Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

INFLUENCIA DE LAS DILIGENCIAS PRELIMINARES EN LOS DELITOS INFORMÁTICOS EN EL CERCADO DE LIMA, AÑO 2024

Línea de investigación:
Procesos jurídicos y resolución de conflictos

Tesis para optar el grado académico de Maestro en Derecho Penal

Autor

López Loayza, Cesar Dinalber

Asesor

Sánchez Camargo, Mario Rodolfo

ORCID: 0000-0002-3368-9102

Jurado

Alarcón Menéndez, Jorge Miguel

Morante León, Salomón Jorge

López Navarro, Lindbergh

Lima - Perú

2025

INFLUENCIA DE LAS DILIGENCIAS PRELIMINARES EN LOS DELITOS INFORMÁTICOS EN EL CERCADO DE LIMA, AÑO 2024.

INFORME DE ORIGINALIDAD

16%	12%	1%	9%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Nacional Federico Villarreal Trabajo del estudiante	8%
2	hdl.handle.net Fuente de Internet	2%
3	repositorio.unfv.edu.pe Fuente de Internet	1%
4	www.coursehero.com Fuente de Internet	<1%
5	www.pensamientopenal.com.ar Fuente de Internet	<1%
6	www.scribd.com Fuente de Internet	<1%
7	Submitted to Escuela de Posgrado PNP Trabajo del estudiante	<1%
8	pt.slideshare.net Fuente de Internet	<1%

Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

INFLUENCIA DE LAS DILIGENCIAS PRELIMINARES EN LOS DELITOS INFORMÁTICOS EN EL CERCADO DE LIMA, AÑO 2024

Línea de investigación:

Procesos jurídicos y resolución de conflictos

Tesis para optar el grado académico de Maestro en Derecho Penal

Autor:

López Loayza, Cesar Dinalber

Asesor:

Sánchez Camargo, Mario Rodolfo

ORCID: 0000-0002-3368-9102

Jurado:

Alarcón Menéndez, Jorge Miguel

Morante León, Salomón Jorge

López Navarro, Lindbergh

Lima - Perú

2025

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Objetivo: Evaluar cómo influye las diligencias preliminares en los delitos relacionados con la informatica en el Cercado de Lima, 2024. Metodo: el trabajo realizado fue de diseño no experimental, nivel explicativo, tipo aplicado y respetó un enfoque cuantitativo, asimismo se optó por seleccionar una poblacion y muestra representada por 58 personas encuestadas entre fiscales y abogados del Ministerio Público. Resultados: El 41% está "totalmente de acuerdo" con su eficacia en la recolección de pruebas, mientras que el 38% "totalmente en desacuerdo" refleja una percepción negativa significativa. Ademas, el 41% está "totalmente de acuerdo" en que las diligencias preliminares influyen positivamente en la resolución de delitos informáticos. Por otra parte, un valor de significancia (Sig.) equivalente a 0.000, la que evidencia una significancia alta a nivel estadístio. Dado que este valor es mucho menor que el umbral común de 0.05, por lo cual se procede al rechazo de la hipótesis nula (Ho) la misma que afirma que las diligencias preliminares no influyen positivamente en los delitos informáticos. Por lo tanto, se concluye que las diligencias preliminares efectivamente tienen un impacto positivo en la labor investigativa y resolución de acciones delictivas vinculadas con la informática. Ademas, el valor de Nagelkerke de 0.791 señala que el modelo de regresión logística brinda una explicación aproximada de 79.1% con respecto a la variabilidad concerniente a la variable dependiente. Conclusiones: La evaluación de las diligencias preliminares en las acciones delictivas relacionados con la informática en el Cercado de Lima.

Palabras clave: diligencias preliminares, delitos informáticos, preventiva.

ABSTRACT

Objective: To evaluate how preliminary proceedings influence computer-related crimes in the Cercado de Lima, 2024. Method: The work carried out was of a non-experimental design, explanatory level, applied type and respected a quantitative approach. Likewise, it was chosen to select a population and sample represented by 58 people surveyed among prosecutors and lawyers of the Public Ministry. Results: 41% "totally agree" with its effectiveness in collecting evidence, while 38% "totally disagree" reflects a significant negative perception. In addition, 41% "totally agree" that preliminary proceedings positively influence the resolution of computer crimes. On the other hand, a significance value (Sig.) equivalent to 0.000, which shows a high significance at a statistical level. Since this value is much lower than the common threshold of 0.05, the null hypothesis (Ho) is rejected, which states that preliminary proceedings do not positively influence computer crimes. Therefore, it is concluded that preliminary proceedings do indeed have a positive impact on the investigative work and resolution of criminal actions related to computer science. In addition, the Nagelkerke value of 0.791 indicates that the logistic regression model provides an approximate explanation of 79.1% with respect to the variability concerning the dependent variable. Conclusions: The evaluation of preliminary proceedings in criminal actions related to computer science in Cercado de Lima.

Keywords: preliminary proceedings, computer crimes, preventive.

I. INTRODUCCIÓN

En la actualidad, el fenómeno de los delitos informáticos se ha consolidado como un reto que la población enfrenta. La revolución digital, que ha transformado la forma en que interactuamos, trabajamos y consumimos información, también ha dado lugar a un aumento significativo en la perpetración de delitos cibernéticos. En el Cercado de Lima, un área caracterizada por su alta densidad poblacional y su dinámica económica, esta problemática se manifiesta de manera aguda, afectando no solo a individuos, sino también a empresas y organismos estatales. La vulnerabilidad de las infraestructuras digitales y la falta de conciencia sobre la seguridad cibernética han creado un entorno propicio para la actividad delictiva, generando la necesidad urgente de desarrollar estrategias efectivas para combatir este fenómeno.

En este contexto, las diligencias preliminares desempeñan un papel fundamental en la investigación de delitos informáticos. Estas diligencias son agrupación de procedimientos y actos que son ejecutados al inicio de una investigación para recabar evidencia y determinar la existencia de un delito. Su eficacia es crucial, ya que una adecuada ejecución de estas diligencias marcaría algún tipo de diferenciación entre el fracaso y el éxito en la persecución de los delincuentes. Sin embargo, en muchos casos, las debilidades en la implementación de estas diligencias contribuyen a la impunidad y a la ineficiencia del sistema judicial. Por lo tanto, es necesario evaluar de manera rigurosa cómo estas diligencias influyen en las diversas resoluciones de las acciones delictivas informáticas que se ha podido evidenciar en Cercado de Lima.

El objetivo general de la presente labor investigativa ha sido fomentar el análisis de la influencia de las diligencias preliminares en las actividades delictivas ligadas a la informática durante el periodo 2024 en Cercado de Lima. Con la finalidad de que pueda lograrse, se optó por un diseño no experimental, de tipo explicativo, nivel aplicado y respetando un enfoque

cuantitativo. Este enfoque permitirá analizar la relación entre la calidad y los niveles de eficacia concerniente a las diferentes diligencias preliminares y los resultados en la investigación de los delitos informáticos. Por otra parte, la recolección de la información será ejecutado por medio de las encuestas y análisis de casos, lo que proporcionará una base sólida para entender las dinámicas en juego.

A través de esta investigación, se busca no solo aportar al campo académico, sino también ofrecer recomendaciones prácticas que puedan ser implementadas por las autoridades competentes. La identificación de las debilidades y fortalezas en los procedimientos concernientes a las diligencias preliminares permitirá a los encargados de operar justicia que puedan optimizar sus procedimientos y mejorar la eficacia en la lucha contra actividades delictivas ligadas a la informática. Asimismo, se proyecta que el resultado de dicha labor investigativa pueda contribuir a la construcción de un marco normativo y operativo más robusto, que responda a los retos que evidencia la criminalidad en el entorno digital.

En conclusión, la evaluación de las diferentes diligencias de carácter preliminar en el contexto de las acciones delictivas ligadas a la informática resulta ser calificada como una tarea de suma importancia. La eficacia de estas diligencias no solo impacta en la resolución de casos individuales, sino que también influye en la percepción de gran parte de los ciudadanos con respecto a diversos asuntos ligados a la capacidad del sistema judicial para enfrentar la diversidad de retos que generalmente suele plantear la criminalidad en el siglo XXI. Este estudio se propone, por tanto, contribuir a un mejor entendimiento de estas dinámicas y ofrecer propuestas que fortalezcan la respuesta institucional ante las actividades delictivas ligadas a la informática en el Cercado de Lima. La importancia de esta labor investigativa radica en su potencial para mejorar la seguridad y la confianza en el sistema judicial, aspectos fundamentales para que la sociedad pueda desarrollarse de una manera más equitativa y justa.

1.1 Planteamiento del problema

Ante el constante avance de las tecnologías vinculadas al ámbito de la información y la comunicación en nuestra sociedad, es fundamental la adaptación del medio en el que nos desarrollamos, la interacción social en el uso de estas herramientas tecnológicas respecto de su seguridad y sus consecuencias, si bien es cierto son útiles y hacen la vida más actualizada, sin embargo, son mayores los retos que se presentan en la interacción de estos instrumentos tecnológicos en el mundo globalizado respectos de su manejo y niveles de seguridad, debido a ello, la sociedad y el estado debe implementar nuevas herramientas y procedimientos orientados a la construcción de un conocimiento positivo y seguro, así como prevenir la comisión de delitos con estos medios de la tecnología.

Es allí donde la legislación peruana, requiere conocer de qué manera se está llevando a cabo el uso del internet y estas herramientas tecnológicas frente a los nuevos desafíos concerniente al manejo de la comunicación e información. El actual desafío es conseguir un equilibrio adecuado entre las acciones sancionadoras y preventivas de todo Gobierno contra el incremento constante de los comportamientos delictivos por parte de diversas personas permitiendo de esta manera el desarrollo de diferentes procedimientos tecnológicos en nuestro medio, pero con un mayor ajuste en seguridad.

Por esta causa, junto con el progreso de la tecnología digital y su impacto en casi todos los aspectos de la vida en sociedad, han emergido una variedad de conductas negativas que antes eran inimaginables y, en ciertos casos, resultan complicadas de que puedan ser clasificadas dentro de las leyes penales convencionales, sin hacer uso de aplicaciones análogas que se tienen algún tipo de prohibición por el principio de legalidad (Acurio, 2016).

Los crímenes cibernéticos son acciones ilegales llevadas a cabo por criminales utilizando software, como la introducción de algún tipo de virus, la falsificación de páginas web, fraudes, piratería y cualquier tipo de infracción que se encuentra ligada a los derechos de

autor, entre otros. Desde una perspectiva global, México ha sido gravemente impactado por la prevalencia de estas actividades delictivas en el ámbito digital, debido a ello, se resalta a Alcalá y Meléndez (2023) quienes mediante su trabajo de investigación realizada expresaron que, en México, la digitalización a nivel global ha simplificado casi todas las actividades humanas, sin embargo, ante la crisis sanitaria provocada por el coronavirus se aceleró este proceso. Como resultado, las áreas comerciales, laborales, de salud, sociales y educativas han adoptado la tecnología digital. Sin embargo, esto también ha dado lugar a un aumento en las actividades delictivas cibernéticas, como se da en los casos de fraude y robo en línea, así como el ciberacoso, que están evolucionando rápidamente y no siempre están reflejados en las leyes penales actuales. A lo largo de la historia, el comportamiento delictivo ha existido y se han transformado periodo tras periodo, asimismo durante el siglo XXI, impulsada por el avance tecnológico, las actividades delictivas informáticas han crecido de manera significativa. La definición, particularidades y legislación relacionada con estos delitos han sido objeto de discusión legal en los últimos años, y en México sigue siendo un tema que requiere una mayor atención, por ello, es fundamental examinar estos aspectos y evaluar si su inclusión explícita en las leyes penales puede ayudar en la denuncia, prevención, persecución, investigación y disminución de las actividades delictivas mencionadas.

Por otra parte, en Colombia se ha podido evidenciar el perjuicio generado por actividades delictivas informáticas, ante ello, se procede a resaltar a Álvarez (2023) quien ha señalado que en Colombia se evidenció un aumento en las actividades delictivas ligadas a la informática durante el último periodo, sin embargo durante el periodo 2022, se reportaron más de 54,000 denuncias por actividades delictivas informáticas, lo que representa un incremento significativo en comparación de las 11,223 denuncias que se ha logrado registrar durante el periodo 2021. Los incidentes más frecuentes ocurren por medio de la telefonía móvil, tabletas y computadora, por su parte el teniente policial Julián Buitrago encargado del centro

informático de Colombia, compartió con la Voz de América las tácticas más habituales que emplea la delincuencia para llevar a cabo fraudes en línea. Recientemente, se ha observado un aumento en las denuncias relacionadas con problemas de la banca y robos en el sistema financiero, ya que los criminales han conseguido acceder a contraseñas. Generalmente, los delincuentes realizan el envío de mensajería que parecen ser de interés, como ofertas de subsidios o convocatorias de la Fiscalía, lo que lleva a las personas a proporcionar información de carácter personal, que luego es utilizada para ejecutar diversas modalidades de estafa.

En los últimos años, Chile se ha convertido en uno de los países de América Latina más vulnerables a los ciberataques. De acuerdo con datos de Nova Red, especialistas en seguridad digital, los delitos cibernéticos en el país evidenciaron un crecimiento del 60% en lo que va del año, impulsados por la crisis sanitaria. En particular, los ataques de phishing se incrementaron en un 360%, mientras que los ataques de ransomware mostraron un aumento del 210%.

De acuerdo con un informe sobre ciberdelincuencia durante el periodo 2020 que aborda avances y riesgos tanto en países Latinoamericanos y el Caribe, a medida que las entidades siguen modernizándose y acelerando su proceso de evolución digital, asimismo, los ataques se vuelven cada vez más complejos y las agrupaciones dedicadas a la criminalidad a nivel global se están organizando mejor. En el contexto de Chile, la institucionalidad y la legislación aún tienen mucho por hacer. Desde hace varios periodos, se están desarrollando diversas legislaciones simultáneamente, pero su progreso no ha sido tan ágil ni sencillo como se esperaba. Por un lado, se encuentra el Proyecto de Ley concerniente a las acciones delictivas ligadas a la informática, que fue aprobado de manera unánime a través del Senado y está listo para la realización de otro trámite en la Cámara de Diputados. Es importante resaltar que uno de los proyectos más relevantes en este ámbito es la Ley Marco de Ciberseguridad, que tiene como objetivo fomentar la búsqueda de la protección de la infraestructura crítica, sin embargo, hasta el momento no ha sido presentada al Congreso.

Además, está en discusión el proyecto de Ley que fomente la protección de datos, que ha estado varios periodos en el Congreso Nacional a la espera de ser aprobado. En este contexto, los expertos en ciberseguridad destacan la importancia de que el Gobierno actúe con mayor celeridad. No cabe duda de que se están logrando progresos y que estos son positivos, pero la gran interrogante es si estamos avanzando a la velocidad necesaria. Es fundamental y urgente que pueda acelerarse dicho proceso y tener listas las normativas que permitirán que el país se actualice en cuestiones regulatorias; establezca una institucionalidad idónea; definiendo los estándares mínimos en materia de seguridad en los sectores privado y público para proteger de manera efectiva la infraestructura crítica.

Tomando en consideración la información de la Ciberseguridad 2020, en situaciones riesgosas, avances y el direccionamiento a continuar en países de Latinoamérica y el caribe (Moisés J Schwartz, Gerente de Instituciones para el Desarrollo del BID), señala que la crisis generada a inicios del periodo 2020 por la coyuntura de la COVID-19 ha evidenciado cierta dependencia de una esencial infraestructura que, para gran parte de la ciudadanía resultó ser prácticamente no visible o simplemente pasa desapercibida. Las actividades cotidianas se centran cada vez más en procesos digitalizados, lo que las hace más vulnerables a situaciones amenazantes de particularidades cibernéticas. Es importante señalar que las alternativas estratégicas en materia de ciberseguridad son cruciales para proteger los derechos de la ciudadanía en el entorno digital, incluyendo la propiedad y la privacidad, además de fomentar la confiabilidad en el ámbito tecnológico - digital, permitiendo que las personas se sientan seguras al utilizarlas. El delito cibernético representa ya cerca de la mitad de la totalidad de las acciones delictivas perpetrados en perjuicio de la propiedad a nivel global. En términos generales, las cifras son aún más alarmantes, ya que los costos en materia de la economía por los ataques cibernéticos podrían superar el 1% del PBI en ciertos países. Cuando se perjudican infraestructuras críticas, se da hasta un 6% del PIB.

El estudio actual revela que en diversos países ubicados en el Caribe y en Latinoamérica. todavía no están adecuadamente equipados para hacer frente a los ciberataques. Solo 7 de los 32 países evaluados en este informe disponen de un adecuado planeamiento para brindar protección a la infraestructura crítica, mientras que 20 han creado determinados equipos para responder diferentes tipos de incidentes, conocido como CSIRT o CERT. Esta situación restringe la habilidad para detectar ataques y reaccionar de manera efectiva ante ellos (Banco Interamericano de Desarrollo [BID], 2020).

El Convenio de Budapest menciona una segunda agrupación de acciones delictivas, los cuales se conocen comúnmente como delitos informáticos, que incluyen las siguientes categorías: falseamiento digital (art.7) asimismo el fraude digital (art.8). Estas categorías son comparables a la Ley 30096, art 8-9. Es importante señalar que las 2 agrupaciones de las acciones delictivas mencionadas anteriormente son considerados como núcleo esencial vinculado al ámbito de la ciberdelincuencia. (Ministerio Público, 2020).

En el Perú, todos los meses suelen reportarse más de 300 casos de delitos cibernéticos, donde el fraude ejecutado en línea resulta ser la categoría más común, la misma que representa un 50% de la totalidad. Los delincuentes digitales utilizan diferentes métodos, como la replicación de páginas web de bancos, compras fraudulentas en internet y la utilización de celulares sustraídos para llevar a cabo sus actividades delictivas. En el periodo 2022, se ha podido registrar 2,382 denuncias por fraude en línea, lo que lo convierte en la acción delictiva informática que mayor ha reportado el Perú. (El Peruano, 2023).

Según, la Defensoría del Pueblo (2023) reportó que la ciudad de Lima Metropolitana y Lima Provincias se ha logrado registrar más del 50% de la totalidad de denuncias por delitos cibernéticos ante la PNP en el periodo 2021.

Las personas pueden caer mediante una serie de trampas tal como es el caso del phishing, una táctica que busca que entreguen todos sus datos e información financiera sin

darse cuenta de que el sitio web que lo requiere termina siendo falso. Los usuarios llegan a estos sitios engañosos a través de la mensajería de texto, correos electrónicos o diferentes tipos de publicaciones plasmadas en las redes sociales. Cuando se reportan delitos en línea, la Policía comienza investigando la cuenta bancaria que ha recepcionado el importe dinerario robado, siendo estas las primeras en ser detectadas, pero las agrupaciones dedicadas al cibercrimen reclutan a otros individuos para que abran cuentas bancarias y puedan recibir las operaciones ofreciéndoles comisiones que pueden ascender a los 100 soles (Diario Gestión, 2020).

A partir de lo anterior, se ha llegado a la conclusión de que actualmente la sociedad no cuenta con una cultura que proteja los datos de carácter personal. Es fundamental recordar la protección del individuo; esto convierte el manejo de sus datos personales en un proceso esencial para garantizar la defensa de las fundamentales libertades, así como los derechos humanos. Los habitantes de Lima Metropolitana suelen compartir su información en línea, a través del correo electrónico y redes sociales, etc. Esto representa un riesgo para su información, puesto que se aceptan los términos y condiciones de los servicios mencionados, a menudo no comprenden completamente lo que están aceptando ni la utilización que se le dará a los datos recopilados.

Los delitos cibernéticos se pueden describir como acciones ilegales que ocurren en un entorno digital, utilizando un computador; estos estaban regulados y penalizados en el Código Penal del Perú, sin embargo, desde el periodo 2013, el marco legal que abarcaba estas acciones delictivas fue reemplazado por otra normativa.

Asimismo, la Ley de Delitos Informáticos que tiene como finalidad fomentar la prevención y castigo de las acciones ilegales que impactan los sistemas y la información digital, así como los diferentes bienes jurídicos de importancia penal, que se llevan a cabo a través de las T.I. Su objetivo es asegurar una lucha efectiva contra la ciberdelincuencia. Aunque esta legislación se ha implementado para proteger la información personal de todo individuo, resulta

poco suficiente, en vista que aún siguen apareciendo reportes de personas que han sufrido acciones delictivas informáticas. Con la aparición de nuevas tecnologías, también surgen más tipos de acciones delictivas ligadas con la cibernética, ya que las TIC ofrecen a los delincuentes la oportunidad de idear nuevas estrategias para cometer sus delitos, planificando los crímenes de manera más efectiva, incluso cruzando fronteras, y eliminar evidencias que podrían ayudar a identificar a los responsables de las acciones delictivas.

1.2 Descripción del problema

La Ley 30096, no es suficiente para procesar y juzgar los delitos informáticos, no se ha tenido en cuenta la evolución de los delitos en el ciber espacio, del sistema informático a nivel internacional, ya que esta rama de la tecnología está en constante cambio, e innovación.

En la actualidad existe un alto índice de delitos informáticos, que en los últimos años se han incrementado, debido a la poca efectividad de los mecanismos de seguridad de las financieras demás sistemas tecnológicos, así tampoco no es menos cierto que la legislación nacional y la participación del estado en estos temas ha sido casi invisible.

Una incorrecta preparación y procesamiento de estos delitos en el sistema de justicia respecto de las diversas modalidades existentes de ciberdelincuencia, tanto más, cuando la criminalidad tecnológica está en constante innovación, que cada día aparece una nueva forma de ciberdelito. Asimismo, las causas de la problemática de las diligencias preliminares y las acciones delictivas informáticas – Ley 30096 en el Cercado de Lima 2023:

- Incorrecta interpretación de la Ley 30096, toda vez que para la aplicación de esta Ley se debió preparar al personal del sistema de justicia, que pudiera procesar estos delitos con mayor efectividad.
- Insuficiente capacidad del sistema de justicia, toda vez que para el seguimiento e investigación de estos delitos es necesario contar con profesionales entendidos en

sistemas de computación, así como abogados capacitados en informática o sistemas de informática.

- Ausencia de lineamientos para unificar criterios y de esa manera asegurar la solución de la labor investigativa en materia de delitos informáticos, pues los diferentes despachos, al no encontrar elementos de convicción en la investigación preliminar archivan las denuncias.

Si es que el problema expuesto continua se resaltarán las siguientes consecuencias:

- Crecimiento de los niveles en las acciones delictivas informáticas en vista que mayormente dichos procesos no se llegan a sancionar.
- Incremento de los archivos de los procesos en estos casos, toda vez que casi un 90% de estos delitos no llegan a la fase jurisdiccional.
- Disconformidad de la sociedad con el sistema de justicia, siendo que, gran parte de los procesos, no son individualizados al autor o autores de latrocinio denunciado.

Control pronostico (posibles soluciones para mejorar problemática):

- Legislar en materia penal, respecto de estos delitos, pero con el estudio correspondiente de profesionales capacitados en esta materia, ya que estos están en constante cambio.
- Capacitar a los profesionales encargados de operar justicia relacionado a dichas acciones delictivas, con el acompañamiento de personal especializado en estos temas.
- Incrementar la seguridad en las financieras y demás sistemas tecnológicos masivos, así como la debida orientación de la población en lo concerniente al uso de los equipos tecnológicos.

1.3 Formulación del problema

1.3.1. Problema general

¿Cómo influye las diligencias preliminares en los delitos informáticos en el Cercado de Lima, año 2024?

1.3.2. Problema Específicos

- ¿Cómo influye la dimensión investigativa en los delitos informáticos en el Cercado de Lima, año 2024?
- ¿De qué manera influye la dimensión preventiva en los delitos informáticos en el Cercado de Lima, año 2024?
- ¿De qué manera influye la dimensión resolutiva en los delitos informáticos en el Cercado de Lima, año 2024?

1.4 Antecedentes

1.4.1. Antecedentes internacionales

Según Beermann (2024) mediante su labor investigativa, resalta la importancia de analizar el ambito de la ciberdelincuencia que se ha evidenciado en las diversas zonas de Panamá así como la importancia de la ejecución del convenio de Budapest durante el periodo 2001, asimismo, resalta que los delitos cibernéticos pueden verse como la intersección de dos áreas que están en cambio constante: primeramente el derecho, especialmente lo referente al derecho penal, y como segundo se tiene a la tecnología. Por esta razón, es fundamental que su análisis y clasificación sean igualmente flexibles y se adapten a las nuevas realidades. Se evidencia una línea muy fina que distingue la utilización legítima de los dispositivos o sistemas de la informática de los abusos que se pueden cometer con ellos o en su perjuicio. Además, el entorno digital facilita la realización de actividades ilegales de manera eficiente, cómoda y rápida. Por ello, es crucial entender la relación entre el Convenio de Budapest con respecto al Código Penal de Panamá en el ámbito del delito cibernético. Esto no solo permite presentar en forma clara y concisa las actualizaciones relevantes, inclusive facilitará un espacio para analizar el mejoramiento jurídico en este campo. Finalmente, se menciona que el proyecto de Legislación 632 concerniente al periodo 2021, que sugiere reestructuraciones y cambios requeridos que beneficiarán a las leyes penales en relación con el delito cibernético.

Asimismo, Alcalá y Meléndez (2023) mediante su trabajo sometido al analisis, considera importante estudiar las acciones delictivas en materia informática, el propósito de este estudio fue examinar y evaluar si las acciones delictivas vinculadas con la informática están definidos en las 32 empresas de México. Con la finalidad de llevar a cabo esta investigación, se empleó un enfoque deductivo y un método exploratorio, con el objetivo de asegurar la observación y poder verificar si las empresas que identifiquen los comportamientos ilegales en el ámbito digital en sus códigos penales facilitan la investigación y la denuncia, o si las mismas que no suelen reconocerlas fomentan su ignorancia, lo que resulta en la falta de denuncias y persecuciones de estas actividades delictivas. Se llegó a la conclusión de que la delincuencia cibernética representa ser un fenómeno global que abarca labores realizadas por medio del internet y tecnologías en materia digital, considerados como comportamientos ilegales vinculados con el manejo, transmisión, tratamiento y uso indebido de información en el sistema, red o programas de la informática, donde el bien jurídico que resultó perjudicado fue la información. Las acciones ilegales que utilizan recursos de la tecnología o medios de comunicación masiva impactan en la información de una persona (sonidos, imágenes, mensajes, etc.), en vista a su tratamiento, difusión, utilización indebida o alteración, lo cual atentará contra intereses jurídicos, bienes y derechos, como la privacidad, honor, dignidad, imagen, libertad sexual, privacidad de la información, propiedad intelectual, otros. Además, se tomó en consideración la importancia de establecer la clasificación de las acciones delictivas cibernéticas relacionados con los datos, ya que, en México, a pesar de la existencia de conceptos en el aspecto federal y algunas en la ley local, estas actividades delictivas no están claramente tipificadas en un marco legal específico. Asimismo, las sanciones establecidas en las normativas son variadas o bastante leves con respecto al impacto sobre el bien jurídico protegido.

Por su parte Díaz et al. (2023) mediante su labor investigativa resaltaron la importancia de analizar los retos de la ley ecuatoriana ante las actividades delictivas ligadas a la informática, para que pueda establecerse los mecanismos necesarios para prevenirlas, el análisis cualitativo de las actividades delictivas cibernética, fundamentado mediante el Código Orgánico Integral Penal, pone de manifiesto una interacción compleja entre las leyes y las percepciones de diferentes actores sociales. asimismo, se llevaron a cabo diferentes entrevistas a empleados bancarios, abogados, fiscales, jueces y miembros de la comunidad en general. Estas entrevistas ofrecen una visión sobre la interpretación personal de las normativas y la falta de competencias respecto a las actividades delictivas mencionadas. Se resalta la urgencia de aumentar la conciencia y la formación mayormente en el trabajador judicial y de la banca, para poder enfrentar de manera efectiva estos delitos, por otra parte, se subraya la necesidad de que la legislación se adapte continuamente para hacer frente a los retos que suelen modificarse en el entorno digital, garantizando de esta manera soluciones de carácter legal adecuada ante las situaciones amenazantes cibernéticas. También se hace evidente la importancia de informar a la población para prevenir que se conviertan en potenciales víctimas de dicha modalidad delictiva.

Según Quevedo (2017), en su tesis indica que el constante avance de las tecnologías informativas y su uso generalizado ha impactado en la criminalidad y la delincuencia, ya que el surgimiento de nuevos delitos y formas de cometer acciones delictivas tradicionales ha incrementado la cantidad de bienes jurídicos que necesitan ser protegidos penalmente, los cuales pueden verse amenazados por los que aplican avances científicos para llevar a cabo sus intenciones delictivas. Las mencionadas modificaciones en la criminalidad convencional han hecho que la delincuencia cibernética se convierta en un desafío importante que requiere una solución legislativa adecuada. Además, se señala que estos comportamientos ilegales, que son planificados y se realizan sacando provecho de las oportunidades que brindan las innovadoras

tecnologías, evidencian una serie de particularidades y complicaciones en su enjuiciamiento e investigación, identificando a las personas que tengan la responsabilidad de dichos actos ilícitos. Sin embargo, el desarrollo de tecnologías nuevas no solo amplía las oportunidades para los delincuentes, sino que también ofrece mecanismos efectivos para la investigación a las autoridades. Por lo tanto, es fundamental que se encuentre un equilibrio delicado entre las competencias de un Gobierno para enfrentar esta nueva forma de criminalidad y el escenario de protección que su sistema constitucional asegura a toda persona ante otras.

Según Santana (2018) mediante su trabajo realizado consideró necesario proponer un programa configurar la privacidad de las redes sociales como es el caso del Facebook durante el periodo 2018 en la escuela secundaria oficial Lic. Isidro Fabela # 136 de San Nicolás Coatepec, ubicado en México, en dicha labor se argumenta que uno de los aspectos más relevantes, y que a menudo la mayoría de los usuarios suelen ignorar, resulta ser el hecho de configurar la privacidad de los perfiles. Los jóvenes piensan que poseer redes sociales, fomentar la búsqueda de amistades, y compartir datos sin considerar los mínimos criterios de privacidad con supuestas "amistades", no tendrá ningún impacto en sus vidas. Esto se debe a que creen que no hay riesgos en las redes sociales. Sin embargo, una configuración de privacidad mínima o inexistente en Facebook puede tener consecuencias graves para todo individuo, afectando su bienestar físico, moral e inclusive su situación económica. En la labor investigativa realizada se menciona que los jóvenes adoptan tres enfoques para determinar la privacidad que corresponda al perfil: primeramente, implementan medidas para proteger los niveles de privacidad; luego, experimentan una apertura gradual de los perfiles; y tercero, deciden hacer su perfil completamente público.

Por otro lado, Ruiz (2016) ha postulado mediante su trabajo investigativo, la importancia de analizar las actividades delictivas de la informática y la forma en la cual se violan los derechos constitucionales, una de las causas del incremento de la modalidad delictiva

cibernética es la complejidad para la identificación y localización de los responsables, lo que provoca que muchos de estas diversas formas de criminalidad queden sin castigo. Esto, a su vez, lleva a que la población pierda la fe en un sistema de justicia que sea efectivo y oportuno y eficaz. Por lo tanto, resulta ser un tema fundamental que el gobierno del Ecuador pueda brindar protección a quienes están detrás de estos delitos, mediante la reforma de las leyes en el país, con la finalidad de que se pueda establecer formas adecuadas de realizar campañas políticas y de esta manera lograr fomentar un nuevo enfoque en la actividad política en Ecuador.

1.4.2. Antecedentes nacionales

Según Arapa et al. (2024) mediante su trabajo de investigación, considera importante analizar los motivos y consecuencias del aumento de las acciones delictivas en materia informática durante el periodo 2023 en Puno. De igual manera, el estudio es de tipo cuantitativo y tiene un enfoque explicativo. Por último, en la ciudad de Puno se ha observado un preocupante aumento continuo de diversas modalidades delictivas cibernéticas, atribuible a diversas razones como la falta de información, el avance tecnológico y la escasa conciencia relacionada con el tema. Además, se ha podido identificar otra razón: la debilidad en nuestros sistemas informáticos, resultado de una seguridad cibernética deficiente, lo que provoca un mayor número de víctimas de estas actividades delictivas, especialmente entre individuos comprendidos en una edad de 27 a 59 años.

Por su parte, Cantorin (2024) resalta la importancia de analizar el perfil del delincuente cibernético en las actividades delictivas ligadas a la informática como el caso del grooming durante el periodo 2023 en la ciudad de Lima, el estudio realizado analiza y detalla las particularidades del perfil de los delincuentes cibernéticos involucrados en actividades delictivas de grooming en Lima. Se utilizó una metodología cualitativa, básica y respetando un enfoque fenomenológico, aplicando entrevistas como técnica principal y un instrumento guía

para las mismas, además de implementar la técnica de triangulación. Los hallazgos revelaron que las características del perfil de estos ciberdelincuentes incluyen: adultos, predominantemente hombres, que sienten una fuerte atracción hacia los menores, emplean identidades ficticias y el anonimato, son manipuladores y acosadores, muestran poca empatía, tienen un alto nivel de conocimiento en informática, se perciben como superiores, provienen de entornos familiares disfuncionales, tienen un nivel económico bajo y buscan obtener beneficios económicos a través de la venta de contenido sexual, aunque en algunos casos lo hacen por placer. En conclusión, las características del perfil de los delincuentes cibernéticos con respecto al grooming están influenciadas por factores sociales, económicos y familiares. Estos rasgos abarcan la conducta del ciberdelincuente, experiencias de rechazo afectivo, antecedentes familiares, situación económica y conocimiento tecnológico, entre otros. Reconocer el perfil de los ciberdelincuentes en grooming va facilitar a las personas encargadas de operar justicia que impongan diversas sanciones que sean idóneas según la legislación vigente e implementar políticas de seguridad en el uso de tecnologías digitales, con el fin de proteger la integridad de las víctimas.

Asimismo, Perez (2021) mediante su labor investigativa resaltó la importancia de analizar el ámbito dl secreto con respecto a toda diligencia realzada preliminarmente en las acciones investigativas contra la criminalizad organizada y como se está relaiconando con el derecho con el que una persona imputado cuenta. Los hallazgos indicaron aproximadamente un 70% de las personas que participaron ha reconocido que con respecto a la confidencialidad de las diligencias iniciales permite al fiscal que pueda fundamentar la gran mayoría de sus decisiones en forma que pueda respetar el derecho a la defensa que posee la persona que resultó ser acusada. Se establece como conclusion que el grado de confidencialidad de las mencionadas diligencias, durante un tiempo razonable, impide que el acusado y su defensa técnica tengan acceso a las acciones del Ministerio Público y los efectivos policiales, los mismos que generan

una serie de perjuicios al principio de contradicción y la igualdad de condiciones, que son los objetivos principales de la reforma de todos los procedimientos de carácter penal.

Por su parte, Poma (2020) mediante su labor investigativa, consideró importante analizar el ámbito de las investigaciones preliminares en los procedimientos de carácter penal evidenciados en el Perú, la problemática y hechos en los cuales se termine afectado los fundamentales derechos, ante ello se ha resaltado a manera de conclusión de que la fase de investigación preliminar, como parte del proceso de investigación preparatoria, tiene como objetivo reunir y recopilar pruebas relevantes y útiles que van a facilitar el esclarecimiento de si los hechos que han sido materia investigativa realmente ocurrieron, así como establecer una serie de garantías que se consideren necesarias para que se pueda presvervar los elementos materiales relacionados con su comisión. Además, en numerosas investigaciones preliminares se han presentado y continúan presentándose violaciones a los derechos fundamentales, como ocurre con los plazos establecidos para la duración de la detención preliminar o en situaciones de flagrancia, que no deben exceder las veinticuatro horas, o los quince días en casos de tráfico de drogas, espionaje y terrorismo.

Según Tenorio (2018), mediante su trabajo realizado considera importante analizar el ámbito de las oportunidades y desafíos concernientes a la decisión del Perú para adherirse al Convenio de Budapest para casos de la delincuencia cibernética durante el periodo 2018, es importante señalar que la ciberdelincuencia se ha convertido en un desafío global el cual evidencia un aumento significativo y constante. En las últimas dos décadas, se han reportado una serie de incidentes como la interrupción de operaciones en diversas organizaciones a nivel mundial debido a software de ransomware y también casos relacionados al robo de información digital con fines de lucro. Por otra parte, en el Perú, se han documentado casos de delitos cibernéticos parecidos que han afectado a instituciones, empresas e individuos comunes, resultando en significativas pérdidas económicas en años recientes. Además, se menciona que

Perú resultó ser uno de los países en abordar la problemática de las actividades delictivas ligadas a la informática en su Código Penal a principios de este siglo, adicionando diversas disposiciones sobre el acceso o uso indebido de bases de datos, redes o sistemas con la finalidad de conseguir diferentes beneficios y causar daños. Sin embargo, este esfuerzo tiene un alcance y jurisdicción nacional, lo que limita la capacidad de respuesta rápida con altos niveles de efectividad ante acciones delictivas perpetradas desde fuera del país.

Asimismo, De la Puente (2020), mediante su trabajo investigativo, resalta la importancia de analizar los aspectos de la difusión e interceptación y difusión de las comunicaciones que son de carácter privado, así como el ámbito de la libertad de la comunicación en los procedimientos judiciales en el Perú durante el periodo 2020. La batalla contra el delito cibernético, en su sentido más concreto (es decir, los delitos perpetrados en línea), representa solo una faceta del reto. Por otra parte, otra faceta es la constante lucha contra el crimen informático en un sentido más amplio, que también está en crecimiento a nivel global. En nuestro país, se han establecido diversos tipos penales mediante el Código Penal con la finalidad de que se pueda abordar ambos fenómenos y se han promulgado una serie de normativas específicas, tal como la Ley Nº 30096.

Según Reyes (2020), mediante su labor investigativa, resalta la importancia de analizar las actividades delictivas informáticas así como la forma en la cual influye en los niveles de integridad individual durante el periodo 2020 en la localidad distrital de Chorrillos, las actividades delictivas ligadas a la informática se define como una conducta ilícita, típica y culpable que se lleva a cabo a través de la aplicación de diversos mecanismos digitales o que tiene como objetivo alterar la información y data concerniente a un dispositivo electrónico. Este concepto busca abarcar la perspectiva de la tecnología, integrando la noción general de actividad delictiva y considerando el uso de herramientas informáticas. Esto implica que puede generar cierta afectación a los niveles de integridad de carácter personal en sus dimensiones

psicológicas, morales y físicas, tanto en personas adultas como en jóvenes y población infantil, quienes resulten ser especialmente susceptibles a esta modalidad delictiva, que se desarrollan en un entorno completamente expuesto a avances tecnológicos y digitales.

1.5 Justificación de la investigación

1.5.1. Justificación metodológica.

Se sustenta en que la labor investigativa servirá de ayuda para orientar proyectos con esta opción metodológica. Por otro lado, los mecanismos empleados en elaboración de la presente investigación son evaluados mediante las acciones pertinentes de profesionales expertos para validar el grado de confiabilidad, por otra parte, el resultado que se obtenga servirá para futuras investigaciones con las variables que se están desarrollando.

1.5.2. Justificación práctica

La labor investigativa realizada no solo representa la actividad en lo que concierne al uso de la tecnología informática en el país; sino a nivel mundial, el internet no conoce de limites como se advierte del último ataque cibernético que se ha ejecutado a nivel mundial afectando de manera directa a más de 74 naciones, perjudicando a instituciones del sector privado y público; debido a ello, el legislador comprendido dicho fenómeno de acelerada evolución, ha visto por conveniente la creación de la Ley 30096, facilitando así su medición en el tiempo.

Siendo así, este trabajo se realizará para medir la eficacia de la parte procesal y la norma sustantiva en lo que respecta a los delitos informáticos, así como proponer alternativas de solución que puedan dotar de mecanismos para el fiel cumplimiento de la ley antes mencionado, cumpliendo su razón de ser, y consecuentemente prevenir y en la medida de lo posible erradicar este flagelo.

1.5.3. Justificación teórica

Consiste en investigar y ampliar la teoría del indubio pro reo vs. Pro societatis, el cual es una derivación del que se refiere a la teoría de la inocencia, entre sus objetivos resalta el hecho de establecer una serie de garantías para que un individuo no sea condenado si es que el medio probatorio no resulte ser trascendental o de gran magnitud para generar la desvirtuación de las que son de descargo. Además, se postulan otro tipo de teorías que se encuentran vinculadas a las variables denominadas como delito informático y diligencias preliminares, en la cual explican los principales componentes y otro tipo de aspectos relacionados con las variables antes mencionadas para equiparar su valor actual con otras investigaciones respecto del tema, como refiere la valoración teórica la misma que está sustentada en que los resultados de la labor investigativa podrán incorporarse y generalizarse al conocimiento de la ciencia, asimismo se utilizará para que se llenen ciertos vacíos cognoscitivos que se estén evidenciando o refutando los diversos resultados de otros trabajos investigativos o ampliando el modelo teórico.

1.5.4. Justificación legal

La justificación legal de esta labor investigativa radica en el requerimiento de que se pueda evaluar y mejorar la efectividad de las diligencias preliminares en la labor investigativa de actividades delictivas ligadas a la informática en el Cercado de Lima, en el marco de la Ley N° 30096, que tipifica estos delitos, y el CPP (DL N° 957), que determina principios fundamentales como la legalidad, eficacia y celeridad en los procesos. Asimismo, se considera la Ley N° 30364, que protege los derechos de las víctimas, y el cumplimiento de convenios de carácter internacional tal como se da con el caso del Convenio de Budapest sobre Cibercriminalidad, que resalta la cooperación en la labor investigativa de las actividades delictivas cibernéticas. Al identificar deficiencias en la ejecución de diligencias preliminares, esta investigación pretende contribuir a la construcción de un sistema de justicia más eficiente

y equitativo, garantizando así el debido respeto por todo derecho y fortaleciendo las acciones pertinentes para que el Perú se sienta comprometido en combatir la criminalidad cibernética a nivel global.

1.5.5 Importancia

La investigación sobre la influencia de las diligencias preliminares en las actividades delictivas ligadas a la informática en el Cercado de Lima es crucial para avanzar en varios ODS, con mayor énfasis en el ODS 16, que promueve la paz, la justicia y la institucionalidad. Al evaluar y establecer un mejoramiento de los niveles de eficacia de la labor investigativa de actividades delictivas informáticas, esta investigación no solo contribuye a la reducción de la criminalidad y para que todo derecho de las víctimas se encuentre debidamente protegidos, sino que también fortalece la confianza en el sistema judicial, un aspecto esencial para que se construya una sociedad inclusiva y justa. Además, al abordar la ciberseguridad y proteger los derechos digitales, la investigación apoya el ODS 9, que busca fomentar la innovación y la infraestructura resiliente, promoviendo un entorno seguro para el desarrollo sostenible en la era digital.

1.6 Limitaciones de la investigación

Entre las principales, se pueden citar la poca cantidad de antecedentes internacionales de postgrado con respecto a la variable denominada diligencias preliminares, no siendo un factor determinante en el logro de las metas principales de la labor investigativa en la totalidad de su contexto.

1.7 Objetivos de la Investigación

1.7.1. Objetivo general

Evaluar cómo influye las diligencias preliminares en los delitos informáticos en el Cercado de Lima, año 2024.

1.7.2. Objetivos específicos

- Explicar cómo influye la dimensión investigativa en los delitos informáticos en el Cercado de Lima, año 2024.
- Evaluar de qué manera influye la dimensión preventiva en los delitos informáticos en el Cercado de Lima, año 2024.
- Explicar de qué manera influye la dimensión resolutiva en los delitos informáticos en el Cercado de Lima, año 2024.

1.8 Hipótesis

1.8.1. Hipótesis general

Las diligencias preliminares influyen positivamente en los delitos informáticos en el Cercado de Lima, año 2024.

1.8.2. Hipótesis específicas

- La dimensión investigativa influye positivamente en los delitos informáticos en el Cercado de Lima, año 2024.
- La dimensión preventiva influye positivamente en los delitos informáticos en el Cercado de Lima, año 2024.
- La dimensión resolutiva influye positivamente en los delitos informáticos en el Cercado de Lima, año 2024.

II. MARCO TEÓRICO

2.1 Marco conceptual

2.1.1 Teorías generales sobre la variable independiente. Diligencias preliminares

2.1.1.1. Enfoque teórico del sistema Inquisitivo. Surgió ante cierta influencia de la Iglesia Católica y se caracteriza por concentrar las funciones de acusación y juicio en una única figura, el juez, ante quien el acusado se encuentra en una posición de desventaja. Entre las principales particularidades se mencionan: (a) La apertura del proceso no dependerá exclusivamente de quien acuse, se aplica el principio de procedat iudex ex oficio; (b) Un juez tiene la facultad de definir tanto de manera objetiva como subjetiva una determinada acusación; (c) Una labor investigativa de los actos y la determinación de las pruebas a presentar son llevadas a cabo por el juez que actúa como acusador; (d) No hay una relación directa entre la sentencia y acusación, ya que el juez puede modificar la acusación en cualquier momento. Además, no existe igualdad ni contradicción entre las partes, ya que no hay una verdadera división. Por otra parte, los poderes del juez resultan ser absolutos frente a una persona acusada que se encuentra indefenso ante él, siendo la detención una práctica común. (Pinto, 2017).

2.1.1.2. Enfoque teórico del sistema acusatorio. Fue dominante en la antigüedad, desarrollándose en la República Romana y en Grecia, y continuó hasta el siglo XIII. Se fundamentaba en la primacía de la persona y la inacción del Estado. De igual manera, el proceso acusatorio se caracteriza por la asignación y delimitación clara de las funciones de cada participante en el proceso. En este contexto, solo el acusador tenía la facultad de perseguir la acción delictiva y ejerciendo el poder de requerimiento; el acusado contaba con diversas oportunidades para refutar la acusación, gracias a las acciones pertinentes que le facilitaron reconocer sus derechos de defensa; y, finalmente, el tribunal tenía la autoridad para tomar decisiones. Además, la persona acusada era vista como un sujeto con derechos, manteniendo una posición de igualdad frente a la persona que cumple el rol de acusador, lo que daba lugar

a principios como el indubio pro reo y la presunción de inocencia. Asimismo, mientras que la libertad era la norma, sin embargo, la detención se consideraba como una excepción (Pinto, 2017).

2.1.1.3. Enfoque teórico del sistema mixto. Emergió durante la Revolución Francesa, radica en la ruptura con los modelos citados con anterioridad. Esto implica que la persecución judicial de actividades delictivas no representa ser un derecho exclusivo de los individuos y que el juez no puede desempeñar simultáneamente el papel de acusador. Entre sus particularidades se resaltan las siguientes: (a) Existe una clara separación entre las funciones de juzgar, instruir y acusar, las cuales son asignadas a diferentes instancias, tribunal, juez de instrucción, fiscal, a excepción del tribunal con jurado, se aplica el principio conocido comúnmente como doble instancia; (b) Se establece también el principio de tribunal colegiado; (c) La administración de justicia recae en jueces profesionales, salvo en los casos en que interviene el jurado; (d) La valoración de las pruebas se realiza de manera libre; (e) Las acciones penales resultan ser indisponible y regirá por los parámetros de la teoría de necesidad a lo largo de todo el proceso. Además, las acciones penales resultan ser irretractable; (f) El acusado deja de ser meta de la labor investigativa y se convierte en un sujeto con derechos. Ante el mencionado contexto, el Estado asume la responsabilidad de presentar pruebas. (Pinto, 2017).

2.1.1.4. Enfoque teórico del principio de indubio pro reo vs. Pro societatis. Se considera una extensión del principio de presunción de inocencia y su objetivo es asegurar que un individuo no sea condenado si las pruebas en su contra no son lo suficientemente significativas como para invalidar completamente las pruebas a su favor. Históricamente, se ha descrito como una norma de interpretación judicial que permite al juez absolver al acusado, ya que la evidencia presentada durante el juicio ha generado incertidumbres sobre la culpabilidad del mismo (San Martín, 2006)

2.1.2. Antecedentes de las diligencias preliminares

Este sistema fue el dominante en la antigüedad, desarrollándose en la República Romana, así como en Grecia y continuó hasta el siglo XIII. Su fundamento se basaba en la primacía del individuo y la inacción del Estado. El proceso acusatorio se caracterizaba por la clara asignación y delimitación de las funciones de cada parte involucrada. De este modo, solo el acusador tenía la facultad para perseguir la actividad delictiva ejerciendo el poder de requerimiento; la persona acusada contaba con amplias oportunidades para que se refute la acusación, gracias al reconocimiento de sus derechos para que pueda ejercer su defensa; y, finalmente, el tribunal tenía la autoridad para poder tomar decisiones. El acusado era visto como un sujeto con derechos, manteniendo una posición de igualdad frente al acusador, lo que daba lugar a principios como el indubio pro reo y la presunción de inocencia. Además, mientras que la libertad era la norma, la detención se consideraba una excepción (Pinto, 2020).

La esencia de este sistema, que emergió durante la Revolución Francesa, radica en la ruptura con los modelos previos. Esto implica que la persecución judicial de actividades delictivas no representa ser un derecho exclusivo de los individuos y que el juez no podrá desempeñar simultáneamente el papel de acusador.

Tomando en consideración a Joan Verguer Grau, sus características son las siguientes:

- Existe una clara distinción entre las funciones de juzgar, instruir y acusar, que son asignadas a diferentes entidades tribunal con jurado, juez de instrucción y fiscal. A excepción del tribunal con jurado, se aplica la doble instancia.
- También se establece los parámetros señalados por medio del principio de tribunal colegiado.
- La administración de justicia recae en jueces profesionales, salvo en los casos en que suele intervenir el jurado.
- La valoración de las pruebas se realiza de manera libre.

- Las acciones de carácter penal resultan ser indisponible y regirán por la teoría de necesidad a lo largo de la totalidad del proceso. Además, resultan ser irretractables.
- El acusado deja de ser un mero objeto de análisis y se convierte en un sujeto con derechos. En este contexto, el Estado asume la responsabilidad de presentar pruebas. (Pinto, 2020).

2.1.3. Definición de las diligencias preliminares

Las diligencias preliminares según Perez (2021) se trata de la primera subfase, prejurisdiccional que se encuentra relacionada con el procedimiento, en la cual un determinado fiscal posee toda la autoridad, conforme a lo establecido por la ley procesal, para clasificar los casos en los que llevará a cabo una investigación formal. Esta fase incluye una investigación preliminar destinada a reunir los elementos necesarios que se utilizarán en la formalización del proceso, así como a obtener pruebas mínimas e identificar al autor de la actividad delictiva. La diligencia preliminar representa ser una etapa dentro de una labor investigativa preparatoria que precede a la fase propiamente dicha de esta investigación, en la que se ejecutan una serie de acciones urgentes e inaplazables para conseguir la verificación de las acciones denunciadas y estableciendo su particularidad delictiva. Esta fase es crucial para el éxito de la investigación, ya que se realizan las primeras acciones ante la sospecha de que se ha cometido un delito. (Vega, 2018).

Según la Casacion-Lima (2011) el objetivo de las diligencias preliminares es llevar a cabo acciones inaplazables y urgentes que permitan verificar si los actos a investigar realmente ocurrieron, garantizar la preservación de las pruebas y, además, lograr la identificación al presunto autor y así como a otros que se encuentren vinculados y que cumplan el rol de cómplices. Sin embargo, en la actualidad, no siempre se realizan estas actividades esenciales por diversas razones. Una labor preparativa investigatoria abarca una agrupación de acciones destinadas a reunir elementos de prueba, tanto de cargo como de descargo, que puedan brindar

las facilidades al fiscal para decidir si presenta o no una acusación y, en su caso, al acusado pueda asegurar la preparación de su defensa. El fiscal es quien lidera la investigación, reforzando el principio acusatorio, y cuenta con el apoyo de los efectivos policiales para llevar a cabo las acciones investigativas. Dentro del escenario de investigación preparatoria, existen 2 sub etapas que tienen sus propias normativas: 1) diligencia preliminar 2) investigación preparatoria.

2.1.4. Componentes de las diligencias preliminares

2.1.4.1.: Interposición de la denuncia. Para López (1993) para entender lo que significa una denuncia debe entenderse como todo acto procesal que consiste en una manifestación de conocimiento, ya sea de forma verbal o escrita, realizada por un individuo específico. A través de esta declaración, se informa al responsable del organismo competente acerca de la presencia de algún tipo de acto que tiene las características de una actividad delictiva.

2.1.4.2. Diligencias a practicar. Para Vanderbosch (1980) define la investigación del delito como una combinación de ciencia y arte, dondse sus misterios solo pueden ser revelados a través de la práctica constante de las diferentes habilidades que se desarrollan con la experiencia al abordar casos, así como por la observación y el análisis exhaustivo del delincuente, su conducta y su entorno físico y social.

2.1.4.3. Plazo máximo. Según la Casacion-La Libertad (2008), se establecen en el caso de las diligencias preliminares aproximadamente 20 días naturales. En cuanto al tiempo que se otorga al fiscal para establecer un plazo diferente, este varía según las particularidades, la circunstancia y la complejidad de los actos que se están investigando. Estos plazos son distintos y no están incluidos en los 120 días naturales, incluida las extensiones señaladas en la normativa correspondiente, que se refieren a la investigación preparatoria en sí.

2.1.5. Importancia de las diligencias preliminares

La fase de investigación preliminar es crucial para el éxito del proceso investigativo, ya que en esta etapa se llevarán a cabo las primeras acciones ante la sospecha de que se ha cometido un delito. En este contexto, se tomarán las primeras declaraciones y se realizarán las primeras actividades de investigación, marcando así el inicio del proceso. Por lo tanto, dado que esta investigación está bajo la responsabilidad del Ministerio Público, el éxito de esta fase dependerá en gran medida de la actuación del fiscal involucrado (Vega, 2018).

La relevancia de esta fase se basa en la obligación del Estado de investigar las conductas delictivas; en la necesidad de atender todas las denuncias que presenten características de delito, con el objetivo de que pueda comprobarse tanto la credibilidad como el contenido, en la importancia de que puedan recibirse las primeras declaraciones; en la recolección de los primeros indicios probatorios; en la preservación de estos elementos; en la implementación de las primeras medidas coercitivas o cautelares; y en la posterior determinación de si hay suficientes pruebas para proseguir con la investigación preparatoria (Sánchez, 2009)

2.1.6. Marco legal de diligencias preliminares

Se encuentran reguladas en el CPP en su art. 330, que establece lo siguiente:

- Un Fiscal, bajo su supervisión, puede solicitar la intervención de los efectivos policiales o llevar a cabo por su cuenta diligencias preliminares de la labor investigativa para establecer si resulta necesario que se formalice la Investigación Preparatoria.
- El propósito inmediato de las Diligencias Preliminares es llevar a cabo acciones inaplazables y urgentes que permitan verificar si los hechos en cuestión han ocurrido y su carácter delictivo, así como garantizar la preservación de los componentes materiales relacionados con su ejecución, identificar a los individuos implicados, incluidos las personas agraviadas, y según las limitaciones legales.

- Cuando el Fiscal tenga pleno conocimiento de una actividad delictiva que implique el ejercicio público de las acciones penales, podrá presentarse de inmediato en el sitio de los actos con el personal y los recursos especializados necesarios, y realizar un riguroso análisis con el objetivo de establecer la veracidad de los hechos y, si es necesario, evitar que el delito genere consecuencias adicionales y que la escena del crimen sea alterada.

Asimismo, el CPP en su art. 331 prescribe en relación a la actuación policial lo siguiente**:**

- En cuanto la Policía tenga conocimiento de la ocurrencia de una actividad delictiva, informará al Ministerio Público de la manera más expedita y también de manera escrita, detallando los aspectos fundamentales del hecho y otros componentes que se hayan recopilado inicialmente, así como las acciones realizadas, sin dejar de mencionar la totalidad de documentación existente.
- Incluso después de haber notificado la acción delictiva, los efectivos policiales seguirán con la labor investigativa que haya comenzado y, tras la participación del Fiscal, llevará a cabo las investigaciones adicionales que le sean asignadas conforme a lo señalado por medio del artículo 68.

Las citaciones que la policía realice a las personas durante la labor investigativa pueden realizarse hasta en tres ocasiones. Además, el CPP en su art. 332 señala en relación al informe policial:

- La policía, en todos los casos en que actúe, deberá presentar un informe al fiscal.
- Este informe incluirá los antecedentes que justificaron su intervención, un resumen de las diligencias realizadas y un riguroso estudio de las acciones investigadas, evitando emitir algún tipo de calificación jurídica o atribuir responsabilidades.
- El informe de la policía deberá adjuntar las actas que se hayan levantado, las declaraciones que se han recibido, los análisis, las sugerencias sobre acciones de

investigación y cualquier otro elemento que considere esencial para aclarar la imputación, así como la verificación del domicilio y la información individual de las personas acusadas.

Asimismo, el Artículo 333° menciona la Coordinación interinstitucional entre el Ministerio Público y la Policía Nacional.

Sin menoscabo de la estructura policial establecida por la Legislación y lo que se dispone mediante el art 69, los efectivos policiales crearán un organismo encargado de la coordinación de funciones investigativas con el Ministerio Público, establecerá los canales de comunicación con los organismos gubernamentales de las fiscalías y Ministerio Público, centralizará el dato en relación al crimen organizado y violento, aportará su experiencia en la formulación de acciones y programas para una persecución adecuada de la actividad delictiva, y desarrollará componentes de seguridad y protección.

2.1.7. Derecho comparado sobre las diligencias preliminares

2.1.7.1. Chile. Según el código de procedimientos penales chileno la diversidad de acciones investigativas se lleva a cabo de la siguiente manera:

Artículo 180. Labor investigativa por parte de los fiscales, quienes tienen la entera responsabilidad de dirigir la labor y realizarán las diligencias que se consideren necesarias por sí mismos o incluso podrán delegarlas a los efectivos policiales, según lo consideren adecuado para aclarar los hechos.

Sin perjudicar lo establecido en el primer párrafo, en las 24hrs posteriores a que tengan conocimiento de un hecho que presente características de actividad delictiva de acción penal pública, a través de los medios establecidos por la legislación, en esos casos un fiscal deberá llevar a cabo todas las diligencias relevantes y de suma utilidad para esclarecer y averiguar el hecho, así como las circunstancias importantes para que se aplique la legislación penal, los involucrados en los actos y los elementos que permitan verificar su responsabilidad. Además,

deberá evitar que el hecho denunciado genere algún tipo de consecuencias adicionales. Por otra parte, es importante resaltar que todo fiscal posee la facultad de solicitar información a cualquier individuo o funcionario público, quienes no podrán negarse a brindarla, con excepción a casos exceptuados a través de las normativas.

Artículo 181. Labores investigativas con el objetivo mencionado en el anterior artículo, dicha labor se realizará de manera que se registre y asegure la totalidad de lo que contribuya a la verificación del hecho y a que se pueda identificar a los involucrados. Se documentará el estado de las personas, objetos o sitios, se tendrá plenamente identificados a los testigos de la acción investigada y se registrarán sus respectivas declaraciones. Asimismo, si el hecho ha dejado señales, rastros y huellas, podrá tomarse nota de las mismas y se especificarán de manera detallada, asimismo se podrá describir el lugar donde ocurrió, del cómo se encuentran los objetos presentes y de cualquier otro tipo de información que sea de carácter relevante.

Para cumplir con los objetivos de la investigación, se podrán tomar fotografías, realizar operaciones científicas, sonidos, videos y en general, reproducir imágenes, sonidos y voces utilizando los mecanismos técnicos que resulten ser más apropiados, requiriendo la colaboración de organismos especializados. En estos casos, una vez realizada la operación, se certificará la fecha, hora y lugar en que se llevó a cabo, así como el nombre, dirección y profesión de quienes participaron, además de la identificación de la persona examinada y la descripción del objeto, evento o fenómeno reproducido o explicado. Ante ello, se tomarán las medidas que sean requeridas para que se evite cualquier tipo de alteración de los originales involucrados en dicha actividad (Biblioteca del Congreso Nacional de Chile, 2023).

2.1.7.2. Colombia. se resalta la importancia del código para procedimientos de carácter penal basándose en:

Artículo 175°. – El plazo que tiene la Fiscalía para presentar la acusación o solicitar la preclusión no podrá ser mayor a 90 días desde el siguiente día de que se formule la imputación,

excepto lo señalado por el art. 294. Este plazo se extenderá a 120 días en caso de concurso de actividades delictivas, si hay 3 o más personas imputadas, o si se trata de actividades delictivas que son calificados como plena competencia del juez penal de especializados circuitos.

Es importante señalar que la audiencia preparatoria se ejecuta en los 45 días posteriores a la audiencia donde se formule la acusación.

Por otra parte, la audiencia correspondiente al juicio oral comenzará en los 45 días posteriores a la finalización de la audiencia preparatoria.

Asimismo, la Fiscalía contará con un plazo máximo de 2 años contados desde que se recepcione la noticia criminis, con la finalidad de establecer la formulación de las imputaciones y decidir que pueda ser archivada. Este plazo se ampliará a 3 años si es que se presenta algún concurso del delito. En investigaciones relacionadas con actividades delictivas que son competencia del juez penal del especializado circuito, el plazo máximo de 5 años.

En los casos de actividades delictivas que caen bajo la competencia del juez especializado en lo penal, así como en delitos contra la Administración Pública y aquellos que afectan el patrimonio estatal, donde se justifique la detención preventiva, los plazos mencionados se duplicarán si hay tres (3) o más personas imputadas o delitos que se encuentren expuestos a investigación (Código de Procedimiento Penal de Colombia, 2004).

2.1.8. Teorías generales sobre los delitos informáticos

2.1.8.1. Teoría sobre la ciber criminología. Según Choi et al. (2023) indica que se fundamenta en un análisis interdisciplinario que incluye áreas como la criminología, la sociología, la informática, la psicología y la ciberseguridad. Su objetivo es entender las razones que impulsan el delito informático en el contexto del sistema penal. La ciber criminología investiga las causas y efectos de los delitos cometidos en línea, así como sus repercusiones legales, éticos y de las estrategias para su control y prevención.

2.1.8.2. Teoría de la transición espacial. Explica cómo las personas manifiestan comportamientos conformistas y no conformistas tanto en el mundo físico como en el digital: a) Una persona que en un ambiente físico limita algunas conductas en vista al contexto y condiciones del lugar, puede no ser capaz de contener esos mismos comportamientos en el entorno virtual. b) Cuestiones relacionadas con el anonimato, la flexibilización concerniente a la identificación y probabilidad alta de actuar de forma encubierta son elementos que el delincuente cibernético toma en cuenta cuando ejecuta sus acciones delincuenciales. c) el actuar de un ciberdelincuente puede ver el espacio virtual como una extensión de sus oportunidades, en vista que le proporciona un mayor nivel de impunidad, así como mecanismos de control acerca de sus acciones. d) El ciberespacio funciona como un lugar de coordinación y encuentro para que se ejecuten dichas actividades delictivas, ya sea en el mundo físico o en el digital, sacando provecho del anonimato y la falta de reuniones de manera presencial para planificar actividades delictivas. e) El entorno cibernético es el lugar ideal para llevar a cabo acciones delictivas que son difíciles de que pueda rastrearse y ofrece mayores oportunidades para que pueda evadirse la captura. f) Los principios y la ética que prevalecen en un entorno netamente físico son notablemente diferentes de los que se suelen aplicar en un entorno digital, lo que afecta la represión de delitos y reduce las barreras inhibidoras para los delincuentes en línea. g) Además, se debe considerar el efecto de la sofisticación y la globalización que caracterizan el mundo digital (Jaishankar, 2008).

2.1.9. Delitos informáticos

Según Luna (2020) es una rama de la ciencia del derecho penal que se ocupa de examinar qué elementos o características deben estar presentes en una conducta para que sea considerada un delito, o, en su defecto, cuáles son los factores que impiden que dicha conducta sea calificada como tal. La teoría del delito establece cuándo una acción es realmente delictiva. Esta teoría aborda el delito a partir de las leyes naturales, conceptualizándolo como una relación

de causa y efecto; en otras palabras, la acción se entiende como un fenómeno causal y/o natural que produce un resultado que puede ser un delito. Se distingue por su claridad en la plena identificación del nivel de culpabilidad, ya que para responsabilizar a una persona solo es necesario demostrar la causa, considerando el efecto como la consecuencia de que una persona será considerada culpable si se prueba que su acción fue la causa del resultado (Barrado, 2018).

2.1.10. Definición de los delitos informáticos

El delito cibernético, entendido como una conducta ilegal que se lleva a cabo a través de medios informáticos con fines sociales, políticos y económicos, en donde generalmente se plantea importantes retos para el marco legal. La inadecuada actualización de las normativas frente a las nuevas modalidades delictivas en el entorno digital crea una problemática a nivel mundial (Lobo et al., 2023).

Los continuos progresos en las actividades cibernéticas dificultan aún más la regulación, demandando una respuesta legal permanente. Los crímenes informáticos, al poner en jaque la seguridad jurídica establecida por la constitución, necesitan enfoques innovadores para salvaguardar los derechos de los individuos, así como sus propiedades y pertenencias. La dificultad de regular el ámbito informático y tecnológico resalta la urgencia de realizar estudios legales que puedan facilitar la implementación de diversos componentes y mecanismos que garanticen la seguridad jurídica en este sector (Arcos et al., 2023).

Según Villavicencio (2014), se han caracterizado los delitos cibernéticos como “acciones destinadas a eludir los sistemas de protección, lo que incluye intrusiones en computadoras, correos electrónicos o bases de datos mediante el uso de contraseñas; son comportamientos que solo pueden llevarse a cabo por medio de componentes tecnológicos, desde un punto de vista más amplio, abarca todas las acciones en las que las TIC resulten ser calificadas como el medio, objetivo, meta o contexto en el que se realizan, inclusive si es que suelen impactar en distintos bienes jurídicos.

2.1.11. Dimensiones de los delitos informáticos

2.1.11.1. Dimensión 1: Acceso ilícito. Basándose en Lopez (1993), en este contexto, se penaliza la infracción de la privacidad, que ocurre mediante el ingreso no permitido al sistema, comprometiendo las medidas de protección diseñadas para impedir que personas no autorizadas accedan a un sistema informático. El término "acceder" se refiere a la acción de entrar o llegar a un lugar, y en este caso, implica el acto de ingresar sin el consentimiento del propietario a un sistema.

2.1.11.2. Dimensión 2: Fraude Informático. según Villavicencio (2014) sanciona varios tipos de conductas. Como las ligadas al diseño (plan o proyecto)(1), introducir (ingresar a un sitio) (2), alteración (dañar, estropear, descomponer) (3), borrar (quitar, desvanecer, lograr que se pueda desaparecer)(4), suprimir (desaparecer)(5), clonación (generar clones) (6) datos de la informática o ciertas interferencias, manipulación (operaciones con instrumentos o con las manos) (7) funcionamiento de mecanismos de la informática (adquiriendo o consiguiendo algo) (8) beneficio para perjudicar a terceras personas.

2.1.11.3. Dimensión 3: Suplantación de identidad. Según Villavicencio (2014) se considera un delito de resultado, ya que no es suficiente con llevar a cabo la acción típica de suplantar la identidad; también es imprescindible que dicha acción produzca un efecto adicional, que es ocasionar un daño. Por ejemplo, elaborar perfiles falsos en plataformas sociales (twitter, Facebook, correos electrónicos) que se hagan pasar por personas físicas o jurídicas con el fin de engañar y dañar a otros.

2.1.12. Marco legal

Durante el periodo 2013, se promulgó la Ley Nº 30096 con la finalidad de combatir las actividades delictivas en perjuicio de la informática, cuyo propósito fue garantizar la prevención y sanción de acciones ilegales que afectan los sistemas y la información digital, así como la integridad y libertad sexual, la privacidad así como todo lo concerniente al ámbito del

secreto de las comunicaciones, fe pública y el patrimonio, en las que el infractor emplea la tecnología moderna para llevar a cabo estos delitos. Esta ley fue modificada por la Ley Nº 30171, que se publicó en el periodo 2014, añadiendo a los delitos penales el acceso no autorizado (art. 2º), la violación de la integridad de información y sistemas de la informática (art 3 y 4), interceptación de información (art7), fraude digital (art8º) y abuso de herramientas y diversidad de dispositivos digitales (art10), incorporando las expresiones "ilegítimamente y deliberada" para enfatizar que estos delitos se ejecuten con dolosa intención. Además, se eliminó el art 6 que definía el tráfico ilegal de la información.

2.1.13. El Perfil del ciberdelincuente

Según Vega y Arévalo (2022) menciona que es una palabra formada por la combinación del prefijo "ciber" y el sustantivo "delincuente", la misma que generalmente se utiliza para la identificación de un individuo que lleva a cabo esta acción ilegal, la cual es desaprobada y rechazada por la comunidad. Según Jiménez (2017), la irrupción de la criminalidad en el entorno digital ha puesto de manifiesto la existencia de un área carente de regulaciones legales, lo que facilita la realización de delitos a través de esta tecnología. Un punto relevante es la notoria dificultad para que se pueda establecer realmente quien ha sido el autor de estas acciones.

En relación a las particularidades de delincuente informático se menciona a Vega y Arévalo (2022), quienes se menciona que cada conducta típica de un infractor está vinculada a ciertas características específicas. En el ámbito del delito informático conocido como grooming, los delincuentes en línea han aportado un cambio importante en el estudio de la criminología. Esto se debe a que las formas de delinquir, las situaciones asociadas y el contexto que rodea estos delitos requieren la elaboración de un nuevo perfil delictivo que se ajuste a los avances tecnológicos y a los recursos utilizados para que se comentan tales actos. Por esta

razón, ha surgido una corriente de pensamiento que se conoce comúnmente bajo el nombre de ciber criminología.

2.1.14. Características del perfil del ciberdelincuente

Es fundamental realizar registros minuciosos sobre diferentes facetas de la vida de un delincuente cibernético, ya que estas particularidades son comunes y se fomenta la búsqueda de la identificación de un patrón, tomando en consideración los siguientes elementos: a) Dimensión social, generalmente son personas introvertidas que tienen preferencia por el aislamiento motivado por la ausencia de aceptación en una determinada población, logrando encontrar cierto refugio en el entorno digital, donde pueden conectarse con comunidades y subculturas que comparten sus intereses. En lo que respecta a su relación con las autoridades, suelen adoptar una actitud crítica hacia el sistema económico y político. Es común que el ciberdelincuente vea a los investigadores como inferiores, principalmente por su escaso conocimiento técnico. b) Dimensión económica, los delincuentes cibernéticos provienen de diferentes niveles sociales o económicos. Anteriormente, el acceso a internet y a sistemas informáticos era exclusivo de las clases más favorecidas; sin embargo, hoy en día, a través de las redes sociales, cualquier persona, sin importar su nivel socioeconómico, puede acceder a estas plataformas. c) Dimensión familiar, en la gran mayoría de los casos se observa un grado mayor de desconexión o debilitamiento de un vínculo familiar, con padres sobreprotectores y ausentes, falta de atención, hechos de disfunción de la familia o metodologías de crianza deficientes (Cámara, 2020).

El perfil del delincuente cibernético se refiere a una descripción de las cualidades, motivaciones y comportamientos comunes de aquellos que participan en actividades ilícitas mediante el uso de tecnología. Comprender a fondo estas características en sus diversas facetas es de gran relevancia, especialmente en los últimos años, ya que estos criminales tienen acceso al ciberespacio de manera libre, especialmente en plataformas de juegos en línea que son muy

populares entre los jóvenes, lo que les facilita seleccionar a sus víctimas y llevar a cabo sus delitos con mayor facilidad. El perfil criminológico del hacker se refiere a personas que utilizan su inteligencia para realizar actividades ilegales, suelen tener una baja sociabilidad y tienden a actuar principalmente durante la noche. Prefieren moverse en entornos urbanos, suelen mostrar desdén por la burocracia, tienen un aspecto descuidado y suelen caracterizarse debido a su nivel de intensidad. Son individuos curiosos que poseen una capacidad notable en lo que respecta al abstracto pensamiento, interesados en lo novedoso y atraídos por lo intelectual. A veces pueden ser egocéntricos y rara vez se sienten satisfechos con sus conocimientos y acciones. Buscan constantemente lo nuevo y están dispuestos a pasar mucho tiempo navegando en internet sin preocuparse por la duración de su actividad (Carbajal, 2022).

2.1.15. Derecho comparado sobre delitos informáticos

2.1.15.1. España. se evidencian diversas normativas que abordan este tipo de comportamientos como: (a) Ley de Propiedad Intelectual, firma electrónica, propiedad intelectual, tlecomunicaciones; (b) Reglamento sobre medidas de seguridad para archivos automatizados que contengan datos personales y (c) Ley Orgánica de Protección de Datos Personales.

Ley de Servicios de la Sociedad de la Información y Comercio Electrónico. Además de estas regulaciones, el Código Penal de España, se incluye numerosas conductas ilegales vinculadas con actividades delictivas cibernéticas. Las mismas que suelen asemejarse a la clasificación sugerida por medio de tratados acerca de la Ciberdelincuencia, donde se evidencian artículos como:

Diversos delitos que suelen afectar la integridad, confidencialidad, así como la disponibilidad de sistemas de la informática e información, por otra marte mediante el art.197 se determinan sanciones para: Aquellos que, con el propósito de poner en descubierto secretos o invadir la privacidad de otra persona, se apoderen de documentos o efectos personales,

intercepten canales de comunicación o usen dispositivos para escuchar, transmitir, grabar o reproducir cualquier señal de comunicación (Recovery Labs, 2020).

2.1.15.2. Colombia. Los crímenes cibernéticos se refieren a acciones ilegales que ocurren en plataformas digitales, ambientes virtuales o en la web. En el contexto colombiano, se puede entender que estas actividades delictivas implican accesibilidad no permitida o ilegal a datos e información que se encuentran protegidos mediante la utilización de formatos digitales. Estas conductas están reguladas por la Ley 1273 de 2009:

- Daño informático, interceptar información, obstaculizar ilegítimamente cualquier red de telecomunicación, violar la información de carácter personal, utilizar programas maliciosos, suplantar páginas de internet con la finalidad de lograr recopilar información personal, hurtar utilizando mecanismos informáticos, transferirse activos.

Un aspecto relevante que contempla la legislación son las que se relacionan con la Agravación Punitiva, lo que implica que ciertas actividades delictivas perpetradas pueden resultar más serios de lo que aparentan. Por ejemplo, si se comete una actividad delictiva informática mediante en redes o sistemas que pertenecen al estado o a instituciones financieras, ya sean nacionales o internacionales, esto podrá considerarse como una agravante. Asimismo, si los delitos son perpetrados a través de funcionarios públicos cuando ejercen sus labores, si el delito tiene propósitos terroristas o pone en riesgo la seguridad del país, o incluso si la persona que administra una red de datos la utiliza para su propio beneficio en forma poco ética, esto podría resultar en una sanción de hasta 3 años de inhabilitación para poder trabajar con sistemas de información, etc. (World Legal Corporation, 2021)

2.1.16. Actos urgentes e inaplazables

Tomando en consideración el CPP se determina que las Diligencias Preliminares se fomentan como objetivo la ejecución de acciones inaplazables y acciones dados por el fiscal o

con la participación de los efectivos policiales, direccionado a la determinación en forma inmediata lo siguiente:

- Aseguramiento de diversidad de vestigios y residuos concerniente al hecho denunciado donde se adoptan las pertinentes medidas, razonables, adecuadas e indispensables para brindar protección y poder aislarlo reduciendo la posibilidad de que pueda ser destruida, desaparecida o contaminada con la finalidad de que se conserve un buen nivel de calidad probatoria (Poma, 2015)

2.1.17. Definición de términos básicos

- **Acción penal**. Dentro del escenario laboral y civil, las acciones podrán ser concebidas como un derecho concerniente a una concreta tutela jurisdiccional en los procedimientos penales, acciones que poseen una concreta particularidad, más bien representa un derecho atribuible al Ministerio Público, el mismo que posee el deber de que sea ejercido según lo determinado por el principio de legalidad (Montero, 1997).
- **Delito**. se considera una valoración concerniente al comportamiento de las personas condicionado a la perspectiva ética de la respectiva clase que ejerce dominio en la sociedad. (Machicado, 2010). Con acciones intencionales que perjudica al estatuto penal (Tappan, 2017).
- **Diligencias preliminares**. Poseen una particularidad investigativa pero no bajo una caracteristica de persecución, su objetivo es la obtencion de nociones claras del hecho punible presunto y la realizacion de la labor investigativa que una determinada fiscalía estima como pertinentes. Asimismo representa ser una sub fase de la labor investigativa preparatoria, por otra parte, se ejecutan las diversas diligencias que resulten ser inaplazables o urgentes direccionadas a la corroboración de los actos que se denuncian determinando el nivel de delictuosidad. (Neyra, 2010).

- **Flagrancia**. Está referido al hecho palpitante y vivo que convence a la persona que presencia una actividad delictiva (Hoyos, 2022).
- **Las Actas**. Es una documentación en donde consta la intervencion de los efectivos policiales con el objetivo de establecer las garantias relacionadas a la veracidad de la respectiva diligencia, tambien pueden ser elaboradas en la fiscalía (Arroyo, 2021)
- **Mandato de detención**. Involucra la restricción de la libertad individual, según los parametros señalados por la doctrina comparada, se establece que esta restricción deberá ser cumplida en un determinado plazo establecido por la constitución, durante el cual la autoridad correspondiente determina su situación legal. (Diaz, 2019).
- **Relación entre el Derecho Penal y las Nuevas Tecnologías de la Información**. Los avances tecnológicos, especialmente en el ámbito de las redes informáticas y la comunicación global, han propiciado la implementación de un estilo nuevo de Revolución Industrial. Esta transformación se fundamenta en la información y en la capacidad de almacenarla y compartirla sin restricciones de tiempo ni distancia. (Suarez, 2021). Estos desarrollos no solo han proporcionado a las personas una forma efectiva para que se reduzcan las distancias y llevar a cabo diversas transacciones globalmente, sino que también han facilitado a los delincuentes la posibilidad de operar sin contacto directo con sus víctimas, permitiéndoles causar daño sin que estas puedan identificar a sus agresores. (Posada, 2017).
- **Tecnología**. Es un enfoque que utiliza el conocimiento científico; más específicamente, se considera una tecnología cuando es compatible con la ciencia actual y puede ser controlada mediante la metodología científica, asimismo, la mencionada técnica generalmente se utiliza para gestionar y transformar tanto procesos naturales como sociales. La tecnología representa una unión entre el conocimiento teórico de la ciencia, orientado a la búsqueda de la verdad, y la práctica técnica, que se centra en la utilidad.

Así, el objetivo de la tecnología sería encontrar cierta veracidad que puede resultar ser de suma utilidad. Por lo tanto, se puede afirmar que la tecnología fomenta el mejoramiento de los procedimientos de comercio y el ciclo productivo. A lo largo del tiempo, las empresas han incorporado tecnología adaptada a sus necesidades y diseños, lo que les ha permitido satisfacer las demandas de sus clientes, y hoy en día, es posible aplicar tecnología de forma virtual (Bunge, 2020).

III MÉTODO

Un paradigma se define como un modelo o teoría que explica las realidades físicas. En el contexto de la investigación científica, el término "paradigma científico" se resaltó por medio de Kuhn (2019) para abordar toda modificatoria y revolución de la ciencia.

Karl Popper argumenta que las teorías pierden su validez cuando emergen nuevas teorías que las desafían, lo que propicia el progreso en la ciencia. En contraste, Thomas Kuhn plantea que las modificatorias de paradigma resulta ser calificado como el verdadero motor del desarrollo de la ciencia; esto significa que una nueva teoría no tiene que desacreditar a la anterior, sino que puede ofrecer una alternativa o un modelo diferente.

A criterio de Kuhn (2019), un paradigma representa un marco conceptual compartido por una comunidad científica, la misma que agrupa conocimientos de la ciencia, creencias, valores y principios con la finalidad de que la realidad pueda ser ampliamente comprendida. Durante un período determinado, este enfoque define los problemas y preguntas que se investigan, así como los métodos y técnicas empleados para encontrar soluciones. Cada paradigma tiende a reflejar una perspectiva única de los integrantes que conforman la comunidad de la ciencia, los mismos que percibirán el entorno real de una manera muy particular y establecen sus propios métodos y procedimientos para abordar los desafíos. Por lo tanto, los paradigmas ejercen una influencia normativa en la labor investigativa, guiando la forma en que los investigadores piensan, toman adecuadas decisiones y actúan. Al analizar los paradigmas, se busca comprender la experiencia y todo indicador que puede influir en el ámbito de los fenómenos de carácter social, reconociendo que la realidad se construye a través de las interacciones constantes entre los individuos y su entorno (Acosta, 2023).

Es importante señalar que, con respecto al paradigma positivista, tomando en cuenta lo establecido por Final y Vera (2020) señalaron que el enfoque positivista se sustenta en la aplicación de métodos hipotético-deductivos y, en algunos casos, inductivos. Este paradigma

sigue una secuencia lógica y estructurada, que comienza con la identificación del problema de investigación, seguido de una revisión exhaustiva de la literatura previa. Posteriormente, se seleccionan teorías relevantes, se formulan hipótesis precisas y se define el diseño de investigación, incluyendo la población objetivo, la muestra representativa, herramientas y diversidad de un riguroso procedimiento metodológico. Finalmente, los datos son analizados mediante la aplicación de diferentes técnicas estadísticas para extraer conclusiones significativas. En un sentido más amplio, el método se refiere a la estrategia empleada para alcanzar un objetivo específico, y en el contexto de la investigación, se convierte en la herramienta clave para comprender y reflejar la realidad objeto de estudio (Rodríguez y Pérez, 2017).

Según Rodríguez y Pérez (2017), el concepto de método investigativo presenta una doble acepción: por un lado, como enfoque general que guía la investigación, y por otro, como técnica específica utilizada en el proceso investigativo, como el método inductivo o deductivo. En este sentido, la metodología investigativa está más que todo referida a las diferentes alternativas estratégicas que la persona que realiza la investigación tiende a utilizar para que pueda interactuar con la meta sujeta al análisis, la variedad de métodos es amplia y depende en gran medida del objeto de investigación. Todas las metodologías brindan los aportes para una perspectiva única en la búsqueda y las acciones pertinentes para profundizar el conocimiento sobre la realidad, y presenta un enfoque particular para abordar el objeto de estudio, lo que da lugar a diferentes criterios de clasificación.

La labor investigativa es de enfoque cuantitativo según Valderrama y Jaimes (2019) en vista a que utiliza las acciones para recolectar y analizar la información para brindar la respuesta a la formulación de la problemática que es materia de estudio, tomando en cuenta a Hernández y Mendoza (2018) es conocido comunmente como ruta cuantitativa y resulta ser idonea en las estimaciones de las ocurrencias o magnitudes de los hechos para comprobar las

hipótesis, se aplicará la estadística descriptiva e inferencial, por otra parte, lo cuantitativo desde la perspectiva hipotética-deductiva brindará una serie de aportes a los procedimientos explicativos y el vínculo de causa y efecto (Herrera, 2018).

La presente labor investigativa se sitúa dentro del enfoque hipotético-deductivo, donde las hipótesis sirven como base para realizar nuevas deducciones. Se inicia con una hipótesis que puede derivarse de principios o leyes, o que es sugerida por datos empíricos. Al aplicar las normas de deducción, se generan predicciones que luego se someten a pruebas empíricas. Si estas predicciones coinciden con los hechos observados, se valida la hipótesis inicial. Inclusive si es que alguna hipótesis está sujeta a cierta predicción contradictoria y empírica, la conclusión será de suma importancia, y se demostrará cierta inconsistencia lógica concerniente a la hipótesis inicial y resultará primordial que se pueda reformular (Rodríguez y Pérez, 2017).

Por otra parte, se fomenta la búsqueda de acciones que permitan explicar los hechos analizados a través de los vínculos casuales (Rojas, 2021).

3.1 Tipo de investigación

Es aplicada basado en lo señalado por medio de Hernández et al. (2017), puesto que realiza interrogantes enfocados en la solución de la problemática específica en un lugar y tiempo, basándose en determinadas teorías que resultaron de la labor investigativa básica. Asimismo, la labor fue de nivel explicativo en vista que su finalidad es brindar las explicaciones del motivo por el cual sucede un hecho o acontecimiento, resaltando los motivos por los cuales sucedieron (Sànchez et al., 2023).

El trabajo fue de diseño no experimental según Valderrama (2019), resaltando que en lo relacionado a las variables independientes no son sujetos a manipulacion en vista que se encuentran dadas. Por otra parte, es de corte transversal, basándose en Arbaiza (2014), en vista a que se direccionan en la obtención de la informacion acerca de lo que ocurre en un instante determinado.

3.2 Población y muestra

3.2.1. Población

Se define como la agrupación de componentes que poseen particularidades que se estiman someter a estudio (Ventura, 2017). Fue representada por 58 encuestados entre fiscales, asistentes y abogados del Ministerio Público.

Tabla 1

Población de estudio

Detalle	Nº
Fiscales	8
Asistentes del Ministerio Público	12
Abogados del Ministerio Público	38
Totales	58

3.2.2. Muestra

Tomando en cuenta a Ramos (2011) se define como el subgrupo representativo que refleja a la población sujeta al análisis, se optó por los 58 entre fiscales, asistentes y abogados del Ministerio Público.

3.2.3 Muestreo

Fue catalogado como no probabilístico en vista que no se aplica formulación de carácter matemático para establecerla, en vista que se encuentra al alcance de la persona que realiza la investigación, por otra parte, se facilita la selección de casos particulares concernientes a una población donde se limitará la muestra únicamente a dichos casos. Es importante señalar que la muestra fue censal en vista que en la totalidad de unidades de análisis se tomaron en cuenta como muestra (Otzen y Manterola, 2017).

3.3 Operacionalización de variables

3.3.1. Definición conceptual de la variable independiente. Diligencias Preliminares

Las acciones iniciales de la labor investigativa suelen estar materializadas por medio de las diligencias preliminares; las cuales se entiende como una agrupación de acciones

progresivas de estudio, las mismas que adquieren forma según el grado de avance, estudio y análisis de los medios probatorios recogidos, las mismas que se adicionan a la labor investigativa (Cáceres, 2017).

3.3.2 Definición operativa de la variable independiente. Diligencias Preliminares

La variable diligencias preliminares se define operativamente tomando en consideración las dimensiones planteadas que son Interposición de la Denuncia, Diligencias que practicar y Plazo máximo.

Tabla 2

Operacionalización de la variable independiente. Diligencias Preliminares

Dimensiones	Indicadores
Interposición de la Denuncia	Ministerio Publico PNP
Diligencias que practicar	Fiscal Partes
Plazo máximo	60 días 120 días

3.3.3. Definición conceptual de la variable dependiente. Delitos informáticos

Según Luna (2020) representa una proporción de la ciencia concerniente al derecho penal encargado de estudiar las características o componentes que deberán concurrir en un comportamiento con la finalidad de que sea calificado como actividad delictiva.

3.3.4. Definición operativa de la variable dependiente. Delitos informáticos

La variable delitos contra informáticos se define operativamente tomando en cuenta las dimensiones planteadas que son acceso ilícito, fraude informático, suplantación de identidad.

Tabla 3

Operacionalización de la variable dependiente. Delitos informáticos

Dimensiones	Indicadores
Acceso Ilícito	Transferencias electrónicas fraudulentas Vishing
Fraude Informático	Clonación de tarjetas de crédito Ransomware:
Suplantación de identidad	Phishing Compras por internet mediante información de tarjetas de crédito o débito

3.4 Instrumentos

Fue el cuestionario, la misma que está definida como la agrupación de interrogantes que se elaboraron en base a diversas variables con la finalidad de que se genere la información y se alcancen las metas investigativas, por otra parte, deberá mantener cierta coherencia con la hipótesis y problemática (Hernández et al., 2018).

Según Martínez y Benítez (2016) define al cuestionario como un componente que facilita la obtención de información a través de formularios que toda persona podría realizar el llenado por sí mismas, en vista que se encuentra integrada a una agrupación de interrogantes en relación a las variables que se estiman someter a medición, posee 3 específicos objetivos:

- Traducción de los datos que se requieren a una agrupación de interrogantes específicas para que puedan ser debidamente contestadas por los diversos usuarios.
- Motivación y constante aliento a las personas que están siendo encuestadas, con la finalidad de asegurar su entera colaboración, cooperación y culmine de manera satisfactoria el cuestionario, razón por la cual, deberá fomentar la búsqueda de la minimización de la fatiga y el tedio.
- Minimización de errores de respuesta, en las cuales se adaptan interrogantes a la persona informante y bajo una escala o formato donde no confunda al usuario.

3.5 Procedimientos

Según Bernal (2016), se resalta la importancia de la estadística la cual deberá aplicarse para asegurar la verificación o realización de la prueba de hipótesis. Se plantean una serie de pasos para su realización:

- Formulación de las hipótesis, sea alterna o nula según la labor investigativa.
- Elección de pruebas de carácter estadístico relacionado con las diversas variables sujetas al análisis.

- Seleccionar el nivel de significancia mediante un tipo de porcentaje para aprobar o refutar una hipótesis, por ejemplo: 0,01; 0,05 o 0,10.
- Recolectar información concerniente a la muestra selecciona para la investigación.
- Estimación de la desviación estándar.
- Conversión de la media concerniente a la muestra mediante valores z o t.
- Elección de decisiones de carácter estadístico a través de los cálculos del valor de z o t crítico (significancia).
- Establecer una serie de conclusiones.

3.6 Análisis de datos

En el análisis de la información se compone de los parámetros de la estadística inferencial y descriptiva, a continuación, se explica la estadística descriptiva de la presente investigación:

Estadística descriptiva: se establece la descripción de las particularidades básicas de la información bajo análisis, brindando simples resúmenes concernientes a la muestra y toda medición que se ha realizado, desde un inicio se muestra información acerca de las frecuencias vinculadas a variables que interesan en la labor de análisis para que sean representadas por medio de un histograma (Herbas y Rocha, 2018).

Asimismo, se ejecuta la regresión logística ordinal con la finalidad de que la hipótesis pueda ser contrastada para establecer el grado de dependencia con respecto a las variables. (Sànchez et al., 2023).

Por otra parte, se define a la regresión logística ordinal como una herramienta que facilita el estudio de la incidencia e influencia concernientes a las variables categoricas y cualitativas, tambien fomenta la factibilidad de que se evalue el grado en el cual una variable independiente influye en la dependiente, con la finalidad de lograr lo mencionado se procederá a emplear los parámetros del coeficiente de Nagelkerke.

El R^2 de Nagelkerke se define como una modificación del R2 de Cox y Snell, el cual brinda la corrección de las escalas de la estadística para que se cubra completamente el rango desde 0 a 1, asimismo, si es que se da el caso que el R2 de Cox y Snell que se ha proyectado resulte equivalente a 0,021 implica que la variable independiente utilizada brinda la explicación del 2,1 % de la varianza de la variable dependiente (Sànchez et al., 2023).

3.7 Consideraciones éticas

- La labor investigativa se ejecuta en base a lo señalado por la Universidad Nacional Federico Villareal y a la Asociación Americana de Psicología (APA).
- En la presente labor investigativa se fomenta el debido respeto de toda teoría y concepto a través de las diversas referencias bibliográficas.
- Para elaborar la data se fomenta el debido respeto a toda opinión de las personas encuestadas.

IV. RESULTADOS

4.1 Análisis descriptivo

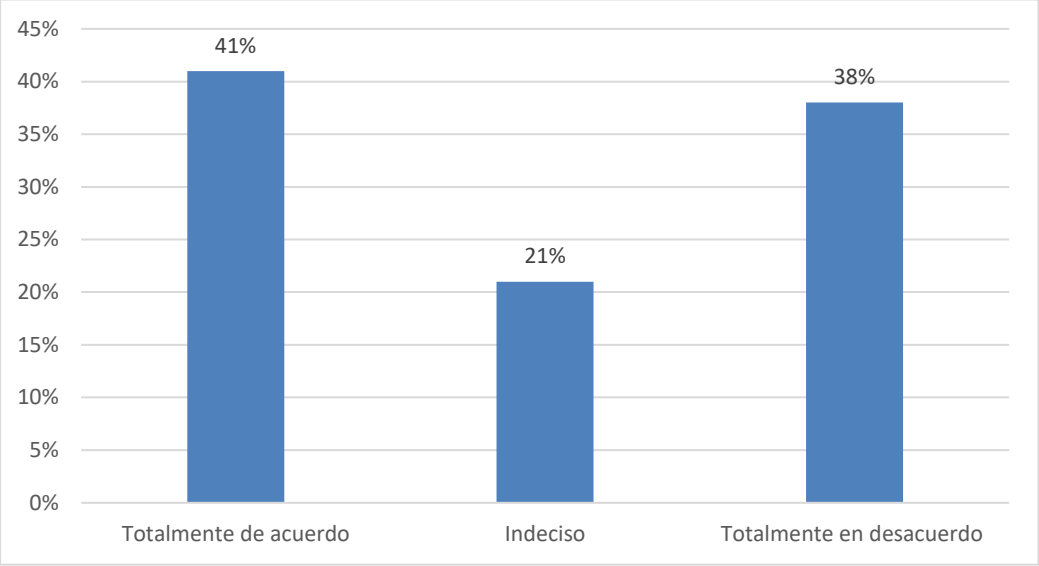
Tabla 4

Frecuencia de la variable independiente. Diligencias preliminares

		Frecuencia	Porcentaje
Válido	Totalmente de acuerdo	24	41
	Indeciso	12	21
	Totalmente en desacuerdo	22	38
	Total	58	100

Figura 1

Histograma de la variable independiente. Diligencias preliminares



Nota. El 41% está "totalmente de acuerdo" con su eficacia en la recolección de pruebas, mientras que el 38% "totalmente en desacuerdo" refleja una percepción negativa significativa. Además, el 21% de los participantes se muestra "indeciso", lo que sugiere que hay preocupaciones o experiencias mixtas respecto a su implementación. Esta distribución indica que, aunque hay un apoyo notable a la efectividad de las diligencias preliminares, también existen dudas que merecen ser exploradas para mejorar su impacto en la labor investigativa y resolución de delitos informáticos.

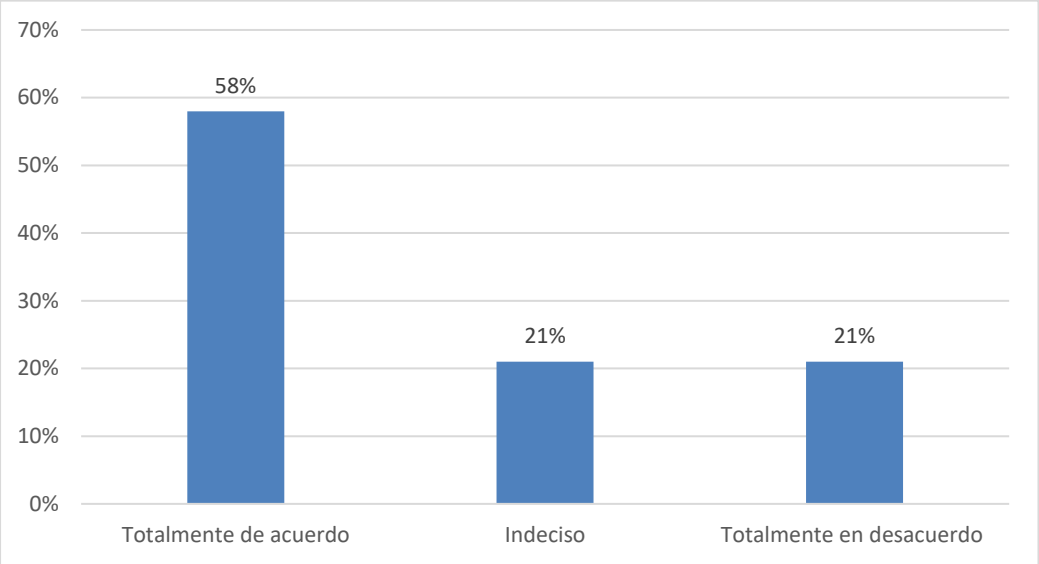
Tabla 5

Frecuencia de la dimensión. Investigativa

		Frecuencia	Porcentaje
Válido	Totalmente de acuerdo	34	58
	Indeciso	12	21
	En desacuerdo	12	21
	Total	58	100

Figura 2

Histograma de la dimensión. Investigativa



Nota. La tabla muestra que el 58% de los encuestados está totalmente de acuerdo en que las denuncias por delitos informáticos se interponen oportunamente, mientras que el 21% se muestra indeciso y otro 21% en desacuerdo. Esto evidencia una percepción mayoritaria positiva respecto a la pronta interposición de denuncias, aunque persisten dudas y críticas sobre aspectos como la inmediatez de la denuncia, la capacidad de respuesta de las comisarías, la suficiencia de personal y la rapidez para informar al Ministerio Público.

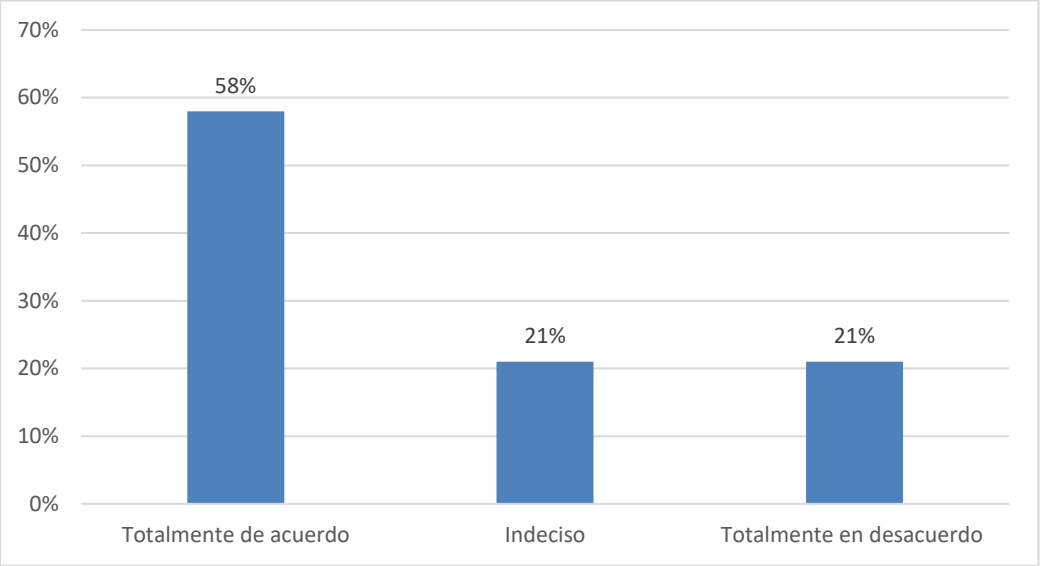
Tabla 6

Frecuencia de la dimensión. Preventiva

		Frecuencia	Porcentaje
Válido	Totalmente de acuerdo	34	58
	Indeciso	12	21
	En desacuerdo	12	21
	Total	58	100

Figura 3

Histograma de la dimensión. Preventiva



Nota. La tabla revela que el 58% de los encuestados está totalmente de acuerdo con la necesidad de realizar diligencias preliminares oportunas y especializadas en casos de delitos informáticos, mientras que un 21% se mantiene indeciso y otro 21% está en desacuerdo. Esto indica que una mayoría reconoce la importancia de actuar rápidamente, capacitar al personal en ciberseguridad y contar con expertos tecnológicos para evitar la pérdida de evidencia, aunque existe un sector que aún duda o no percibe la urgencia de estas acciones especializadas.

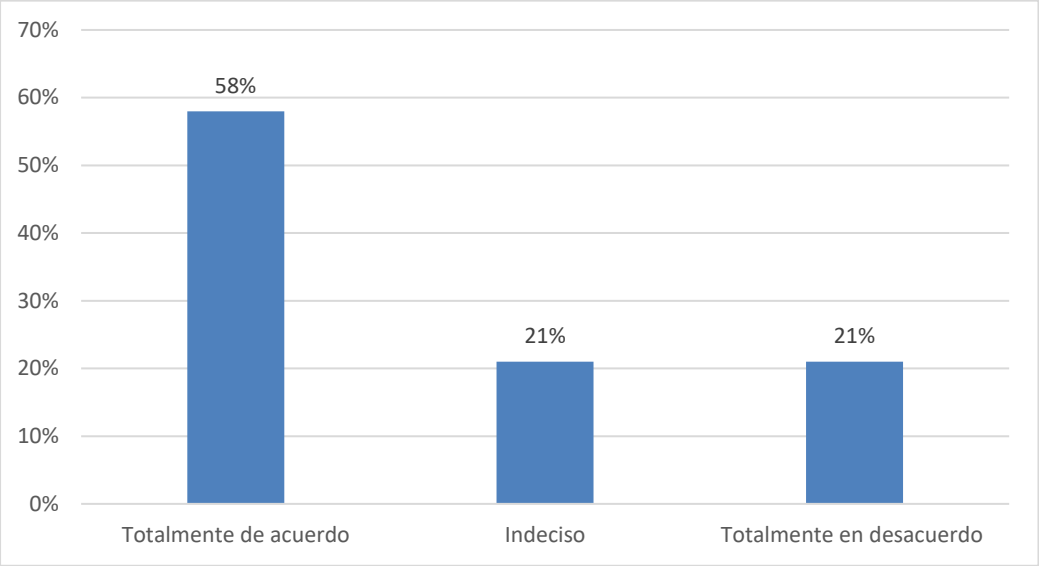
Tabla 7

Frecuencia de la dimensión. Resolutiva

		Frecuencia	Porcentaje
Válido	Totalmente de acuerdo	12	21
	Indeciso	34	58
	En desacuerdo	12	21
	Total	58	100

Figura 4

Histograma de la dimensión. Resolutiva



Nota. La tabla muestra que solo el 21% de los encuestados está totalmente de acuerdo con la necesidad de modificar los plazos para las diligencias preliminares en delitos informáticos, mientras que la mayoría (58%) se mantiene indecisa y un 21% está en desacuerdo. Esta tendencia refleja incertidumbre respecto a si los plazos actuales contribuyen a la impunidad o dificultan la obtención de pruebas, lo que sugiere la necesidad de mayor información o debate sobre la urgencia y efectividad de acortar los plazos procesales en estos delitos.

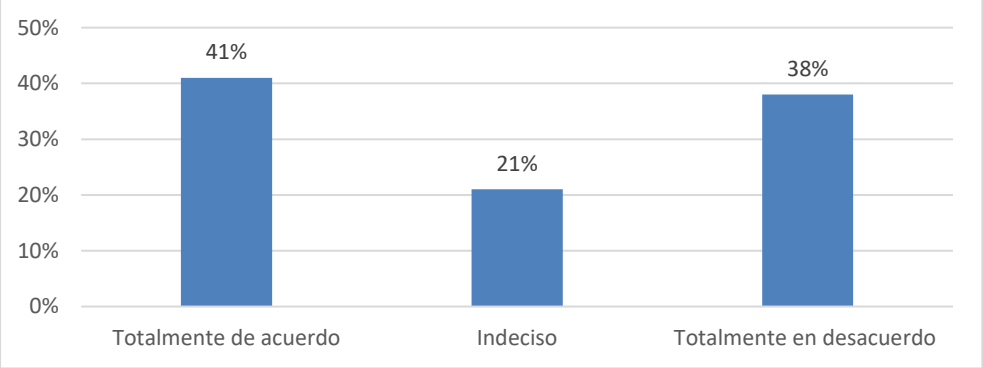
Tabla 8

Frecuencia de la variable dependiente. Delitos informáticos

		Frecuencia	Porcentaje
Válido	Totalmente de acuerdo	24	41
	Indeciso	12	21
	Totalmente en desacuerdo	22	38
	Total	58	100

Figura 5

Histograma de la variable dependiente. Delitos informáticos



Nota. El 41% está "totalmente de acuerdo" en que las diligencias preliminares influyen positivamente en la resolución de delitos informáticos, mientras que un 38% "totalmente en desacuerdo" muestra una percepción negativa. Además, el 21% se muestra "indeciso", lo que indica una falta de claridad en su opinión sobre la efectividad de las diligencias. Este panorama resalta que, a pesar de que una parte considerable de las personas encuestadas reconoce el valor de las diversas diligencias preliminares, existe una división significativa en la percepción general sobre su impacto en la resolución de delitos como el acceso ilícito, fraude informático y suplantación de identidad. La diversidad de opiniones sugiere la necesidad de explorar más a fondo las experiencias de los encuestados con estos delitos y la efectividad de las diligencias realizadas para abordar sus preocupaciones.

4.2 Contrastación de hipótesis

4.2.1 Contrastación de la hipótesis general

Ha. Las diligencias preliminares influyen positivamente en los delitos informáticos en el Cercado de Lima, año 2024.

Ho. Las diligencias preliminares no influyen positivamente en los delitos informáticos en el Cercado de Lima, año 2024.

Tabla 9

Contrastación de la hipótesis general

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo interceptación	44,107			
Final	,000	44,107	3	,000

Nota. Se tiene un valor de significancia (Sig.) equivalente a 0.000, señalando una significancia alta a nivel estadístico. Dado que este valor es mucho menor que el umbral común de 0.05, procediendo al rechazo de la hipótesis nula (Ho). Por lo tanto, se concluye que las diligencias preliminares efectivamente tienen un impacto positivo en la investigación y resolución de delitos informáticos en el Cercado de Lima.

Tabla 10

Pseudo R cuadrado

Cox y Snell	,795
Nagelkerke	,791
McFadden	,616

Nota. Se evidencia un Nagelkerke de 0.791 que resalta que el modelo de regresión logística brinda una explicación de que aproximadamente el 79.1% de la variabilidad en la variable dependiente. Este alto porcentaje implica que las diligencias preliminares tienen un impacto significativo en la explicación de las actividades delictivas vinculados a la informática en el Cercado de Lima.

4.2.2. Contrastación de la hipótesis especifica 1

Ha. La dimensión investigativa influye positivamente en los delitos informáticos en el Cercado de Lima, año 2024.

Ho. La dimensión investigativa no influye positivamente en los delitos informáticos en el Cercado de Lima, año 2024.

Tabla 11

Contrastación de la primera hipótesis específica

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo interceptación	26,170			
Final	4,492	25,138	1	,000

Nota. Se tiene un valor de significancia (Sig.) de 0.000. Dado que este valor es significativamente menor que el umbral de 0.05, se rechaza la hipótesis nula (Ho), que sostiene que la dimensión investigativa no influye positivamente en los delitos informáticos. Esto indica que hay evidencia suficiente para aceptar la hipótesis alternativa (Ha), sugiriendo que la dimensión investigativa efectivamente tiene un impacto positivo en la resolución de delitos informáticos en la región estudiada.

4.2.3. Contrastación de la hipótesis especifica 2

Ha. La dimensión preventiva influye positivamente en los delitos informáticos en el Cercado de Lima, año 2024.

Ho. La dimensión preventiva no influye positivamente en los delitos informáticos en el Cercado de Lima, año 2024.

Tabla 12 *Contrastación de la segunda hipótesis específica*

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo interceptación	37,458			
Final	,000	37,449	3	,000

Nota. Se tiene un valor de significancia (Sig.) de 0.000. Dado que este valor es significativamente menor que el umbral de 0.05, se rechaza la hipótesis nula (Ho), que sostiene que la dimensión preventiva no influye positivamente en los delitos informáticos. Por lo tanto, hay evidencia suficiente para aceptar la hipótesis alternativa (Ha), lo que sugiere que la dimensión preventiva efectivamente tiene un impacto positivo en la reducción y manejo de los delitos informáticos en la región estudiada.

4.2.4. Contrastación de la hipótesis especifica 3

Ha. La dimensión resolutiva influye positivamente en los delitos informáticos en el Cercado de Lima, año 2024.

Ho. La dimensión resolutiva no influye positivamente en los delitos informáticos en el Cercado de Lima, año 2024.

Tabla 13 *Contrastación de la tercera hipótesis específica*

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo interceptación	38,256			
Final	,000	38, 253	3	,000

Nota. Se tiene un valor de significancia (Sig.) de 0.000. Dado que este valor es significativamente menor que el umbral de 0.05, se rechaza la hipótesis nula (Ho), que afirma que la dimensión resolutiva no influye positivamente en los delitos informáticos. Así, hay evidencia suficiente para aceptar la hipótesis alternativa (Ha), indicando que la dimensión resolutiva efectivamente tiene un impacto positivo en la investigación y resolución de delitos informáticos en la región estudiada.

V. DISCUSIÓN DE RESULTADOS

La diversidad de resultados que se han logrado obtener ofrecen un marco interesante para la discusión a través de diversas teorías generales del derecho y criminología.

Desde el enfoque teórico del sistema inquisitivo, se puede argumentar que la fase de diligencias preliminares actúa como una herramienta fundamental para buscar la veracidad material, permitiendo que un determinado juez acumule pruebas de forma activa. Sin embargo, este enfoque puede chocar con la necesidad de salvaguardar los derechos del imputado, lo que lleva a considerar el sistema acusatorio, donde el rol del fiscal es más protagónico y se enfatiza la importancia de las pruebas obtenidas de manera legal y justa. En este contexto, los resultados sugieren que una adecuada ejecución de las diligencias preliminares puede garantizar una base sólida para la acusación, fortaleciendo el debido proceso.

El sistema mixto, que combina elementos de ambos enfoques, refleja la necesidad de un equilibrio entre la efectividad en la recolección de pruebas y acciones para proteger los fundamentales derechos. Los resultados apuntan a que, con respecto al ámbito de las diligencias preliminares, cuando se realizan de manera estructurada y conforme a los principios del debido proceso, favorecen una resolución más justa en los delitos informáticos, minimizando el riesgo de abusos.

Es importante señalar los parámetros señalados por la teoría del principio de indubio pro reo vs. pro societatis también resulta pertinente en esta discusión. Los hallazgos revelan que las diligencias preliminares no solo deben centrarse en la recolección de pruebas que favorezcan a la acusación, sino también en garantizar que la investigación no vulnera los derechos del imputado. La correcta aplicación de estas diligencias puede ser vista como una herramienta para satisfacer los intereses de la población en asuntos relacionados con la seguridad, sin sacrificar los derechos individuales, contribuyendo así a un enfoque más equilibrado en la lucha contra la criminalidad digital.

La teoría sobre la cibercriminología proporciona un contexto crucial para entender cómo las diligencias preliminares impactan en la dinámica de los delitos informáticos. Los resultados sugieren que una respuesta efectiva a la cibercriminalidad requiere no solo de una adecuada recolección de pruebas, sino también de la continua capacitación de las personas encargadas de operar la justicia en tecnologías emergentes y métodos de investigación específicos, destacando la importancia de una respuesta adaptativa a la cambiante naturaleza de las actividades delictivas ligadas a la informática.

Finalmente, la teoría de la transición espacial es relevante para comprender cómo las diligencias preliminares pueden influir en la dinámica de la criminalidad en el entorno digital. La investigación muestra que una adecuada respuesta a los delitos informáticos puede disuadir a los delincuentes, lo que a su vez podría llevar a una reducción de la criminalidad en el espacio digital. Esto resalta la necesidad de que las autoridades no solo se enfoquen en la resolución de delitos ya ocurridos, sino también en la prevención, utilizando las diligencias preliminares como un instrumento proactivo.

Asimismo, el resultado de la labor investigativa deja en claro que las diligencias preliminares son una pieza clave en el entramado de los mecanismos penales de justicia frente a los delitos informáticos, y su adecuada implementación, alineada con las teorías discutidas, puede contribuir a una mejor respuesta judicial y social ante esta creciente problemática.

Sobre la primera discusión, los resultados de la labor investigativa sobre la influencia del ámbito de toda diligencia preliminar en los delitos informáticos en el Cercado de Lima muestran una percepción mixta entre los participantes: un 41% se declara "totalmente de acuerdo" con la eficacia de estas diligencias en la recolección de pruebas, asimismo, 38% evidencia sentirse "totalmente en desacuerdo". Este contraste sugiere que, aunque existe un reconocimiento significativo de su utilidad, persisten dudas y experiencias negativas que deben ser atendidas para maximizar su efectividad. La presencia de un 21% de "indecisos" indica que

hay espacio para la mejora, probablemente reflejando preocupaciones sobre la implementación o la calidad de estas diligencias en la práctica.

El valor de significancia (Sig.) de 0.000 refuerza la conclusión de que las diligencias preliminares tienen un impacto positivo en la labor investigativa y resolución de los ciberdelitos, desestimando de esta manera la hipótesis nula. Además, el coeficiente de Nagelkerke de 0.791 sugiere que la regresión logística señala un 79.1% de la variabilidad de los delitos informáticos, indicando un ajuste robusto del modelo y la relevancia de las diligencias preliminares en este contexto.

Al comparar estos hallazgos con las teorías de Beermann (2024), que argumenta la necesidad de un enfoque dinámico y evolutivo en la ciberdelincuencia, es evidente que las diligencias preliminares deben adaptarse continuamente a las transformaciones tecnológicas y los métodos delictivos emergentes. Asimismo, las investigaciones de Alcalá y Meléndez (2023) resaltan la relevancia de la tipificación clara de las actividades delictivas informáticas, sugiriendo que una adecuada clasificación y sanción puede facilitar la denuncia y la investigación.

Por otra parte, los estudios de Arapa et al. (2024) y Cantorin (2024) subrayan el impacto de factores sociales y tecnológicos en el aumento de los delitos informáticos, lo que implica que las diligencias preliminares deben ser complementadas con programas de educación y concienciación que fortalezcan la seguridad cibernética y reduzcan la vulnerabilidad de la población.

Sobre la segunda discusión, los resultados obtenidos indican que un 58% de las personas encuestadas toman en cuenta que en lo que respecta a diligencias preliminares son efectivas en la recolección de pruebas y en la resolución de delitos informáticos. Sin embargo, la presencia de un 21% de indecisos y un 21% en desacuerdo revela una división significativa en las percepciones sobre la eficacia de estas diligencias. Esto sugiere que, a pesar de la mayoría

que reconoce su importancia, existe un número considerable de personas que tiene dudas o experiencias negativas, lo que resalta la necesidad de realizar investigaciones más profundas para abordar estas inquietudes y mejorar la implementación de las diligencias.

El valor de significancia (Sig.) de 0.000 respalda la afirmación de que la interposición de la denuncia influye positivamente en los delitos informáticos en el Cercado de Lima, año 2024. Este hallazgo se alinea con las conclusiones de Díaz et al. (2023), quienes resaltan la relevancia de la capacitación y fomentar conciencia entre los actores sociales para abordar eficazmente los delitos cibernéticos, lo que podría contribuir a disminuir la percepción negativa de las diligencias preliminares.

Asimismo, las afirmaciones de Quevedo (2017) refuerzan la idea de que el avance tecnológico ha transformado la criminalidad, creando nuevos desafíos para la persecución e investigación de acciones delictivas. La capacidad del Estado para investigar eficazmente los delitos informáticos debe equilibrarse protegiendo el ámbito de los fundamentales derechos, como indica Pérez (2021), sugiriendo que la secreta naturaleza concerniente a las diligencias preliminares podría comprometer todo el entorno del derecho de defensa, un aspecto crítico en los procedimientos penales.

Por último, Poma (2020) destaca los problemas asociados a la investigación preliminar, como la duración y la protección de los fundamentales derechos, lo que refuerza la necesidad de un marco normativo que garantice tanto los niveles de eficacia relacionada con las diligencias preliminares como la protección de los derechos de los imputados.

Sobre la tercera discusión, la información evidencia que un 58% de las personas encuestadas considera que las diligencias preliminares son efectivas para la conservación de pruebas y la prevención de la pérdida de datos críticos en casos de delitos informáticos. Sin embargo, el hecho de que un 21% se muestre "indeciso" y otro 21% "en desacuerdo" sugiere una percepción dividida y la existencia de preocupaciones significativas sobre la efectividad

de estas medidas. Esto pone de manifiesto que, a pesar del respaldo mayoritario, es esencial investigar más a fondo las razones detrás de estas dudas para optimizar la implementación de las diligencias y maximizar su eficacia.

La significancia estadística (Sig.) de 0.000 refuerza la afirmación de que las diligencias que practicar influye positivamente en los delitos informáticos en el Cercado de Lima, año 2024. Este hallazgo se alinea con la visión de Santana (2018), quien enfatiza la relevancia de la educación para que se configure la privacidad de las redes sociales, destacando que la ausencia de conocimiento sobre la protección de los datos personales puede facilitar la ciberdelincuencia.

Por otro lado, Tenorio (2018) señala que el crecimiento de la ciberdelincuencia a nivel internacional requiere de una legislación dinámica y efectiva. A pesar de los esfuerzos realizados en el Perú, como la adiciono del ciberdelito en el Código Penal, aún se enfrenta al desafío de una respuesta rápida ante delitos cometidos desde fuera del país. Este contexto resalta la necesidad de fortalecer la colaboración internacional y la competencia de los encargados de operar justicia en el uso de tecnologías para la protección de la evidencia.

Finalmente, De la Puente (2020) pone de manifiesto que la lucha contra el ciberdelito implica no solo la definición de tipos penales, sino también la creación de un marco normativo que contemple la privacidad y las libertades comunicativas. Este equilibrio es fundamental para asegurar que las diligencias preliminares no solo sean efectivas en la conservación de pruebas, sino que también respeten los derechos fundamentales de los individuos.

Sobre la cuarta discusión, el resultado señala que solo el 21% de los encuestados se encuentran "totalmente de acuerdo" en que las diligencias preliminares facilitan la resolución de casos y mejoran la rapidez de las respuestas en los delitos informáticos. Esta cifra es alarmantemente baja, especialmente considerando que el 58% se muestra "indeciso", lo que refleja una falta de confianza y claridad sobre la efectividad de estas diligencias en el proceso

resolutivo. Además, el 21% que se encuentra "en desacuerdo" sugiere una percepción negativa o escepticismo respecto a su capacidad para influir positivamente en la resolución de delitos, un hallazgo que subraya la necesidad urgente de investigar las causas subyacentes de esta indecisión y desacuerdo.

La significancia estadística (Sig.) de 0.000 refuerza la decisión de que se rechace lo señalado por la hipótesis nula, proporcionando evidencia suficiente para aceptar que el plazo máximo influye positivamente en los delitos informáticos en el Cercado de Lima, año 2024.

Ruiz (2016) señala que la dificultad para identificar a los causantes de actividades delictivas ligadas a la informática contribuye a la impunidad, erosionando la confianza en la justicia. Esta percepción se refleja en los resultados, donde un porcentaje significativo de encuestados duda de la efectividad de las diligencias para resolver casos. Reyes (2020) complementa esta perspectiva al señalar que los delitos informáticos no solo afectan a los sistemas, sino que también tienen un impacto profundo en la integridad personal de las víctimas, quienes pueden sufrir consecuencias psicológicas, morales y físicas. Esta vulnerabilidad, especialmente en grupos como adolescentes y niños, hace aún más relevante el diseño y la implementación efectivas de diligencias preliminares que realmente aborden las necesidades de protección de estas poblaciones.

VI CONCLUSIONES

- La evaluación de las diligencias preliminares en los delitos informáticos en el Cercado de Lima durante el año 2024 revela que estas diligencias tienen una influencia significativa y positiva en la recolección de pruebas, la conservación de información crucial y la resolución de casos, lo que resalta su papel fundamental en la mejora de la efectividad de las investigaciones y en la prevención de futuros delitos informáticos. Esto sugiere que optimizar los procedimientos y enfoques utilizados en las diligencias preliminares podría resultar en una respuesta más eficiente ante este tipo de delitos, fortaleciendo así la seguridad digital en la región.
- La investigación revela que la dimensión investigativa de las diligencias preliminares desempeña un papel crucial en la efectividad de la respuesta a los delitos informáticos en el Cercado de Lima durante el año 2024, al facilitar la recolección y análisis de pruebas relevantes, lo que a su vez contribuye a una mejor resolución de los casos. Este hallazgo subraya la importancia de fortalecer las capacidades investigativas en el ámbito digital, lo que no solo mejora la identificación y procesamiento de los infractores, sino que también incrementa la confianza pública en el sistema de justicia frente a los delitos informáticos.
- La evaluación de la dimensión preventiva de las diligencias preliminares en los delitos informáticos en el Cercado de Lima durante el año 2024 indica que estas medidas son efectivas para reducir la incidencia de tales delitos, al facilitar la conservación de pruebas y la implementación de medidas cautelares que previenen la reofensiva. Este hallazgo resalta la necesidad de priorizar estrategias preventivas en el ámbito de la seguridad digital, lo que no solo contribuye a la protección de los ciudadanos, sino que también fortalece la capacidad del sistema judicial para actuar de manera proactiva frente a las amenazas cibernéticas.

- La explicación de la dimensión resolutiva de las diligencias preliminares en los delitos informáticos en el Cercado de Lima durante el año 2024 revela que estas diligencias son fundamentales para acelerar la resolución de casos, al facilitar procesos extrajudiciales y mejorar la coordinación entre las autoridades competentes. Este impacto positivo no solo contribuye a una respuesta más rápida ante los delitos informáticos, sino que también fortalece la confianza de la ciudadanía en el sistema de justicia, destacando la necesidad de implementar prácticas eficientes que optimicen la resolución de estos delitos en un contexto cada vez más digital.

VII. RECOMENDACIONES

- Se recomienda fortalecer la especialización y capacitación de los diversos operadores de justicia en el manejo de diligencias preliminares relacionadas con delitos informáticos, implementando programas de formación continua que aborden las particularidades del entorno digital y las mejores prácticas en la recolección y preservación de pruebas. Esto no solo mejorará la efectividad de las investigaciones, sino que también permitirá una respuesta más ágil y adecuada ante los desafíos que presentan los delitos informáticos, contribuyendo así a una mayor seguridad y confianza en el sistema judicial en el Cercado de Lima.
- Se recomienda fortalecer la capacidad operativa de las comisarías del Cercado de Lima mediante la implementación de módulos especializados en delitos informáticos, con personal capacitado y canales digitales de denuncia que permitan una atención rápida, segura y eficiente.
- Se recomienda implementar programas permanentes de capacitación en informática forense y ciberseguridad para el personal policial y fiscal encargado de diligencias preliminares, asegurando así intervenciones técnicas que garanticen la conservación de evidencias digitales.
- Se recomienda revisar y reformar la normativa vigente para establecer plazos más breves y específicos en la investigación de delitos informáticos, adaptando el marco legal a la urgencia que requiere la preservación de evidencias digitales y la acción penal oportuna.

VIII. REFERENCIAS

Acosta, S. (2023). *Los paradigmas de investigación en las Ciencias Sociales*. Editorial Idicap Pacífico. https://doi.org/10.53595/eip.007.2023.ch.4.

Acurio, S. (2016). *Delitos Informáticos: Generalidades.* El Buho.

Alcalá, M., y Meléndez, M. (2023). Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas. *PAAKAT: Revista de Tecnología y Sociedad, 13(24)*, 1-37. https://dialnet.unirioja.es/servlet/articulo?codigo=8956682.

Álvarez, C. (2023). *Colombia registró un crecimiento de ataques informáticos en el ultimo año*. https://www.vozdeamerica.com/a/colombia-registro-crecimiento-ataques-informaticos-ultimo-ano-/6916577.html#:~:text=Colombia%20registr%C3%B3%20en%202022%20m%C3%A1s,computadoras%2C%20tablets%20y%20tel%C3%A9fonos%20celulares

Arapa, J., Cari, K., y Lipe, J. (2024). Causas y consecuencias del incremento de los delitos informáticos en la ciudad de Puno 2023. *Revista de Derecho, 9(1)*, 1-13. https://www.redalyc.org/journal/6718/671876168004/.

Arbaiza, L. (2014). *Como elaborar una tesis de grado.* Esan Editores.

Arroyo, A. (2021). *Diligencias preliminares – formulación de actas*. [Tesis de grado, Universidad Peruana de las Amèricas]. http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/1944/TRABAJO%20WORD.pdf?sequence=1&isAllowed=y.

Banco Interamericana de Desarrollo [BID]. (2020). *Estado de la Ciberseguridad en América Latina y El Caribe*. https://blog.segu-info.com.ar/2020/12/estado-de-la-ciberseguridad-en-america.html

Barrado, R. (2018). *Teoría del delito. Evolución, elementos integrantes.* https://ficp.es/wp-content/uploads/2019/03/Barrado-Castillo.-Comunicaci%C3%B3n.pdf

Beermann, H. (2024). La ciberdelincuencia en Panamá y el convenio de Budapest de 2001. *Boletin de ciencias penales, 21*, 77-97. https://facderecho.up.ac.pa/sites/facderecho/files/2023-12/BOLET%C3%8DN%20DE%20CIENCIAS%20%20PENALES%20No%2021%20enero-julio%202024%20COMPLETO.pdf#page=78.

Bernal, C. (2016). *Metodologia de la investigacion.* Pearson.

Biblioteca del Congreso Nacional de Chile. (2023). *Ley 19696*. https://www.bcn.cl/leychile/navegar?idNorma=176595

Bunge, M. (2020). *La ciencia. Su método y su filosofía.* https://posgrado.unam.mx/musica/lecturas/LecturaIntroduccionInvestigacionMusical/epistemologia/Mario-Bunge-la-Ciencia-su-Metodo-y-Filosofia.pdf

Cáceres, R. (2017). *La prueba indiciaria en el proceso penal.* Instituto Pacífico.

Cámara, S. (2020). Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. *Derecho y Cambio Social, 60*, 470-512. https://dialnet.unirioja.es/descarga/articulo/7524987.pdf.

Cantorin, V. (2024). *Perfil del ciberdelincuente en el delito informático de grooming, Lima 2023*. [Tesis de maestría, Universidad Cesar Vallejo]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/133221/Cantorin_AVH-SD.pdf?sequence=1&isAllowed=y.

Carbajal, M. (2022). *Las fiscalías especializadas en delitos informáticos como mecanismo para la lucha contra el cibercrimen*. [Tesis de maestría, Universidad de San Martin de Porres]. https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/11398/carbajal_cm.pdf?sequence=1&isAllowed=y.

Choi, S., Back, S., y Toro-Alvarez, M. (2023). *Digital Forensics and Cyber Investigation.* https://www.researchgate.net/profile/Kyung-Shick-Choi/publication/364302361_Digital_Forensics_and_Cyber_Investigation/links/63443bdf9cb4fe44f3199e6b/Digital-Forensics-and-Cyber-Investigation.pdf

Código de Procedimiento Penal de Colombia. (2004). *Ley 906.* https://perso.unifr.ch/derechopenal/assets/files/legislacion/l_20190708_03.pdf

De la Puente, J. (2020). *La interceptación y difusión de las comunicaciones privadas y las libertades comunicativas en el proceso de judicialización peruano. Ponderación, límites e interés público*. [Tesis de maestría, Universidad Nacional Mayor de San Marcos]. https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/15611/DelaPuente_mj.pdf?sequence=1&isAllowed=y.

Defensoría del Pueblo. (2023). *La ciberdelincuencia en el Perú: Estrategias y retos del estado*. https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Diario Gestion. (08 de agosto de 2020). *Fraudes en línea se disparan este año en Perú ante mayor uso de Internet.* https://gestion.pe/peru/fraudes-en-linea-se-disparan-este-ano-en-peru-ante-mayor-uso-de-internet-noticia/

Diaz, C. (2019). *Ampliación del plazo de detención en flagrancia delictiva y el test de proporcionalidad en el tribunal constitucional e instrumentos internacionales*. [Tesis de maestria, Universidad Privada Antenor Orrego]. https://repositorio.upao.edu.pe/bitstream/20.500.12759/6625/1/rep_dere_cinthya.diaz_ampliaci%c3%93n.plazo.detenci%c3%93n.flagrancia.delictiva.test.proporcionalidad.tribunal.constitucional.instrumentos.internacionales.pd.

Diaz, I., Ojeda, P., Cajas, C., y Cabrera, E. (2023). Desafíos legales en Ecuador frente a los delitos informáticos, importancia de su prevención. *Universidad Y Sociedad, 15(6)*, 746-754. https://rus.ucf.edu.cu/index.php/rus/article/view/4195/4102.

El mostrador. (2021). *Delitos informáticos en Chile han aumentado en 60% tras inicio de la crisis sanitaria.* https://www.elmostrador.cl/agenda-pais/2020/10/14/delitos-informaticos-en-chile-han-aumentado-en-60-tras-inicio-de-la-crisis-sanitaria/#:~:text=Seg%C3%BAn%20cifras%20de%20NovaRed%2C%20expertos,del%20tipo%20ransomware%20en%20210%25.

El Peruano. (2023). *¡Cuidado con los fraudes informáticos! Estas son las modalidades más denunciadas en Perú*. https://www.elperuano.pe/noticia/216043-cuidado-con-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-en-peru#:~:text=21%2F06%2F2023%20Cada%20mes,de%20la%20mitad%20del%20total

Finol, M., y Vera, J. (2020). Paradigmas, enfoques y métodos de investigación: análisis teórico. *Revista Mundo Recursivo, 3(1)*, 1-24. https://www.atlantic.edu.ec/ojs/index.php/mundor/article/view/38.

Hernández, R., y Mendoza, C. (2018). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta.* McGraw Hill.

Hernández, R., Mendez, S., Mendoza, C., y Cuevas, A. (2017). *Fundamentos de investigacion.* Mc Graw Hill education.

Herrera, I. (2018). Las prácticas investigativas contemporáneas. Los retos de sus nuevos planteamientos epistemológicos. *Revista Scientific., 3(7)*, 1-10. https://doi.org/10.29394/Scientific.issn.2542-2987.2018.3.7.0.6-15.

Hoyos, N. (2022). *Flagrancia delictiva como instrumento procesal y la lucha contra la criminalidad en el Perú*. (Tesis de maestria, Universidad Inca Garcilaso de la Vega).

http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/7035/TESIS%20COMPLETA%20HOYOS%20CUBAS%20NELY.pdf?sequence=1&isAllowed=y

Jaishankar, K. (2008). *Space transition theory of cybercrimes.* Prentice Hall.

Jiménez, J. (2017). *Manual de derecho penal informático.* Jurista Editores E.I.R.L.

Kuhn, T. (2019). *La estructura de las revoluciones científicas.* Fondo de cultura económica.

Ley de Delitos Informáticos. (2013). *Plataforma digital única del Estado Peruano*. https://www.gob.pe/institucion/mpfn/informes-publicaciones/1678028-ley-n-30096

Lopez, I. (1993). *Especialidades procesales en el enjuiciamiento de delitos privados y semiprivados.* Libreria Dykinson.

Luna, P. (2020). *La intervención judicial de las comunicaciones privadas.* https://forojuridico.mx/la-intervencion-judicial-de-las-comunicaciones-privadas/

Machicado, J. (2010). *Derecho Procesal Penal.* Universidad San Francisco Xavier.

Martínez, H., y Benítez, L. (2016). *Metodología de la Investigación social I.* Cengage Learning Editores, S.A. de C.V.

Ministerio Publico. (2020). *Ciberdelincuencia en el Peru - Pautas para una Investigacion Fiscal.* https://cdn.www.gob.pe/uploads/document/file/1669400/1667473-ciberdelincuencia-en-el-per-pautas-para-una-investigacin-fiscal-especializada.pdf?v=1709212413

Montero, J. (1997). *Derecho jurisdiccional. T. 1, Parte general.* Tirant lo Blanch.

Neyra, J. (2010). *Manual del nuevo Proceso Penal & de litigacion oral.* https://www.mpfn.gob.pe/escuela/contenido/archivosbiblioteca/dpp0608.pdf

Otzen, T., y Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. *International Journal of Morphology*, *1,* 227-232. http://dx.doi.org/10.4067/S0717-95022017000100037 .

Perez, R. (2021). *Alcance del secreto de las diligencias preliminares en la investigación contra el crimen organizado y su relación con el derecho de defensa del imputado*. [Tesis de maestría, Universidad Nacional Jóse Faustino Sánchez Carrión]. https://repositorio.unjfsc.edu.pe/bitstream/handle/20.500.14067/4461/RICARDO%20ADOLFO%20PEREZ%20CAPCHA.pdf?sequence=1&isAllowed=y.

Pinto, M. (2017). *El rol del ministerio público y la PNP en las etapas de investigación preliminar y preparatoria en el nuevo sistema procesal penal*. [Tesis de grado, Universidad Inca Garcilaso de la Vega]. http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/4901/TRSUFICIENCIA_PINTO%20CHAVEZ.pdf?sequence=1&isAllowed=y.

Pinto, M. (2020). El rol del ministerio publico y la PNP en las etapas de investigacion preliminar y preparatoria en el nuevo sistema procesal . [Tesis de grado, Universidad Inca Garcilaso de la Vega]. http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/4901/TRSUFICIENCIA_PINTO%20CHAVEZ.pdf?sequence=1&isAllowed=y.

Poma, J. (2020). *La investigación preliminar en el proceso penal peruano, problemas y situaciones de afectación a los Derechos Fundamentales*. [Tesis de maestrìa, Universidad Nacional Daniel Alcides Carrión]. http://repositorio.undac.edu.pe/bitstream/undac/2299/1/T026_15300068_M.pdf.

Poma, R. (2015). *La Diligencia preliminar y la investigación preparatoria.* https://biblioteca.cejamericas.org/bitstream/handle/2015/2403/LaDiligenciapreliminarylainvestpreparatoria.pdf?sequence=1&isAllowed=y

Posada, M. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad. *Nuevo Foro Penal, 13(88)*, 72-112. https://dialnet.unirioja.es/servlet/articulo?codigo=6074006.

Quevedo, J. (2017). *Investigacion y Prueba del Ciberdelito*. [Tesis doctoral, Universidad de Barcelona]. https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAll.

Ramos, J. (2011). *¡Graduese! de magister y doctor en ciencias juridicas* (2 ed.). Grijley.

Recovery Labs. (2020). *Servicio de recuperación de datos recomendado por los principales fabricantes de discos duros.* https://www.recoverylabs.com/

Reyes, C. (2020). *Los Delitos Informáticos y su influencia en la Integridad Personal*. [Tesis de grado, Universidad de las Ámericas]. http://repositorio.ulasamericas.edu.pe/handle/upa/1272.

Rodríguez, A., y Pérez, O. (2017). Métodos científicos de indagación y de construcción del conocimiento. *Revista Escuela de Administración de Negocios, 82*, 1-26. https://www.redalyc.org/pdf/206/20652069006.pdf.

Rojas, T. (2021). Postura paradigmática del docente investigado. *Universidad Centroccidental Lisandro Alvarado*, *1,* 195-205. http://aulavirtual.web.ve/revista/ojs/index.php/aulavirtual/article/view/25/154.

Ruiz, C. (2016). *Analisis de los delitos informaticos y su violación de los derechos constituciones de los ciudadanos*. [Tesis de grado, Universidad Nacional de Loja]. https://dspace.unl.edu.ec/jspui/bitstream/123456789/17916/1/Tesis%20Lista%20Carolin.pdf.

San Martín, C. (2006). *Derecho procesal penal.* Grijley.

Sànchez, M., Velasco, M., Espinoza, R., Gonzales, A., Romero, R., y Mory, W. (2023). *Metodología y estadística en la investigación científica.* Puerto Madero Editorial Académica. https://doi.org/10.55204/PMEA.17.

Sánchez, P. (2009). *El Nuevo Proceso Penal.* IDEMSA.

Santana, G. (2018). *Propuesta de un programa de prevención enfocado a la configuración de privacidad de la red social facebook aplicado en la escuela secundaria oficial Lic. Isidro Fabela*. [Tesis de grado, Universidad Autónoma del estado de México]. http://ri.uaemex.mx/bitstream/handle/20.500.11799/106027/TESIS%20GRISELDA%20%281%29.pdf?sequence=3&isAllowed=y.

Suarez, M. (2021). *El delito de interceptación de datos informáticos en el ordenamiento jurídico colombiano: inconvenientes en su tipificación y aplicación*. [Tesis de grado, Universidad Santo Tomas]. https://repository.usta.edu.co/bitstream/handle/11634/34852/2021miguelsuarez.pdf?sequence=1.

Tappan, P. (2017). ¿A qué se llama delincuente? *Delito soc., 26(44)*, 1-11. http://www.scielo.org.ar/pdf/delito/v26n44/v26n44a07.pdf.

Tenorio, J. (2018). *Desafios y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia*. [Tesis de maestría, Academia diplomática del Perú]. https://repositorio.adp.edu.pe/bitstream/handle/ADP/71/2018%20Tesis%20Tenorio%20Pereyra%2c%20Julio%20Eduardo.pdf?sequence=1&isAllowed=y.

Valderrama, S. (2019). *Pasos para elaborar proyectos de investigacion cientifica.* Editorial San Marcos.

Valderrama, S., y Jaimes, C. (2019). *El desarrollo de la tesis. Descriptiva - comparativa, correlacional y cuasiexperimental.* Editorial San Marcos.

Vanderbosch, C. (1980). *Investigacion de delitos.* Limusa.

Vega, J., y Arévalo, M. (2022). *Ciberdelitos, análisis en el sistema penal.* Editorial Iustitia S.A.C.

Vega, R. (2018). *La investigación preliminar en el nuevo código procesal penal*. https://www.derechoycambiosocial.com/revista023/Diligencias_preliminares.pdf

Ventura, J. (2017). ¿Población o muestra?: Una diferencia necesaria. *Revista Cubana de Salud Pública, 43(3)*, 648-649. http://scielo.sld.cu/pdf/rcsp/v43n4/spu14417.pdf.

Villavicencio, f. (2014). Delitos Informaticos. *Revista IUS ET VERITAS, 49*, 284-304. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630/14253.

World Legal Corporation. (2021). *Delitos informáticos en Colombia*. https://www.worldlegalcorp.com/blog/delitos-informaticos-en-colombia/

IX ANEXOS

Anexo A. Matriz de consistencia

INFLUENCIA DE LAS DILIGENCIAS PRELIMINARES EN LOS DELITOS INFORMÁTICOS EN EL CERCADO DE LIMA, AÑO 2024.

PROBLEMA

Problema General

¿Cómo influye las diligencias preliminares en los delitos informáticos en el Cercado de Lima, año 2024?

Problemas específicos

¿Cómo influye la dimensión investigativa en los delitos informáticos en el Cercado de Lima, año 2024?

¿De qué manera influye la dimensión preventiva en los delitos informáticos en el Cercado de Lima, año 2024?

¿De qué manera influye la dimensión resolutiva en los delitos informáticos en el Cercado de Lima, año 2024?

OBJETIVOS

Objetivo General

Evaluar cómo influye las diligencias preliminares en los delitos informáticos en el Cercado de Lima, año 2024.

Objetivos específicos

Explicar cómo influye la dimensión investigativa en los delitos informáticos en el Cercado de Lima, año 2024.

Evaluar de qué manera influye la dimensión preventiva en los delitos informáticos en el Cercado de Lima, año 2024.

Explicar de qué manera influye la dimensión resolutiva en los delitos informáticos en el Cercado de Lima, año 2024.

HIPÓTESIS

Hipótesis General

Las diligencias preliminares influyen positivamente en los delitos informáticos en el Cercado de Lima, año 2024.

Hipótesis específicas

La dimensión investigativa influye positivamente en los delitos informáticos en el Cercado de Lima, año 2024.

La dimensión preventiva influye positivamente en los delitos informáticos en el Cercado de Lima, año 2024.

La dimensión resolutiva influye positivamente en los delitos informáticos en el Cercado de Lima, año 2024.

VARIABLES

Variable independiente: Diligencias preliminares

Dimensiones	Indicadores	Ítems
Investigativa	Pruebas Recolectadas	1, 2
	Calidad de la Información Recopilada	3, 4
Preventiva	Conservación de Pruebas	5, 6
	Medidas Cautelares Solicitadas	7, 8
Resolutiva	Resolución Extrajudicial	9, 10
	Promedio de Resolución	11, 12

Variable dependiente: Los delitos informáticos

Dimensiones	Indicadores	Ítems
Acceso Ilícito	Transferencias electrónicas fraudulentas	1, 2
	Vishing	3, 4
Fraude Informático	Clonación de tarjetas de crédito	5, 6
	Ransomware:	7, 8
Suplantación de identidad	Phishing	9, 10
	Compras por internet mediante información de tarjetas de crédito o débito	11, 12

METODOLOGÍA
Enfoque. Cuantitativo
Tipo de la investigación: Explicativo
Diseño: No experimental
Población: 30 profesionales en derecho penal de Lima Centro
Muestra: 30 profesionales en derecho penal de Lima Centro
Muestreo: No probabilístico

Anexo B. Validación de instrumentos

La validez es el grado en que un instrumento en verdad mide la variable que se busca medir. Se logra cuando se demuestra que el instrumento refleja el concepto abstracto a través de sus indicadores empíricos (Hernández y Mendoza, 2018).

La validez de expertos se refiere al grado en que un instrumento realmente mide la variable de interés, de acuerdo con expertos en el tema (Hernández y Mendoza, 2018).

El instrumento de medición fue sometido a juicio de expertos para su validación de instrumentos, los cuales fueron los siguientes:

Tabla 14

Expertos durante la evaluación de los instrumentos

Experto	Decisión
Sánchez Sotomayor, Segundo	Si existe suficiencia
Begazo de Bedoya Luis	Si existe suficiencia
Sánchez Camargo Mario	Si existe suficiencia

Certificado de validación de instrumentos

EUPG
ESCUELA UNIVERSITARIA DE POSTGRADO

UNIVERSIDAD NACIONAL FEDERICO VILLAREAL
VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
POR CRITERIO DE JUECES

I.DATOS GENERALES

1.1 Apellido y nombre del Juez : Sánchez Carranza María Rebeca

1.2 Cargo e institución donde labora : Universidad Nacional Federico Villarreal

1.3 Nombre del instrumento evaluado: Cuestionario

1.4 Autor del instrumento : Lopez Ibarra Cesar

II.ASPECTO DE LA VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE 1	BAJA 2	REGULAR 3	BUENA 4	MUY BUENA 5
1. CLARIDAD	Esta formulado con lenguaje apropiado y Comprensible					X
2. OBJETIVIDAD	Permite medir hechos observables					X
3. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACIÓN	Presentación ordenada					X
5. SUFICIENCIA	Comprende aspectos de las variables en cantidad y calidad suficiente					X
6. PERTINENCIA	Permite conseguir datos de acuerdo a los objetivos planteados					X
7. CONSISTENCIA	Pretende conseguir datos basados en teorías o modelos teóricos					X
8. COHERENCIA	Entre variables, indicadores y los ítems					X
9. METODOLOGÍA	La estrategia responde al propósito de la investigación					X
10. APLICACIÓN	Los datos permiten un tratamiento estadístico pertinente					X
CONTEO TOTAL DE MARCAS (Realice el conteo en cada una de las categorías de la escala)		A	B	C	D	E

Coeficiente de validez = 1 x A + 2 x B + 3 x C + 4 x D + 5 x E = $\frac{E}{50}$

III.Calificación global (Ubique el coeficiencia de validez obtenido en el intervalo respectivo y marque con un aspa en el círculo asociado)

CATEGORÍA	INTERVALO
Desaprobado ( )	[0,00-0,60]
Observado ( )	<0,60-0,70]
Aprobado (X)	<0,70-1.00]

IV.Calificación de aplicabilidad

Aprobado

Lugar: Lima 21 de 02 del 2024

FIRMA DEL JUEZ

EUPG
ESCUELA UNIVERSITARIA DE POSTGRADO

UNIVERSIDAD NACIONAL FEDERICO VILLAREAL
VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
POR CRITERIO DE JUECES

I.DATOS GENERALES

1.1 Apellido y nombre del Juez : Sánchez Sotomayor Segunda

1.2 Cargo e institución donde labora : Universidad Nacional Federico Villareal

1.3 Nombre del instrumento evaluado: Cuestionario

1.4 Autor del instrumento : Lopez Lozoya César

II.ASPECTO DE LA VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE 1	BAJA 2	REGULAR 3	BUENA 4	MUY BUENA 5
1. CLARIDAD	Esta formulado con lenguaje apropiado y Comprensible					X
2. OBJETIVIDAD	Permite medir hechos observables					X
3. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACIÓN	Presentación ordenada					X
5. SUFICIENCIA	Comprende aspectos de las variables en cantidad y calidad suficiente					X
6. PERTINENCIA	Permite conseguir datos de acuerdo a los objetivos planteados					X
7. CONSISTENCIA	Pretende conseguir datos basados en teorías o modelos teóricos					X
8. COHERENCIA	Entre variables, indicadores y los ítems					X
9. METODOLOGÍA	La estrategia responde al propósito de la investigación					X
10. APLICACIÓN	Los datos permiten un tratamiento estadístico pertinente					X

CONTEO TOTAL DE M/ RCAS (Realice el conteo en cada una de las categorías de la escala)	A	B	C	D	E

Coeficiente de validez = 1 x A + 2 x B + 3 x C+ 4 x D + 5 x E = $\frac{E}{50}$

III. **Calificación global** (Ubique el coeficiencia de validez obtenido en el intervalo respectivo y marque con un aspa en el círculo asociado)

CATEGORÍA	INTERVALO
Desaprobado ( )	[0,00-0,60]
Observado ( )	<0,60-0,70]
Aprobado (X)	<0,70-1.00]

IV.Calificación de aplicabilidad

Aprobado

Lugar: Lima 27 de 02 del 2024

FIRMA DEL JUEZ

EUPG POSTGRADO

UNIVERSIDAD NACIONAL FEDERICO VILLAREAL
VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN POR CRITERIO DE JUECES

I.DATOS GENERALES

1.1 Apellido y nombre del Juez: Begazo De Bedoya Ines

1.2 Cargo e institución donde labora: Universidad Nacional Federico Villarreal

1.3 Nombre del instrumento evaluado: Cuestionario

1.4 Autor del instrumento: Lopez Izaguirre Cesar

II.ASPECTO DE LA VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE 1	BAJA 2	REGULAR 3	BUENA 4	MUY BUENA 5
1. CLARIDAD	Esta formulado con lenguaje apropiado y Comprensible.					X
2. OBJETIVIDAD	Permite medir hechos observables					X
3. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACIÓN	Presentación ordenada					X
5. SUFICIENCIA	Comprende aspectos de las variables en cantidad y calidad suficiente					X
6. PERTINENCIA	Permite conseguir datos de acuerdo a los objetivos planteados					X
7. CONSISTENCIA	Pretende conseguir datos basados en teorías o modelos teóricos					X
8. COHERENCIA	Entre variables, indicadores y los ítems					X
9. METODOLOGÍA	La estrategia responde al propósito de la investigación					X
10. APLICACIÓN	Los datos permiten un tratamiento estadístico pertinente					X

CONTEO TOTAL DE MARCAS (Realice el conteo en cada una de las categorías de la escala)	A	B	C	D	E

Coeficiente de validez = 1 x A + 2 x B + 3 x C+ 4 x D + 5 x E = $\frac{E}{50}$

III. **Calificación global** (Ubique el coeficiencia de validez obtenido en el intervalo respectivo y marque con un aspa en el circulo asociado)

CATEGORÍA	INTERVALO
Desaprobado ( )	[0,00-0,60]
Observado ( )	<0,60-0,70]
Aprobado (X)	<0,70-1.00]

IV.Calificación de aplicabilidad

Aprobado

Lugar: Lima 01 de 03 del 20 23

FIRMA DEL JUEZ

Anexo C. Confiabilidad de Instrumentos

En la confiabilidad del instrumento por ser variables de escala ordinal se utilizo el Alfa de Cronbach.

La confiabilidad es la precisión del instrumento para medir la variable de interés. A mayor fiabilidad sera menor la cantidad de errores aleatorios e impredecibles que apareceran al utilizarlo.

Tabla 15

Resumen de procesamientos de casos

		N	%
Casos	Válido	58	100,0
	Excluido[a]	0	,0
	Total	58	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Nota. Según la tabla 15, los resultados de las 58 encuestas que fueron procesadas mediante el SPSS, no presenta casos de exclusion, el 100% fueron aceptados.

Tabla 16

Confiabilidad del instrumento de la variable independente

Alfa de Cronbach	N de elementos
,976	12

Nota. Mediante el SPSS se obtuvo un coeficiente de fiabilidad de 0.976, se interpreta como una alta fiabilidad.

Tabla 17

Confiabilidad del instrumento de la variable dependiente

Alfa de Cronbach	N de elementos
,886	12

Nota. Mediante el SPSS se obtuvo un coeficiente de fiabilidad de 0.886, se interpreta como una alta fiabilidad.

Anexo D. Instrumento de medición

Esta información será utilizada en forma confidencial, anónima y acumulativa; por lo que agradeceré proporcionar información veraz, sólo así serán realmente útiles para la presente investigación. Lea con atención y conteste a las preguntas marcando con una "X" en un solo recuadro, teniendo en cuenta la siguiente escala de calificaciones:

CALIFICACIÓN		
1	2	3
Totalmente en desacuerdo	Indeciso	Totalmente de acuerdo

	Diligencia Preliminares	**1**	**2**	**3**
	Dimensión. Investigativa			
01	Las diligencias preliminares realizadas en los casos de delitos informáticos son efectivas para la recolección de pruebas.			
02	La calidad de las pruebas recolectadas durante las diligencias preliminares influye positivamente en la resolución de los delitos informáticos.			
03	La información recopilada durante las diligencias preliminares es relevante para los delitos informáticos.			
04	La calidad de la información obtenida en las diligencias preliminares mejora la efectividad de la investigación de delitos informáticos.			
	Dimensión. Preventiva			
05	Las diligencias preliminares contribuyen a una adecuada conservación de pruebas en los delitos informáticos.			
06	La conservación de pruebas durante las diligencias preliminares previene la pérdida de información crucial en los delitos informáticos.			
07	Las medidas cautelares solicitadas durante las diligencias preliminares son efectivas para prevenir la comisión de delitos informáticos.			
08	La implementación de medidas cautelares en las diligencias preliminares contribuye a la protección de las pruebas en los casos de delitos informáticos.			
	Dimension. Resolutiva			
09	Las diligencias preliminares facilitan la resolución extrajudicial de los casos de delitos informáticos.			
10	La resolución extrajudicial lograda durante las diligencias preliminares contribuye a una respuesta más rápida en los delitos informáticos.			

11	El promedio de resolución de los casos de delitos informáticos ha mejorado gracias a las diligencias preliminares.			
12	Las diligencias preliminares permiten un promedio de resolución más rápido en los delitos informáticos.			

	Variable dependiente. Delitos informáticos	1	2	3
	Dimensión. Acceso ilícito			
1	¿Entiende usted el significado del delito Acceso Ilícito?			
2	¿Alguna vez ha sido víctima del delito de acceso Ilícito?			
3	¿Estando a su respuesta anterior, luego de ser víctima del delito antes referido, denunció el hecho?			
4	¿Estando su respuesta anterior, luego de la denuncia se logró dar con los autores del delito denunciado?			
	Dimensión. Fraude informático			
5	¿Entiende usted el significado del delito Fraude Informático?			
6	¿Alguna vez ha sido víctima del delito de Fraude Informático?			
7	¿Estando a su respuesta anterior, luego de ser víctima del delito antes referido, denunció el hecho?			
8	¿Estando su respuesta anterior, luego de la denuncia participo usted de las diligencias preliminares a fin de dar con los responsables del delito denunciado?			
	Dimensión. Suplantación de identidad			
9	¿Conoce usted de víctima del delito de suplantación de identidad?			
10	¿Tiene conocimiento del resultado de denuncias por este tipo de denuncias?			
11	¿Considera usted que las diligencias realizadas en este tipo de delitos son adecuadas y oportunas?			
12	¿Considera usted los delitos Informáticos son resueltos oportunamente?			