Ley N°30096 y su modificatoria ha ayudado a mejorar el nivel de calificación de las denuncias por la presunta comisión de delitos informáticos?	X				X				X				
11	Desde su experiencia ¿Qué tan negativo fue el impacto de calificar denuncias por delitos informáticos hasta antes de la aplicación de la Ley N° 30096?	X				X				X				
CATEGORIA 3: TRATAMIENTO JUDICIAL														
12	¿Considera que la Ley N°30096 tiene vacíos legales que imposibilitan la sanción de los delitos informáticos? SI / NO ¿Por qué?	X				X				X				
13	¿Cuál cree que es la principal razón para que la mayoría de los casos de delitos informáticos sean archivados?	X				X				X				
14	¿Cuáles son los motivos de archivamiento o sobreseimiento de las denuncias por delito informático?	X				X				X				
15	Desde su experiencia ¿considera usted que el tratamiento que le da el Estado, a través de las instituciones que operan en el sistema de justicia, en relación a los delitos informáticos es el correcto o tiene deficiencias?	X				X				X				

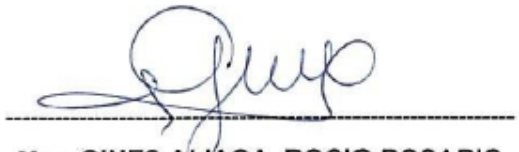
Observaciones (precisar): CONFORME

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

DATOS DEL JUEZ EXPERTO VALIDADOR:

- **Apellidos y Nombres** : **GINES ALIAGA, ROCIO ROSARIO.**
- **DNI N°** : **21136727**

- **Profesión** : ABOGADA
- **Especialidad** : ESPECIALIDAD PENAL
- **Cargo** : MAGISTRADA DEL JUZGADO UNIPERSONAL
- **Institución** : PODER JUDICIAL – CORTE SUPERIOR DE JUSTICIA DE LIMA ESTE



Mag. GINES ALIAGA, ROCIO ROSARIO

DNI N° 21136727

Lima, 11 de mayo del 2023

EVALUACIÓN POR JUICIO DE EXPERTOS

UNIVERSIDAD CÉSAR VALLEJO

1. **Datos generales**

Nombre del juez:	**REYNA DE LA CRUZ, JAVIER ENRIQUE**
Grado profesional:	Maestría (X) Doctor ( )
Área de formación académica:	Clínica ( ) Social (X) Educativa ( ) Organizacional ( )
Áreas de experiencia profesional:	Área Penal
Institución donde labora:	Universidad Nacional del Santa
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	Trabajo(s) psicométricos realizados Título del estudio realizado.

2. **Propósito de la evaluación:**
Validar el contenido del instrumento, por juicio de expertos.

3. **Datos Complementarios:**

Nombre de la Prueba:	Delitos informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022.
Autor (a):	Anicama Arones, Yessica Angelica
Objetivo:	Determinar la causa del incremento de los delitos informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022
Año:	2023
Ámbito de aplicación:	Lima Centro
Niveles o rango:	Alto nivel, moderado nivel, bajo nivel, no cumple con el criterio
Cantidad de ítems:	12 ítems
Tiempo de aplicación:	1 hora

4. **Presentación de instrucciones para el juez:**
A continuación, a usted le presento el cuestionario elaborado por Anicama Arones, Yessica Angelica en el año 2023 de acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la

		ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente.

4: Alto nivel
3: Moderado nivel
2: Bajo Nivel
1: No cumple con el criterio

CATEGORÍA 01: DELITOS INFORMÁTICOS

Definición de la categoría: En nuestro Código Penal, en su artículo 207-A, define los delitos informáticos como actos que hacen mal uso o ingresan a una base de datos, red informática o cualquier parte de la misma, para crear, ejecutar o modificar un circuito o similar, o destruir, interferir, acceder o copiar contenido existente. si se trata de una base de datos, será sancionado con prisión de hasta dos años o servicio público de 52 a 140 días.

Subcategoría 1: Delitos contra datos y sistemas informáticos. Delitos informáticos contra la indemnidad y libertad sexual. Delitos informáticos contra la intimidad y el secreto de las comunicaciones. Delitos informáticos contra el patrimonio. Delitos informativos contra la fe pública. Evaluación de los hechos.

CATEGORÍA 02: TRATAMIENTO FISCAL

Existe un estudio de hecho que es objeto de la denuncia que conduce a la prueba de la existencia del delito o de su inexistencia, por esa posición adicional que puede tomar la fiscalía para encontrar la verdad, antes de que esto suceda. el fiscal examina los hechos, promete ser cuidadoso, y lo principal es que trata de averiguar qué tipo de delito se comete para seguir el proceso de investigación, y finalmente pretende averiguar cuál es el delito (Sánchez, Fernández y Díaz, 2021).

Subcategoría 2: Situación jurídica/Elementos subjetivos
La aplicación temporal o vigencia temporal de la ley penal constituye el conjunto de principios o reglas que tratan de conflicto entre diferentes leyes penales en el tiempo en relación a un hecho imputado. En relación a los elementos subjetivos en este tipo de delitos devienen en aquellas características que la denoten como tal, por ello debe de apreciarse que la acción delictiva sea dolosa para que no incurra en nulidad y a futuro se puedan plantear excepciones para librar de responsabilidad penal al investigado. (Calle, 2020).

CATEGORÍA 03: TRATAMIENTO JUDICIAL:

El Tratamiento Judicial según los estados procesales de los delitos informáticos se pueden encontrar archivadas, en proceso, sobreseimiento, sentencia, Terminación anticipada. Encontramos también los motivos de archivamiento por la falta de colaboración de la parte afectada, en la falta de información y falta de pericias. (Ministerio Público Fiscalía de la Nación, 2021)

Subcategoría 3: Estado procesal de los delitos informáticos / Motivo de archivamiento.
Hace referencia a la situación en la que se encuentra el proceso y las causas que conllevan a su archivamiento.

Mag. REYNA DE LA CRUZ, JAVIER ENRIQUE

DNI N° 41585576

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO DE GUÍA DE ENTREVISTA.

Nº	CATEGORÍAS / INTERROGANTES	CLARIDAD				COHERENCIA				RELEVANCIA				SUGERENCIAS
		Alto nivel 4	Moderado nivel 3	Bajo nivel 2	No cumple 1	Alto nivel 4	Moderado nivel 3	Bajo nivel 2	No cumple 1	Alto nivel 4	Moderado nivel 3	Bajo nivel 2	No cumple 1	
CATEGORIA 1: DELITOS INFORMÁTICOS														
1	¿Cuáles son los delitos informáticos perpetrados en el capítulo II de la Ley N°30096?	X				X				X				
2	¿En cuánto ha sido el incremento de los delitos informáticos en los últimos años?	X				X				X				
3	¿Cuáles son las causas del incremento de los delitos informáticos y la ciberdelincuencia?	X				X				X				
4	¿A qué se debe la existencia de una deficiente investigación fiscal con relación a los delitos informáticos? Explique	X				X				X				
5	¿Cuáles son los casos de delitos informáticos y ciberdelincuencia más comunes en el Lima Centro?	X				X				X				
6	¿Considera que quiénes desconocen el uso de las nuevas tecnologías: aplicaciones y/o redes sociales, son más propensas a ser víctimas de la ciberdelincuencia? SI / NO ¿Por qué?	X				X				X				
CATEGORIA 2: TRATAMIENTO FISCAL														
7	Dentro de su experiencia ¿Qué tanto influye la calificación fiscal en la tramitación de investigaciones relacionadas a delitos informáticos?	X				X				X				
8	¿La deficiente investigación fiscal se debe a los diferentes vacíos legales y escasez de normativa en relación a la criminalidad informática? SI / NO ¿Por qué?	X				X				X				
9	¿Cuáles son las principales diligencias que se realizan a nivel fiscal y policial que ayudan a determinar directamente la comisión de los delitos informáticos?	X				X				X				

10	Desde su perspectiva ¿desde la aplicación de la Ley N°30096 y su modificatoria ha ayudado a mejorar el nivel de calificación de las denuncias por la presunta comisión de delitos informáticos?	X				X				X				
11	Desde su experiencia ¿Qué tan negativo fue el impacto de calificar denuncias por delitos informáticos hasta antes de la aplicación de la Ley N° 30096?	X				X				X				
CATEGORIA 3: TRATAMIENTO JUDICIAL														
12	¿Considera que la Ley N°30096 tiene vacíos legales que imposibilitan la sanción de los delitos informáticos? SI / NO ¿Por qué?	X				X				X				
13	¿Cuál cree que es la principal razón para que la mayoría de los casos de delitos informáticos sean archivados?	X				X				X				
14	¿Cuáles son los motivos de archivamiento o sobreseimiento de las denuncias por delito informático?	X				X				X				
15	Desde su experiencia ¿considera usted que el tratamiento que le da el Estado, a través de las instituciones que operan en el sistema de justicia, en relación a los delitos informáticos es el correcto o tiene deficiencias?	X				X				X				

Observaciones (precisar): CONFORME

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

DATOS DEL JUEZ EXPERTO VALIDADOR:

- **Apellidos y Nombres** : **REYNA DE LA CRUZ, JAVIER ENRIQUE.**
- **DNI N°** : **41585576**

- **Profesión** : ABOGADO
- **Especialidad** : ESPECIALIDAD PENAL
- **Cargo** : DOCENTE UNIVERSITARIO
- **Institución** : UNIVERSIDAD NACIONAL DEL SANTA

Lima, 12 de mayo del 2023

Mag. REYNA DE LA CRUZ, JAVIER ENRIQUE

DNI N° 41585576

EVALUACIÓN POR JUICIO DE EXPERTOS

UNIVERSIDAD CÉSAR VALLEJO

1. **Datos generales**

Nombre del juez:	**PAZ ORTEGA, LUCERY YAMALI.**
Grado profesional:	Maestría (X) Doctor ( )
Área de formación académica:	Clínica ( ) Social (X) Educativa ( ) Organizacional ( )
Áreas de experiencia profesional:	Área Penal
Institución donde labora:	Poder Judicial – Corte Superior de Justicia de Ica
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	Trabajo(s) psicométricos realizados Título del estudio realizado.

2. **Propósito de la evaluación:**
Validar el contenido del instrumento, por juicio de expertos.

3. **Datos Complementarios:**

Nombre de la Prueba:	Delitos informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022.
Autor (a):	Anicama Arones, Yessica Angelica
Objetivo:	Determinar la causa del incremento de los delitos informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022
Año:	2023
Ámbito de aplicación:	Lima Centro
Niveles o rango:	Alto nivel, moderado nivel, bajo nivel, no cumple con el criterio
Cantidad de ítems:	12 ítems
Tiempo de aplicación:	1 hora

4. **Presentación de instrucciones para el juez:**
A continuación, a usted le presento el cuestionario elaborado por Anicama Arones, Yessica Angelica en el año 2023 de acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de

		acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente.

4: Alto nivel
3: Moderado nivel
2: Bajo Nivel
1: No cumple con el criterio

CATEGORÍA 01: DELITOS INFORMÁTICOS

Definición de la categoría: En nuestro Código Penal, en su artículo 207-A, define los delitos informáticos como actos que hacen mal uso o ingresan a una base de datos, red informática o cualquier parte de la misma, para crear, ejecutar o modificar un circuito o similar, o destruir, interferir, acceder o copiar contenido existente. si se trata de una base de datos, será sancionado con prisión de hasta dos años o servicio público de 52 a 140 días.

Subcategoría 1: Delitos contra datos y sistemas informáticos. Delitos informáticos contra la indemnidad y libertad sexual. Delitos informáticos contra la intimidad y el secreto de las comunicaciones. Delitos informáticos contra el patrimonio. Delitos informativos contra la fe pública. Evaluación de los hechos.

CATEGORÍA 02: TRATAMIENTO FISCAL

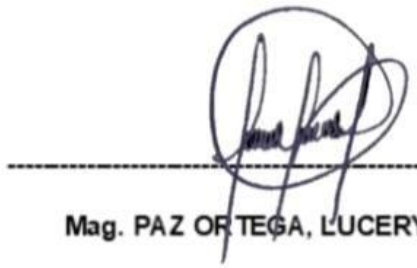
Existe un estudio de hecho que es objeto de la denuncia que conduce a la prueba de la existencia del delito o de su inexistencia, por esa posición adicional que puede tomar la fiscalía para encontrar la verdad, antes de que esto suceda. el fiscal examina los hechos, promete ser cuidadoso, y lo principal es que trata de averiguar qué tipo de delito se comete para seguir el proceso de investigación, y finalmente pretende averiguar cuál es el delito (Sánchez, Fernández y Díaz, 2021).

Subcategoría 2: Situación jurídica/Elementos subjetivos
La aplicación temporal o vigencia temporal de la ley penal constituye el conjunto de principios o reglas que tratan de conflicto entre diferentes leyes penales en el tiempo en relación a un hecho imputado. En relación a los elementos subjetivos en este tipo de delitos devienen en aquellas características que la denoten como tal, por ello debe de apreciarse que la acción delictiva sea dolosa para que no incurra en nulidad y a futuro se puedan plantear excepciones para librar de responsabilidad penal al investigado. (Calle, 2020).

CATEGORÍA 03: TRATAMIENTO JUDICIAL:

El Tratamiento Judicial según los estados procesales de los delitos informáticos se pueden encontrar archivadas, en proceso, sobreseimiento, sentencia, Terminación anticipada. Encontramos también los motivos de archivamiento por la falta de colaboración de la parte afectada, en la falta de información y falta de pericias. (Ministerio Público Fiscalía de la Nación, 2021)

Subcategoría 3: Estado procesal de los delitos informáticos / Motivo de archivamiento.
Hace referencia a la situación en la que se encuentra el proceso y las causas que conllevan a su archivamiento.



Mag. PAZ ORTEGA, LUCERY YAMALI

DNI N° 71897944

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO DE GUÍA DE ENTREVISTA.

Nº	CATEGORÍAS / INTERROGANTES	CLARIDAD				COHERENCIA				RELEVANCIA				SUGERENCIAS
		Alto nivel 4	Moderado nivel 3	Bajo nivel 2	No cumple 1	Alto nivel 4	Moderado nivel 3	Bajo nivel 2	No cumple 1	Alto nivel 4	Moderado nivel 3	Bajo nivel 2	No cumple 1	
CATEGORIA 1: DELITOS INFORMÁTICOS														
1	¿Cuáles son los delitos informáticos perpetrados en el capítulo II de la Ley N°30096?	X				X				X				
2	¿En cuánto ha sido el incremento de los delitos informáticos en los últimos años?	X				X				X				
3	¿Cuáles son las causas del incremento de los delitos informáticos y la ciberdelincuencia?	X				X				X				
4	¿A qué se debe la existencia de una deficiente investigación fiscal con relación a los delitos informáticos? Explique	X				X				X				
5	¿Cuáles son los casos de delitos informáticos y ciberdelincuencia más comunes en el Lima Centro?	X				X				X				
6	¿Considera que quiénes desconocen el uso de las nuevas tecnologías: aplicaciones y/o redes sociales, son más propensas a ser víctimas de la ciberdelincuencia? SI / NO ¿Por qué?	X				X				X				
CATEGORIA 2: TRATAMIENTO FISCAL														
7	Dentro de su experiencia ¿Qué tanto influye la calificación fiscal en la tramitación de investigaciones relacionadas a delitos informáticos?	X				X				X				
8	¿La deficiente investigación fiscal se debe a los diferentes vacíos legales y escasez de normativa en relación a la criminalidad informática? SI / NO ¿Por qué?	X				X				X				
9	¿Cuáles son las principales diligencias que se realizan a nivel fiscal y policial que ayudan a determinar directamente la comisión de los delitos informáticos?	X				X				X				

10	Desde su perspectiva ¿desde la aplicación de la Ley N°30096 y su modificatoria ha ayudado a mejorar el nivel de calificación de las denuncias por la presunta comisión de delitos informáticos?	X				X				X				
11	Desde su experiencia ¿Qué tan negativo fue el impacto de calificar denuncias por delitos informáticos hasta antes de la aplicación de la Ley N° 30096?	X				X				X				
CATEGORIA 3: TRATAMIENTO JUDICIAL														
12	¿Considera que la Ley N°30096 tiene vacíos legales que imposibilitan la sanción de los delitos informáticos? SI / NO ¿Por qué?	X				X				X				
13	¿Cuál cree que es la principal razón para que la mayoría de los casos de delitos informáticos sean archivados?	X				X				X				
14	¿Cuáles son los motivos de archivamiento o sobreseimiento de las denuncias por delito informático?	X				X				X				
15	Desde su experiencia ¿considera usted que el tratamiento que le da el Estado, a través de las instituciones que operan en el sistema de justicia, en relación a los delitos informáticos es el correcto o tiene deficiencias?	X				X				X				

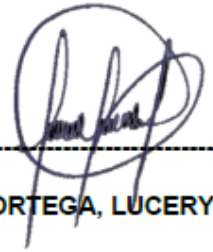
Observaciones (precisar): CONFORME

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

DATOS DEL JUEZ EXPERTO VALIDADOR:

- **Apellidos y Nombres** : **PAZ ORTEGA, LUCERY YAMALI.**
- **DNI N°** : **71897944**

- **Profesión** : ABOGADA
- **Especialidad** : ESPECIALIDAD PENAL
- **Cargo** : ESPECIALISTA JUDICIAL DE JUZGADO
- **Institución** : PODER JUDICIAL – CORTE SUPERIOR DE JUSTICIA DE ICA



Lima, 16 de mayo del 2023

Mag. PAZ ORTEGA, LUCERY YAMALI

DNI N° 71897944

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

ESCUELA PROFESIONAL DE MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Declaratoria de Autenticidad de los Asesores

Nosotros, MANUEL BENIGNO VILLANUEVA DE LA CRUZ, docente de la ESCUELA DE POSGRADO de la escuela profesional de MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesores de Tesis Completa titulada: "Delitos Informáticos y la Ciberdelincuencia con el Uso de las Nuevas Tecnologías en Lima Centro 2022", cuyo autor es ANICAMA ARONES YESSICA ANGELICA, constato que la investigación tiene un índice de similitud de 10.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

Hemos revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis Completa cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual nos sometemos a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 26 de Julio del 2023

Apellidos y Nombres del Asesor:	**Firma**
MANUEL BENIGNO VILLANUEVA DE LA CRUZ **DNI:** 40284159 **ORCID:** 0000-0003-4797-653X	Firmado electrónicamente por: MVILLABEN01 el 05-08-2023 09:30:13

Código documento Trilce: TRI - 0621246

INVESTIGA UCV