UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Los actos de investigación en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, distrito fiscal de Lima, 2021

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestra en Derecho Penal y Procesal Penal

AUTORA:

Usaqui Barbaran, Karina (ORCID: 0000-0002-5867-7730)

ASESOR:

Dr. Menacho Rivera, Alejandro Sabino (ORCID: 0000-0003-2365-8932)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal

LIMA – PERÚ

2022

Dedicatoria:

A mí querido padre quién siempre estuvo conmigo alentándome a ser cada día mejor persona, mis hijos que son mi fortaleza de uno pude seguir creciendo pese a las dificultades y finalmente a Dios que sin él no somos nada.

Agradecimiento:

A la Escuela de Post Grado de la universidad César Vallejo y toda su plana docente por haber contribuido a mi formación profesional y en especial a mi asesor de tesis al Dr. Alejandro Menacho Rivera que con su apoyo, paciencia y asesoría que contribuyó a la mejora del trabajo de investigación.

Índice de Contenidos

Índice de Tablas

Pág.

Índice de Figuras

RESUMEN

El presente trabajo se titula “Actos de investigación en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, distrito fiscal de Lima, 2021”, en el cual se tuvo como objetivo establecer los actos de investigación durante la etapa de investigación preparatoria incide en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, Distrito Fiscal de Lima, 2021. De modo que, el trabajo fue de enfoque cuantitativo de tipo básico, de diseño transeccional y no experimental, habiéndose aplicado como técnica de investigación la encuesta a 20 fiscales penales, 15 abogados patrocinados y 15 policías, y siendo validada por 3 expertos. Se llegó a la conclusión que los actos de investigación durante la etapa de investigación preparatoria inciden en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, en el Distrito Fiscal de Lima, 2021, debido a que resultados de la prueba de bondad de ajuste señalan un Chi cuadrado de 2,191 donde el rechazo es de la hipótesis alterna y aceptar la nula, tal es así que es posible referirse que el modelo empleado para la prueba estadística con es la regresión logística ordinal es acertada para la prueba de hipótesis.

Palabras clave: Actos de investigación, Persecución eficaz y Ciberdelincuencia.

ABSTRACT

This work is entitled "Evidence activity in the effective prosecution of crimes committed by cybercrime, fiscal district of Lima, 2021", in which the objective of establishing the investigation acts during the preparatory investigation stage affects the effective prosecution of crimes committed by cybercrime, Fiscal District of Lima, 2021. Thus, the work was of a basic quantitative approach, of a transectional and non-experimental design, having applied as a research technique the survey to 20 criminal prosecutors, 15 sponsored lawyers and 15 police officers, and being validated by 3 experts. It was concluded that the acts of investigation during the preparatory investigation stage have an impact on the effective prosecution of crimes committed by cybercrime in the Public Prosecutor's District of Lima, 2021, because the results of the goodness of fit test show a Chi square of 2.191 where the rejection is of the alternative hypothesis and accept the null, so it is possible to refer that the model used for the statistical test with ordinal logistic regression is successful for the hypothesis test.

Keywords: Investigative acts, Effective prosecution and Cybercrime.

I. INTRODUCCIÓN

En el año 2021, se cumple 51 años del nacimiento del servicio de internet, donde se ha podido apreciar cómo la red sirve tanto para la comunicación, para el acceso al conocimiento, para las actividades económicas de comercio y un sinfín de actividades fundamentales para el desarrollo de los países de todo el mundo. Sin embargo, los servicios de la red global también han traído consigo actividades delictivas como los delitos informáticos a nivel mundial, nacional y local, cuyas consecuencias ha generado no solo la afectación al patrimonio de las personas sino también a su honorabilidad.

En el aspecto de los delitos cometidos mediante el uso de las vías informáticas Proaño y Gavilanes. (2018) mencionaron como estas son realizadas por sujetos con conocimientos elevados en informática que, se aprovechan de las debilidades de los sistemas para poder vulnerarlos y acceder a información privada, con conocimiento de esta, se suelen producir los secuestros de datos, extorsiones, suplantación de identidad y demás.

En el Perú, la comisión de los delitos en el área informática encuentra una libertad absoluta para moverse y un anonimato que protege al agresor, esto, debido a que las medidas de reconocimiento por redes suelen ser limitadas y de acceso especializado, mostrando así la IP como el protocolo de identificación único de internet de cada equipo y la localización vía GPS, sin embargo, estos pueden ser fácilmente cubiertos al momento de realizar los ilícitos.

Este anonimato presentado en las redes y los modos de encubrir la identificación de los agresores, requiere que las autoridades tengan un conocimiento alto en sistemas informáticos a fin de poder ejercer una adecuada persecución eficaz del delito. Sin embargo, en el país se empezó a regular la materia en un modo deficiente a finales del 2013, para posteriormente con el Convenio Budapest en 2019, reformular todos los planteamientos. Según el Ministerio Público (2020) gracias a esta regulación, permitió identificar desde el 2013 hasta el 2020, unas 21687 denuncias realizadas en el país, de las cuales casi el 60% se encuentran archivadas. Esto demuestra una deficiencia en las

investigaciones a nivel preliminar, muchas veces por falta de capacitación de los operadores de justicia y en otras oportunidades por denunciar de manera tardía, lo que hace imposible preservar evidencia, siendo las redes sociales muy volátil.

De otro lado, con la creación de las Fiscalías Especializadas de Ciberdelincuencia, se busca contar con operadores judiciales más preparados, que permita bajar el alto índice de denuncias archivadas, ya que menos del 1% de denuncias tramitados por el Ministerio Público se requirió información a los proveedores de redes sociales sobre los ilícitos sucedidos, se puede mencionar también que para obtener la geolocalización es necesario enviar una solicitud a las empresas de telefonía e internet, sin embargo, estas suelen ser rechazadas ya que para brindar los datos se requiere del dictamen judicial, IMEI del equipo móvil y DNI del titular del servicio, trámite burocrático, que suele retrasar la obtención de elementos de convicción que permita vincular el hecho ilícito con los imputados y muchas veces con el retardo se pierden evidencias que no pueden ser recuperadas por ser las redes sociales muy volátil.

Respecto al peritaje se puede apreciar cómo estos encuentran deficiencias en su gestión, pues los mismos deben hacerse respetando los derechos de toda persona, por tanto, esto conlleva para el apartado de equipos personales no vulnerar los sistemas de seguridad empleados por la persona como el patrón o contraseña PIN, sin embargo, al brindar el consentimiento se podrá acceder haciendo uso de “llaves informáticas” lo cual genera demora y posible deterioro en los datos, esto pone en duda la efectividad de los modelos empleados.

Tratándose de efectividad al realizarse la apertura de la información, los fiscales argumentan en su requerimiento “recabar información relevante” sin especificar lo requerido, lo cual deja a una libre decisión del experto perito para determinar qué información podría ser relevante para el proceso.

Estas deficiencias sobre el acceso a la información e imposibilidad de identificación son los motivos principales por los cuales se llegan a archivar las denuncias en materia, generando así una deficiencia en las investigaciones.

Por tanto, se consideró como problema general: ¿De qué manera, los actos de investigación durante la etapa de investigación preparatoria inciden en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, en el Distrito Fiscal de Lima, 2021?, teniendo como problemas específicos: 1) ¿De qué manera, la recopilación de elementos de convicción por parte del fiscal incide en la persecución eficaz de los delitos cometidos por la ciberdelincuencia en el Distrito Fiscal de Lima, 2021? 2) ¿De qué manera, la recopilación de elementos de convicción por parte de la policía incide en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, en el Distrito Fiscal de Lima, 2021? 3) ¿De qué manera, la recopilación de elementos de convicción por parte del fiscal incide en el patrimonio de las víctimas en los delitos cometidos por la ciberdelincuencia en el Distrito Fiscal de Lima, 2021?, 4) ¿De qué manera, la recopilación de elementos de convicción por parte de la policía incide en la integridad psicológica de la víctima en los delitos cometidos por la ciberdelincuencia, en el Distrito Fiscal de Lima, 2021?

Por esto, la justificación teórica del estudio tiene como sustento el análisis de la problemática existente en los actos de investigación y como esta incide en la persecución eficaz de los delitos cometidos por la ciberdelincuencia para contrastar las actuaciones con los pronunciamientos de países extranjeros e investigaciones donde en verdad se demostró una eficacia frente a los delitos en el área informática. Asimismo, la justificación práctica tiene la necesidad de analizar la gestión de los fiscales y la calidad de los peritajes realizados para determinar deficiencias como posibles medios idóneos a emplear. Además, tiene justificación social en que las contribuciones de este estudio brindarán soluciones a los delitos cometidos por la ciberdelincuencia. Para finalizar, tiene justificación metodológica debido a que identifica al estudio cuantitativo para medir el problema estadísticamente.

De este modo, el objetivo general planteado es: Establecer los actos de investigación durante la etapa de investigación preparatoria, si incide en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, en el Distrito Fiscal de Lima, 2021; entre los objetivos específicos: 1) Determinar la manera en que la recopilación de elementos de convicción por parte del fiscal incide en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, en el Distrito Fiscal de Lima, 2021, 2) Establecer la manera en que la recopilación de elementos

de convicción por parte de la policía incide en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, en el Distrito Fiscal de Lima, 2021. 3.- Tercer objetivo específico, el de Determinar la manera en que la recopilación de elementos de convicción por parte del fiscal incide en el patrimonio de las víctimas en los delitos cometidos por la ciberdelincuencia en el Distrito Fiscal de Lima, 2021, 4) Establecer la manera en que la recopilación de elementos de convicción por parte de la policía incide en la integridad psicológica en los delitos cometidos por la ciberdelincuencia, en el Distrito Fiscal de Lima, 2021

II. MARCO TEÓRICO

Para comprender a fondo la situación de los actos de investigación en los delitos informáticos y su eficiencia en la persecución eficaz del delito en el marco de antecedentes internacionales es necesario consultar a Sampaoli (2018), Peritaje informático Marco teórico – práctico. Tesis de Licenciatura en sistemas y computación. Universidad Católica de Argentina. El autor mencionó como se analizó en el país argentino los mecanismos de peritaje realizado en computadoras, celulares e identificó como prioridad conforme a ley, el mantenimiento de estándares internacionales y su importancia de la adopción a su realidad, pues normalmente los planteamientos internacionales difieren de la naturaleza de los sistemas y circunstancias de cada nación, siendo esto necesario para responder en misma medida y mantener una eficacia, siendo así, el acceso a la información deberá proseguir con el consentimiento de la parte y de requerir información se deberá proceder con dictámenes que permitan dar poder suficiente al fiscal para solicitar la información ante empresas que gestionen sistemas complejos como las redes sociales o los dispositivos de Apple, Google, Huawei o Xiaomi, pues los mismos aceptan solicitudes de la justicia de cada país debidamente acreditada para brindar la información de sus dispositivos cuando existas delitos de por medio, sobre esta información brindada es que podrá realizarse el peritaje especializado con mayor eficacia debido a que el tiempo de acceso a los sistemas se ve drásticamente reducido.

Por otro lado, los autores Ramírez y Castro (2018) analizaron la evidencia digital en Colombia como soporte judicial de delitos informáticos mediante cadena de custodia. Informe final de proyecto aplicado par optar por el título de Especialista en seguridad informática. Universidad Nacional Abierta y a Distancia. Demuestran en su proyecto de investigación como para obtener un desarrollo en la sociedad las personas requieren estar a la vanguardia de las nuevas tecnologías, pues están proporcionan facilidades en cuanto a la relación humana y puestos laborales, lo cual los convierte en herramientas sumamente necesarias para el acceso a la información. Esta alta dependencia es lo que convierte a estos dispositivos en los blancos preferidos de ataques cibernéticos, pues en ellos se almacena información personal de carácter social, laboral y económico, con lo que es un importante

bloque de información. Siendo así, producto del avance social el derecho se va adaptando a regular estos nuevos bienes y es que recoge el apartado de ciberdelincuencia, las conductas criminales destinadas al secuestro de información, extorsión, afección de la libertad y el acceso a las cuentas bancarias. Esto sirvió como precedente para el Ministerio de Telecomunicaciones en la creación de la Ley 1273 que se destina a facilitar tanto personal como tecnología para la cooperación con el Poder Judicial a fin de mantener un personal capacitado, este trabajo en conjunto desarrolló las cadenas de custodia, pues la información informática a diferencia de la física, puede ser fácilmente manipulada por lo que, el valor probatorio de esta debe considerarse por encima de la física, lo que genera un tratamiento distinto y prioritario en las actuaciones, sin embargo, esta cooperación se limite a la misma, no extiende manual de procedimiento ni protocolos, por lo que, las cadenas de custodia van a depender mucho del personal a cargo y es posible prever comúnmente un deterioro o extravío de la evidencia.

Por lo explicado, se puede apreciar como el país considera al personal del Ministerio de Tecnología como parte también del Poder Judicial, puesto que, los ajenos son encargados a realizar las pericias tecnológicas, cierres de información e informes, sin embargo, en la manipulación esto se encomienda al Poder, donde a falta de guías se evidencia un gran deterioro de la información y perdida del material.

Mientras la autora López (2016) indicó que los delitos informáticos y la investigación fiscal en las entidades financieras cooperativas, segmento uno de la economía popular y solidaria en el Cantón de Ambato, Provincia de Tungurahua. Trabajo de graduación previo a la obtención del título de abogada en los juzgados tribunales. Universidad técnica de Ambato. Mediante la investigación realizada se puede evidenciar como el objetivo más común en los delitos informáticos vienen a ser las transacciones financieras por internet, principalmente por la falta de conocimiento de las personas sobre su seguridad y riesgos, ante esto, se encuentra la modalidad de phishing donde sin mucho conocimiento de informática, el agresor envía a la víctima un correo donde se hace pasar por la entidad bancaria y solicita número de tarjeta como contraseña, una vez obtenido la información, el delincuente

transfiere el dinero de la cuenta de la víctima hacia una cuenta de un tercero, para retirarlo posteriormente.

Se menciona, además, como las personas al navegar por internet no mantienen un amplio conocimiento sobre el cifrado de redes o correos sospechosos y haciendo provecho del desconocimiento es como los criminales abusan de esto para, con un bajo conocimiento de informática acceder a la información de sus víctimas.

Desde una perspectiva de los antecedentes nacionales se encontró materia de investigación relevante para el tema, siendo así es que el autor Pastor (2020) precisó que el modelo de gestión del análisis forense de hechos delictivos informáticos en el marco del sistema de justicia peruano. Tesis para optar el grado académico de doctor en ingeniería de sistemas. Universidad nacional Federico Villareal. Preciso como la necesidad de modernización es constante para los sectores especializados de la fiscalía en el análisis forense de los delitos de carácter informático, pues la labor no culmina en la identificación del sujeto, si no, en la constatación de los hechos realizados por el mismo, esto genera un amplio conocimiento del tema, lo que evidentemente demuestra que el ente persecutor del delito tiene deficiencias en cuanto a su organización, pues no existe un protocolo de funciones sobre los peritajes a emplear, tampoco sobre el mantenimiento y gestión de los sistemas como de responsabilidad de cada acto o dependencia de determinados sistemas. Esto genera una problemática y especie de suerte al aire, debido a que el personal que se encargará de realizar el peritaje deberá ser un experto en la materia informática con una alta capacitación a fin de obtener resultados eficientes, sin embargo, de no serlo, es posible que el caso termine siendo archivado. Por ello, el autor desarrolla el modelo FORESYS, por el cual, se gestionaron apartados metodológicos relevantes que sirven como un correcto sistema de optimización de las actuaciones que actúa en base a la urgencia y productividad, donde primero se identifica el modo de comisión del ilícito, luego las herramientas empleadas y finalmente los patrones de la persona que los empleó.

También, Alarcón y Barrera, (2017) plantearon el uso de internet y delitos informáticos en los estudiantes de primer semestre de la universidad pedagógica y tecnológica de Colombia, sede seccional Sogamoso 2016. Tesis para optar por el

grado académico de Maestro en informática educativa. Universidad Norbert Wiener. Los autores realizaron durante su proyecto de investigación un proceso de análisis exhaustivo donde llegan a determinar en base a la estadística recogida de la practica como las personas objeto del estudio, determinando que las conductas de estos incurren muchas veces en el desarrollo de delitos informáticos, sin embargo, no tienen conocimiento de la legalidad de los mismos, esto se debe a la facilidad que mantienen las personas objeto del estudio en cuanto al acceso a las tecnologías y donde sus principales actuares se motivan por extraer información, localizar a personar, registrar sucesos en material audiovisual. La normalidad y cotidianidad de los sucesos demuestra como existen estudiantes que demuestran tener altas habilidades en el uso de la informática, sin embargo, estas se emplean para la comisión de delitos y por falta de guía u organización, la capacidad de su propio uso no puede ser explotadas para un fin positivo para los mismos. Sobre los escenarios que los autores pudieron analizar llegaron a la conclusión que los ilícitos cometidos suelen ser un delito de acción, ya que el propio empleo de los medios tecnológicos se suele motivar por un fin de beneficio propio y perjuicio a la víctima, sobre este, se desarrollaran determinadas actitudes que siguen un proceso ordenado, lo cual demuestra un accionar constante y premeditado.

Es relevante considerar a Huarcaya, (2021) quien refirió sobre la influencia de los delitos informáticos en el crimen organizado en el distrito de San Isidro 2020. Tesis para optar por el título de abogado. Universidad Peruana de las Américas. La autora desarrolla que, en San Isidro el crimen informático organizado presenta una alta complejidad sobre el desarrollo de sus actividades, lo que impide una respuesta estatal efectiva, pues una posible intervención sería imposible de realizarse por el poco abordaje en la materia legal y encontraría conflictos con otros derechos.

La falta de normas en este apartado genera un campo libre para el crecimiento de los crímenes organizados en materia informática, pues como principal objetivo se tienen los datos personales, sin embargo, estos no son sustraídos, si no, copiados en un dispositivo de almacenamiento y empleando mecanismos como puertas bajas o puertos abiertos, no se considera para el país legalmente como una violación a alguna norma. Lo que podría generar un ilícito es

la comercialización de la información y las extorsiones a las que deriven, ya que, estas conductas serían las únicas vistas como lesivas al ordenamiento jurídico.

Entre algunas otras conductas se aprecian las estafas románticas, sexuales y extorsiones de mismas características, estos son los resultados finales de la mayoría de información obtenida y sobre el cual es necesario realizar avances tecnológicos a nivel legal que no solo permitan recuperar la información, si no, acceder e identificar a las personas que las realizan y facilitan los medios para su comisión, por ello la municipalidad del distrito propone dos proyectos de ley, 5630-2020 y 4929-2020 que mencionan como los delitos informáticos deberán consignarse como aquellos que vulneren cualquier sistema informático y accedan a la información privada de la persona, tanto en el valor social como financiero, esto quiere decir que no será necesario configurar una sustracción o deterioro de la información para considerarse como delito.

En razón a la primera variable encontramos relevante mencionar a los actos de investigación, a lo que los autores Nobles, et al., (2020) señalaron como las actuaciones durante los actos de investigación deben considerarse que esta tendrá un valor informático, es decir, conceptúa a la prueba electrónica por lo que el enfoque en relación a las pericias normales debe cambiar sus planteamientos, principalmente desde el apartado metodológico, la recolección de esta información va a referirse a los criterios que se emplearan para lo mismo, la definición y conceptualización serán elementos principales para mantener una autenticidad en unos datos tan frágiles, la confianza de la fuente de la información y la necesidad de relación con el suceso para poder fundar una hipótesis y demostrarla.

Por ello, los autores Quispe, et al., (2019) mencionaron como las practicas forenses en informática deberán analizar la información con un backup a fin de mantener un respaldo original y no deteriorar la información como poder visualizar en un futuro el estado intacto de lo encontrado para contrastarlo, principalmente se requiere esto debido a que, cuando se realiza la apertura de archivos estos suelen registrar hora y fecha de su acceso, entonces después de una pericia sin un backup genera un deterioro completo de la prueba, tanto en su originalidad como en su credibilidad, pues el solo acceso posterior ya podría ser suficiente como para aducir

a una modificación del contenido de los archivos, siendo esto en materia legal un motivo suficiente para restar credibilidad y cuestionar la prueba.

Es sumamente relevante precisar los medios de convicción y su recopilación, por ello, Sundt (2006) mencionó que, el propio hecho de emplear técnicas forenses ya está generando una violación a la seguridad del propio sistema, por ello, su obtención va a verse constantemente atacada en si la misma fue recogida por medios lícitos, esto suele suceder fundamentalmente por la imprecisión de las regulaciones sobre las telecomunicaciones y el secreto a las mismas. Sobre esto, el autor menciona también como las actividades forenses en tecnología no deben conducirse únicamente a la extracción e información, si no, en el análisis de las técnicas empleadas por los propios delincuentes para establecer mecanismos en la memoria de la propia institución y en una dualidad de funcionalidad permitir hacer una efectiva reconstrucción del hecho minuciosamente, pues los infractores suelen desarrollar métodos que en un futuro sean empleados por terceros y traten de tan alta complejidad que al no haber previsto y catalogado los pasos, sería imposible generar una recolección adecuada en un próximo suceso, esto es, lo que se conoce como “el suceso de las causas”.

Para la recolección de los medios de convicción se emplea la informática forense, esta no solo busca detectar la comisión del ilícito y sus formas, si no, hallar una solución posible para evitar la comisión de los ilícitos en un futuro, pues su tratamiento se centra en la seguridad informática para seguir los rastros de futuros perpetuadores y controlar el espacio de acceso. Por tanto, estos equipos de informática forense deberán ser multidisciplinarios, su conformación debe verse por personal de informática y abogados especializados en la materia para definir qué actuaciones serian consideradas ilegales y conocer los límites que el derecho plantea a la información de carácter personas.

Por ello, el autor anterior visto plantó cuatro etapas necesarias para la recolección de los medios: 1.- Actos preparatorios. 2.-Detección de la conducta y análisis. 3.- Recuperación de la información e informe de inseguridad. 4.- Back up y análisis de la información.

Estos pasos permitirán organizadamente mantener la información en dos modos, el primero de carácter igual al obtenido y perfectamente conservado,

mientras el segundo sirve para analizar a profundidad y realizar los métodos informáticos necesarios para acceder a esta.

Lo visto hasta el momento permite comprender al autor Canedo (2010) como la información de las personas puestas en sistemas informáticos genero un interés para la comisión de crímenes, por ello, estos suelen forzar los sistemas y en una atención acorde la informática forense debe seguir pilares fundamentales, la obtención del medio, los actos de preservación y el análisis de datos, esto no deberá verse como una actuación aislada puesto que, se requieren informes no únicamente sobre el acontecer criminal, si no también, sobre la vulnerabilidad encontrada en el sistema para prevenir ataques y proteger la privacidad de las personas. Los informes deben contener el tipo de información sustraída en el apartado de su naturaleza, el tipo de acceso perpetuado y los medios de comisión como los correos electrónicos o redes social para cooperar con la construcción de los mapas de delitos informáticos.

Respecto a la metodología forense, el autor reforzó la idea de la recopilación de datos y realizar backups para mantener un estado actual sin modificación de la evidencia obtenida y que los datos extraídos puedan ser corroborados en un futuro, en el lado del derecho especializado puede verse como mantener el estado original de la evidencia va a mantener la convicción de los elementos y sobre este actuará todo el peso de los actos de investigación, sin embargo, es necesario conservar adecuadamente el contenido, por ello es que se prevén determinados medios de almacenamiento a fin de no dañar el contenido tanto informáticamente como físico, esto deberá verse en los protocolos y tras el análisis del profesional en informática determinar cómo se debe realizar adecuadamente el traslado como su conservación.

En la variante de peritaje se consideró importante desarrollar lo plasmado por el Ministerio del Interior (2019) quienes, en relación con lo visto anteriormente, encontraron como ideales los siguientes dispositivos electrónicos para obtener y conservar información: Equipos de cómputo, servidores; a) sistemas de disco duros, b) Sistemas de discos duros, c) Memorias USB y SD, d) Skimmers, CD, impresoras y cámaras, e) Teléfonos móviles y relojes inteligentes, f) Tarjetas SIM, g) Reproductores MP3 y los POS.

Respecto al almacenamiento se mencionó como los dispositivos capaces de transportar la información deben responder según al volumen en un primer filtro y las limitaciones físicas en la segunda. En el manual se establece pasos controversiales para acceder a la información contenida en equipos: 1. Encender el monitor, 2. Mover el cursor lentamente, 3. Si se visualiza contraseña desconectar el equipo, 4. De acceder, desconectar el equipo si se observa la eliminación de datos, 5. Al terminar redactar en un acta lo presenciado, datos de identificación del equipo y otros dispositivos que pueda contener, rotular y lacrar.

Esto evidenciaría un manejo con falta de conocimiento y un protocolo que no contemplaría la delicadeza del manejo de la información, puesto que, el acceso solo debe ser permitido al equipo de peritaje especializado para evitar la pérdida de información por un manejo con desconocimiento.

Respecto a la variante de recopilación de medios de convicción por parte de la policía se puede citar a Del Río (2006) quien explicó cómo la policía actúa directamente en recoger testimonio y realizar peritaje sobre el material tecnológico que no contemple un acceso dificultoso y se limite a la observación del contenido y estado, sin embargo, mencionó como es normal encontrarse con un lenguaje extraño en la informática y donde en materia de criminal el lenguaje predominante es el inglés con un abundante número de contracciones, lo que para la labor se considera una brecha no solo de conocimiento, si no también, de comunicación y preparación pues las actividades tendrán que ser trasladas a la fiscalía para actuar con mayor especialidad y conocimiento.

El autor anterior también mencionó como es de preocupación que, las comisarias que cuentan con personal policial especializado en materia informática, son muy escasas, por lo que, el funcionamiento de su actuar no es suficiente para realizar una adecuada gestión de la información como del estado en el que se encuentra y ante una posible manipulación inadecuada que pueda deteriorar completamente su valor probatorio como contenido.

Sin embargo, el autor mencionó también como los medios que suele recolectar el personal policial se dirige más a cuenta personales de redes sociales de la persona e imágenes, ignorando que el apartado a considerar deberá ser el de la información que incrimine al sujeto, es decir, aquel que vincule al sujeto con el

ilícito ocurrido para determinar una culpabilidad lo que en algunas ocasiones suele ser complicado pues ante el desentendimiento de sistemas y la falta de la presencia del testigo que pueda indicar como cada actuar se vincula con el caso para su reconocimiento, resulta difícil identificar las conductas que pudieron desarrollar el delito, es aquí donde el autor valora a los testigos.

Respecto a los testigos se van a considerar los testimonios dados con razón a los hechos y estos deberán posteriormente ser contrastados con las pruebas obtenidas de los medios informáticos para contrastar las actuaciones, por ello, las declaraciones en esta materia deberán aportar datos y mecanismos de comisión que puedan conectar directamente con la información y sean relevantes para el perito.

El autor Téllez (2009) afirmó como la doctrina y la jurisprudencia en la rama de derecho informático es escasa lo que origina una regulación muy imprecisa en los apartados de procedimientos y protocolos para el manejo de la información como actuación frente a este tipo de crímenes, pues la mayoría tiende a entender que, en un delito informático el daño siempre debe ser posible a determinarse en cuantía, lo cual en la práctica no puede configurarse ya que la vulneración a un sistema que permita acceder a los datos personales no una persona no genera un daño económico medible, por lo que las autoridades no podrán valorarlo adecuadamente, respecto a esto nacen otros puntos con severos vacíos legales como la apropiación de información, seguimiento de caudales, copia del material intelectual, video vigilancia entre otros. Sin duda el derecho busca simplificarse, sin embargo, no puede mantener esta óptica en escenarios que desconoce, ya que, se va a conducir a imprecisiones y riesgos para la sociedad con resultados altamente lesivos en la seguridad de los individuos.

Se considera pertinente considerar la variable de la persecución eficaz de los delitos de ciberdelincuencia, para ello el autor Temperini (2013) mencionó como es relevante para actuar en margen a la norma, esta debe existir y contemplar las variantes de la criminología cibernética, pero, ante un escenario con limitada regulación e imprecisa no es posible detectar la comisión de ilícitos, si no, esto origina un paraíso informático para la realización de conductas criminales, pues las tecnologías no deben ser vistas únicamente como un medio de comunicación, si

no, ante cada dispositivo y red se debe anticipar ante posibles vulneraciones criminales que puedan aprovecharlas para la sustracción de información y regularse.

Por ello Fernández (2011) mencionó como se debe realizar en todo país una homogenización de la normativa con la realidad en materia informática, esta debe prestar atención a la labor cooperativa con entidades privadas mayormente, pues estas generan un interés principal para la ciberdelincuencia y en la actuación se debe asegurar mantenerse a la vanguardia en conocimientos. Respecto a la región sudamericana se puede encontrar como su legislación nace a partir de la información vista y obtenida por convenios, mas no se adecua su configuración a la propia realidad de los países, lo que lleva a generar una deficiencia en la persecución eficaz del delito, desprotegiendo así a la víctima en su integridad como a su economía por la exposición a la que esta se puede encontrar.

Es aquí donde la persecución eficaz del delito tiene que romper con los moldes clásicos del derecho penal y centrarse en una vanguardia con alta competitividad para contrarrestar los cuadros de acción de la criminología informática y como base se deberá tener la Convención de Budapest, sin embargo, la adopción a la realidad dependerá de las necesidades de la población y de las investigaciones especializadas realizadas al interior del país.

Dada la antigüedad de la Convención y la evolución de las tecnologías es posible prever conductas actuales que para ese entonces no existían y pudieran considerarse delitos, para ejemplificar se menciona como el acceso ilícito será penado, sin embargo, en la actualidad es posible acceder a los sistemas lícitamente para recabar información, lo cual no genera una acción con responsabilidad criminal.

Es por esto es relevante la variante de la protección a los bienes jurídicos, siendo así, la autora Mayer (2017) expresó que, existe un interés relevante para proteger adecuadamente los bienes jurídicos en los delitos informáticos, principalmente porque en este tipo de delitos, los mismos puedes contenerse de modo tanto tangible como intangible, además, debe comprenderse su naturaleza de conectividad, esto quiere decir que, la información se encuentra no almacenada en un dispositivo físico, si no, es parte de un bloque electrónico con acceso a

Internet para lo que en una filtración o exposición no bastaría con la recuperación del dispositivo, si no, sería necesario el uso de técnicas informáticas avanzadas por parte de la autoridad para retirar esta información de los servidores, la misma podrá hacerse directamente o indirectamente, la primera se refiere a eliminar la información de los servicios en línea con el acceso a las cuentas, mientras las segundas hacen referencia al envío de solicitudes a las empresas que administran los medios informáticos para su pronta eliminación.

Entendiendo este preámbulo, la misma autora detalló como los bienes jurídicos serán los vinculados al libre desarrollo del individuo, esta cierta precisión general es la que se encuentra determinada en la escasa bibliografía, sin embargo, conforme a la realidad y avance de este proyecto es posible indicar que existe un daño patrimonial y violación de la privacidad, la primera porque el mantener cuentas informáticas en diversos servicios son parte de la propiedad, pues sobre esta se ejerce el uso y disfrute que se verá mermado ya que, el agresor hará uso de estos como poseedor, en un segundo punto se menciona la privacidad, pues el contenido en las cuentas se almacena bajo contraseña y forma parte de la esfera privada de la persona.

Según el autor Medina (2014) mencionó como el bien jurídico protegido debe entenderse desde dos aristas, la primera va a hacer relación a la vulnerabilidad cometida al sistema, pues está, es entendida como el ciberdelito y la segunda, es la base al contenido extraído o el daño causado, donde podría aplicarse la valoración tradicional del derecho, este ciberdelito es aquello que genera dificultad para su regulación, pues el sabotaje y violación de medios no serían los únicos métodos que generarían una vulnerabilidad en el sistema, esto se demuestra en los casos de espionaje o el empleo se software de terceros. Este tratamiento mostraría tanto un patrimonial para forzar la infraestructura como de violación a las telecomunicaciones.

Estas posturas para el autor Mata (2007), llevaron a afirmar la existencia de una teoría, la cual desarrolla un bien jurídico netamente informático y de nuevo carácter para regular, pues la actividad se realiza completamente en un sistema alejado de una concepción clásica de los bienes, esto marcaría una clara diferencia del delito informático en los accesos y el de fondo que causaría la pérdida o lesión,

por ello, es necesario impulsar la regulación de este nuevo bien jurídico denominado “seguridad en medios informáticos”.

Existe controversia según el autor Cárdenas (2008) quien afirmó como no existiría una lesión específica de un bien jurídico tutelado en los delitos informáticos, pues la informática vendría a ser la modalidad para la comisión del delito, donde es necesario únicamente valorar el resultado del daño y conceptuar el daño en los bienes jurídicos tradicionales como la privacidad o el patrimonio.

Pudiendo entender ambas posturas teóricas, se consideró importante valorar la posibilidad de la regulación del bien jurídico “seguridad en los medios informáticos” ya que, los delitos que emplean estos sistemas actúan en dos modos como parte de una conducta desagregada y posible a dividir en partes, donde en un primer momento se produce la violación de los sistemas informáticos y en un segundo, se accede al sistema a realizar la conducta criminal en la alteración, sustracción, manipulación, modificación o secuestro de la información. Este tratamiento exclusivo va a facilitar la creación de un marco legal ante el alarmante crecimiento de los delitos informáticos que permita actuar de manera oportuna y eficaz.

Es importante mostrar la postura del González (20014) quien mencionó como los delitos de carácter informático, comprometen la información vertida en los sistemas, pudiendo señalar que existe una falsedad documental y hacer de esta el bien jurídico protegido, pues el tráfico de la información que se generará será sobre la extraída ilícitamente.

La postura del autor anterior es un claro ejemplo de tratar de adaptar el derecho informático a la concepción del derecho clásico, lo que naturalmente va a generar deficiencias en el apartado práctico, prueba de ello es el número creciente de delitos informáticos y la poca actuación ideal sobre la materia. Por ejemplificar el supuesto de la falsedad de información, esta debe ser considerada como una suposición, pues extraer información de los sistemas tendría el mismo valor a la original almacenada, por lo que, la protección estaría incorrectamente inclinada a cuestionar su veracidad y no los modos de obtención.

Esto lleva a entender que, existe una necesaria protección en base a las siguientes categorías; software, Internet, funcionamiento de los sistemas e integridad de los datos.

En base a lo observado se considera relevante desarrollar las variables referentes a la afectación económica, psicológica y patrimonial donde Temperini (2014) explicó como el hombre requiere necesariamente de una identificación y a través de esta es que se da su reconocimiento en la sociedad, este mismo concepto debe extenderse al espacio informático donde el sujeto mantendrá una identidad propia, pues a través de los medios informáticos la persona desarrollará su vida privada, económica y social, bajo estas semejanzas es sumamente importante declarar que, el sujeto mantiene un aspecto económico en los medios informáticos a través de las cuentas bancarias y servicios financieros, privada en los almacenamiento de información y social a través de sus redes, por lo que una vulneración a estos sistemas va a lesionar gravemente a la persona, mermando su económica, deteriorando su estabilidad emocional y psicológica como comprometiendo información confidencial.

Según Federal Trade Commission (2012) explicó cómo las personas afectas por delitos informáticos en gran parte comprometieron su información personal y ante la imposibilidad de poder actuar la autoridad rápidamente debido a la alta carga de casos complejos se pudo determinar cómo generó daños al honor de las personas, la imagen pública de algunos e integridad lo que evidenciaría una alteración a la estabilidad psicológica de las personas, pues los ataques de pánico y ansiedad suelen ser figuras muy repetitivas en los casos.

El boletín mexicano que expidió La Cámara de Diputados (2011) mencionó como los delitos informáticos que más abundan suelen ser lo de robo de identidad, estos se presentan con la finalidad de suplantar al agraviado frente a entidades bancarias para retirar todos los ahorros, esto es un problema preocupante para el país del norte puesto que, las pérdidas al año suelen superar altamente los 8 millones de dólares, por lo que, la Cámara ve pertinente la reforma de los delitos penales que puedan ser susceptibles a realizarse en un entorno informático para proteger a la persona, en esta propuesta se acuerda que la pena máxima a aplicar

debe ser de hasta doce años, ello principalmente debido al grado de lesión bajo o nulo en fuerza que se ejerce sobre la persona y alto en cuanto a patrimonio.

En un aspecto muy relevante se considera a Olivera (2012) quien mencionó que en los delitos informáticos que afectan al patrimonio y este se encuentre al interior de cuentan bancarias, solo se logra recuperar el dinero del cincuenta y cuatro por ciento de los casos, lo que genera preocupación en cuanto a la eficiencia del derecho en este campo, por ello, se estima que son alrededor de 4 millones de dólares en pérdidas para la región latinoamericana y únicamente sobre los casos denunciados, esta falta de denuncia por las personas evidencia que, el actuar de las autoridades no siempre suele ser eficiente y renuncian a formalizar una denuncia.

De acuerdo al marco normativo: se tiene en cuenta El convenio Budapest, Conocido como el convenio sobre la ciberdelincuencia, realizado en el 2001 por iniciativa de la OCDE, sentó las principales bases legislación peruana en los delitos informáticos.

Respecto a Perú, este fue adherido en el año 2015, lo que permite pensar como en el año 2019 recién se ratifica la adhesión por el congreso, esto sin duda generó un atraso importante en la legislación nacional, sin embargo, este convenio permitió ser las bases fundamentales para la norma específica en ciberdelincuencia.

Según la Ley Nº 30096, Ley de delitos informáticos se presenta como aquella que busca tanto la prevención como sanción de los ilícitos que empleos mecanismo tecnológicos, para el cumplimiento de este objetivo es que se desarrollan diez tipos penales:

Como primer artículo se encuentra el acceso ilícito, este articulo va a sancionar con uno a cuatro años a aquellos sujetos que realicen vulneraciones de seguridad a un “sistema informático.” Además, en la normativa se regula la sanción para aquel que altera datos de sistemas informáticos, del mismo modo la proposición de actos sexuales contra menores en uso de medios tecnológicos y la interceptación de los datos informáticos, este mantiene verbos rectores muy distantes a las acciones de las prácticas comunes, se regula la interceptación de datos y las emisiones en fuentes electromagnéticas. Sobre la interceptación se

puede hacer una precisión, está en la práctica no puede ser entendida como una interceptación, principalmente porque el acceso a los datos suele darse cuando estos ya se encuentren alojados en un servidor y respaldados para poder ser copiados, pues la interceptación haría referencia a una conducción de la información hacia una fuente distinta durante la emisión.

En relación al derecho comparado: Colombia, En su cuerpo normativo penal se encuentra el artículo 269 con un número amplio de incisos que regula el forzamiento de sistemas informáticos con una sanción privativa de la libertad de hasta cuatro años, la normativa colombiana además menciona la obstaculización al acceso de los sistemas, bases de datos secuestradas, la captura de datos informáticos y el uso de programas para fines ilícitos. Finalmente, se puede resaltar como en el apartado de interceptación, esta se refiere a acceder a ellos desde un origen y además interceptar redes, esto agrega un punto interesante con más precisión en comparación de la regulación peruana.

Chile: El país cuenta con una dependencia especializada lo que le permite tener leyes específicas, en razón a ello se cuenta con la 20.009 referida al uso de información fraudulenta para realizar pagos como de fraudes en las transacciones y la 19.223 en razón a los delitos informáticos, estos se van a relacionar sobre los ilícitos de violencia, violación de los secretos de las telecomunicaciones y alteración del normal funcionamiento de los sistemas.

Paraguay: Los delitos de materia informática se encuentran vistos en el cuerpo normativo penal donde se regula al igual que los anteriores países el acceso indebido, alteración de datos falsificación de información relacionada a materia financiera y estafas. Estos son los principales bloques en los que se pueden encontrar los delitos informáticos y su especialización por sectores, esto se debe al trabajo en conjunto con la cooperación internacional desde el 2017 con su adhesión al convenio de Budapest.

Un aspecto importante de la nación es su elaborado Manual Policial de Criminalística que regula el levantamiento de evidencia y primeras investigaciones donde para el análisis se dota al personal de realizar backup de la información a fin de mantener su originalidad.

III. METODOLOGÍA

3.1. Tipo y Diseño de Investigación

La presente investigación fue de enfoque cuantitativo, por lo que el autor Sánchez (2019), precisó que los datos que se obtuvieron surgen de una conducta continua, que busca ubicar las derivaciones del escenario en el cual se está desarrollando actualmente.

El mencionado trabajo fue de tipo básico debido a que buscamos obtener nuevos conocimientos científicos, debido a que buscamos establecer los actos de investigación durante la etapa de investigación preparatoria, incide en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, en el Distrito Fiscal de Lima

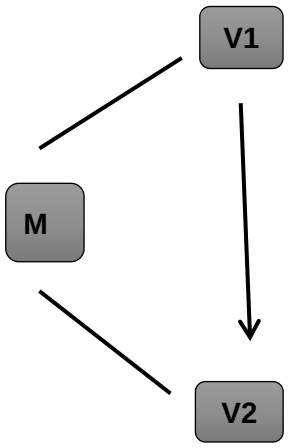
Es de Nivel descriptivo porque buscamos describir el fenómeno objeto de estudio, al respecto Tamayo (2003) señaló que, en una investigación descriptiva, se examina el fenómeno que esta materia de estudio.

El diseño es transeccional y no experimental

El diseño de estudio, es no experimental corte transversal, dado que no altera las variables para su estudio, es decir no habrá experimento alguno al respecto y será trasversal porque el estudio es el presente año 2021.

Por ello, el diseño postula estudia la relación causal de las variables de causa efecto, señala Mejía (2005).

Gráficamente se muestra de la siguiente manera:



Dónde:

V1: Variable independiente Actos de investigación.

V2: Variable dependiente Eficacia en persecución delito de ciberdelincuencia.

M: Muestra.

3.2. Variables y Operacionalización:

Variable 1: Actos de investigación

Definición conceptual: Actuaciones que permite recabar pruebas en la etapa de investigación preparatoria.

Definición operacional: (Rosas, 2012) Los actos de investigación son todos los actos procesales que realiza el fiscal y la policía en procura de recabar o recopilar los elementos de prueba o de convicción que lleven a esclarecer debidamente los hechos.

Variable 2: Persecución eficaz en los delitos de Ciberdelincuencia

Definición conceptual: Persecución eficaz en los delitos de Ciberdelincuencia surge una protección a los bienes jurídicos protegidos.

Definición operacional: (Ministerio Publico 2020) La afectación de la víctima depende de la modalidad del delito informático; es así que la afectación puede ser económica o patrimonial, pero también puede ser moral o psicológica. En este último caso, la afectación también podría estar generada por la pérdida de sus cuentas en redes sociales y por la frustración al no poder identificar a los autores de los delitos.

Para poder medir la variable actos de investigación se ha tomado como dimensiones, recopilar elementos de convicción por parte del fiscal y recopilar elementos de convicción por parte de la policía.

De igual manera, se han determinado para la variable persecución eficaz en los delitos de Ciberdelincuencia como dimensiones, afectación económica y afectación psicológica.

La matriz de operacionalización de variables se encuentra en el Anexo 1.

3.3. Población, muestra y muestreo

La población estuvo compuesta por los 180 Fiscales penales y adjuntos provinciales del Distrito Fiscal de Lima.

Asimismo, existieron 200 abogados que laboran del Distrito Fiscal de Lima. En ese sentido, Tamayo (1997) refirió que la población es la totalidad de las unidades de investigación, asimismo 80 policiales que laboran en el área de delitos informáticos

La muestra es no probabilística, así lo explico Hernández, Fernández y Baptista (2014) que señalaron que la muestra es la porción de unidades de análisis del cual se reciben los datos, el mismo que debe ser representativo.

Para los operadores – fiscales, abogados y policías – se aplicó la técnica del muestreo de la bola de nieve, es decir, que se utilizó las recomendaciones: En ese sentido, la muestra que se aplicó fue la siguiente:

Tabla 1

Distribución de la muestra

Sujetos	Número	Total
Fiscales	15	15
Efectivos policiales	15	15
Abogados patrocinantes	20	20
		50

***Nota**: fuente de elaboración propia*

3.4. Técnicas e instrumentos de recolección de datos

Se optó por la técnica de la encuesta aplicando el cuestionario semi estructurado a escala Likert, por lo cual es fundamental para recoger información de naturaleza cuantitativa, por lo que resulta importante registrar los datos organizados, conforme lo señala Gómez (2016).

El instrumento de recolección de dato fue el cuestionario que estuvo conformado por 12 interrogantes para medir la variable independiente (actos de investigación) y 13 interrogantes para medir la variable dependiente (persecución eficaz en los delitos de Ciberdelincuencia).

Sobre la validez del instrumento, fue realizado a través del juicio de expertos, donde calificaron cada ítem de todos los instrumentos, la calificación que se obtuvo fue de tener un instrumento aplicable. A continuación, se presenta la relación de expertos y su calificación:

Tabla 2

Juicio de experto

Experto	Especialidad	Calificación
Experto 1	Temático	Aplicable
Experto 2	Temático	Aplicable
Experto 3	Metodólogo	Aplicable

Con respecto a la confiabilidad, participaron 50 participantes para lo cual se procedió a evaluar su coeficiente de confiabilidad del instrumento a través del alfa de Cronbach.

3.5. Procedimientos

Después de haber solicitado los permisos a las autoridades correspondientes se coordinó con los sujetos para poder hacer la aplicación respectiva mediante programa SPSS26.

Para el procedimiento de recolección de data e información, se procedió a efectuar encuestas por un lado a los fiscales penales y por otro lado a los efectivos policiales y los abogados defensores, lo cual arrojó los cuadros estadísticos que son expuestos en la presente investigación.

Se debe aplicar el cuestionario semi estructurado a escala Likert, lo cual se efectuará en base a los indicadores planteados en la matriz, tal como lo señaló

Gómez (2016). Tanto los cuadros como los gráficos fueron objeto de interpretación y análisis.

3.6. Método de análisis de datos

Para el método de análisis de datos se ha tenido en cuenta la obtención de una base de datos producto de los instrumentos aplicados, en función de ello se ha realizado el análisis descriptivo de las tablas y figuras arrojadas por el programa estadístico SPS26 con motivo de las encuestas realizadas lo cual sirvió para efectuar la comprobación de la hipótesis a través de la prueba no paramétrica de regresión logística ordinal.

3.7. Aspectos Éticos

Con relación al aspecto ético, se ha ceñido en estricto procedimiento, de acuerdo a las indicaciones de la guía de la elaboración APA 7 edición y de la Universidad César Vallejo, el tratamiento de la información ha sido estrictamente confidencial, así como también se ha tenido en consideración las referencias y respetando el no plagio y similitud.

IV. RESULTADOS

4.1 Resultados descriptivos

Tabla 3

Niveles frecuenciales de la variable actos de investigación

		Frecuencia	Porcentaje	Porcentaje válido
Válido	Malo	4	8,0	8,0
	Regula	20	40,0	40,0
	Bueno	26	52,0	52,0
	Total	50	100,0	100,0

Figura 1

Niveles de los actos de investigación

De los resultados descriptivos se señala que el 52% de los encuestados afirmaron que de los actos de investigación, realizan en un nivel bueno, el 40% afirman que los actos de investigación se ejecutan en un nivel regular y el 8% mencionan que dichos actos están en un nivel malo en el Distrito Fiscal de Lima, 2021.

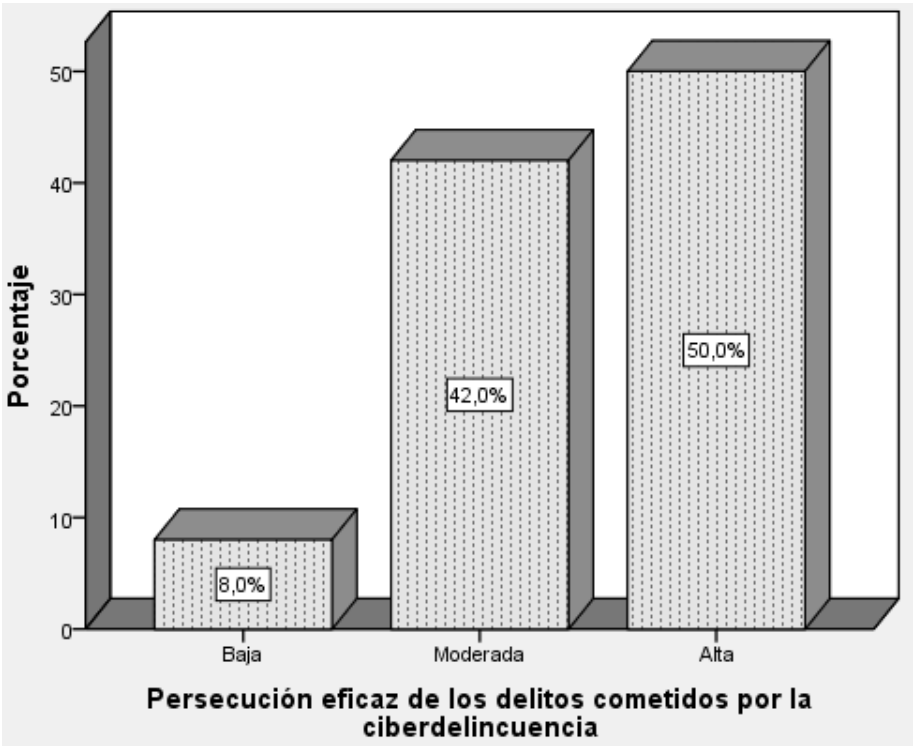
Tabla 4

Niveles frecuenciales de la persecución eficaz de los delitos cometidos por la ciberdelincuencia

		Frecuencia	Porcentaje	Porcentaje válido
Válido	Baja	4	8,0	8,0
	Moderada	21	42,0	42,0
	Alta	25	50,0	50,0
	Total	50	100,0	100,0

Figura 2

Niveles de la persecución eficaz de los delitos cometidos por la ciberdelincuencia



Asimismo, en relación a los resultados descriptivos de señala que el 50% de los encuestados afirmaron la persecución de los delitos cometidos por la ciberdelincuencia se ejecutan en un nivel alta, asimismo el 42% mencionaron que dicha persecución se lleva a cabo en un nivel moderado y solo el 8% mencionaron que la persecución se ejecuta en un nivel bajo el Distrito Fiscal de Lima, 2021.

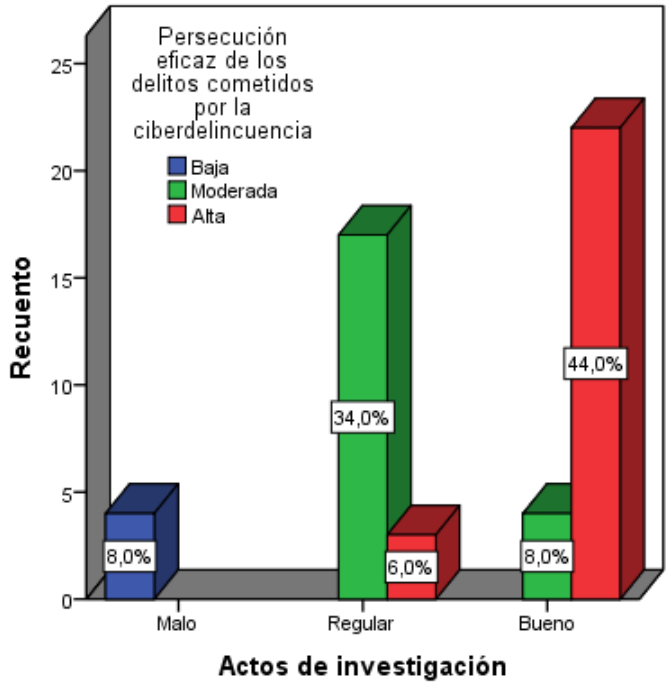
Tabla 5.

Resultados de contingencia de Actos de investigación en la Persecución eficaz de los delitos cometido por la ciberdelincuencia

			Persecución eficaz de los delitos cometido por la ciberdelincuencia			Total
			Baja	Moderada	Alta	
Actos de investigación	Malo	Recuento	4	0	0	4
		% del total	8,0%	0,0%	0,0%	8,0%
	Regular	Recuento	0	17	3	20
		% del total	0,0%	34,0%	6,0%	40,0%
	Bueno	Recuento	0	4	22	26
		% del total	0,0%	8,0%	44,0%	52,0%
Total		Recuento	4	21	25	50
		% del total	8,0%	42,0%	50,0%	100,0%

Figura 3

Resultados de contingencia de las variables de estudio



De acuerdo al resultado de contingencia se visualizó la incidencia de la variable independiente con respeto a la variable dependiente, puesto que el 44% de los encuestados afirman que los actos de investigación son de nivel bueno frente a un nivel alto de los actos de investigación persecución eficaz de los delitos cometido

por la ciberdelincuencia, asimismo otros 34% afirman que los actos de investigación se sitúa en un nivel regular frente a una persecución de nivel regular, asimismo 8% afirmaron que los actos de investigación está en un nivel malo cuando la persecución de los delitos de cometidos por la ciberdelincuencia tiene un nivel baja.

4.2. Resultado inferencial: prueba de hipótesis

De acuerdo a los resultados obtenidos del instrumento de escala politómica que mide la incidencia de los actos de investigación en la persecución de los delitos cometidos por la ciberdelincuencia en el Distrito Fiscal de Lima, 2021, que de acuerdo a los resultados de la prueba de bondad de ajuste se indica que el modelo a usar es la Regresión Logística Ordinal para el análisis inferencial de la presente investigación. A continuación, se presenta la tabla de la prueba referida.

Tabla 6

Resultado de la prueba de normalidad por Shapiro-Wilk

Pruebas de normalidad[a,c,d,e]

		Shapiro-Wilk		
	Actos de investigación			
Persecución eficaz de los delitos cometido por la ciberdelincuencia	Regular	,433	20	,000
	Bueno	,436	26	,000
Afectación económica	Regular	,351	20	,000
Afectación psicológica	Regular	,433	20	,000
	Bueno	,619	26	,000

Tabla 7

Prueba de bondad de ajuste de los actos de investigación en la persecución de los delitos cometidos por la ciberdelincuencia

	Bondad de ajuste		
	Chi-cuadrado	gl	Sig.
Pearson	2,191	2	1,000
Desvianza	4,383	2	1,000

Función de enlace: Logit.

Los resultados de la prueba de bondad de ajuste señalan un Chi cuadrado de 2,191 donde el rechazo es de la hipótesis alterna y aceptar la nula, tal es así que es posible referirse que el modelo empleado para la prueba estadística es la regresión

logística ordinal, siendo la acertada para la prueba de hipótesis.

Tabla 8

Resultados de la variabilidad de la persecución de los delitos cometidos por la ciberdelincuencia.

Los actos de investigación inciden en la	Cox y Snell	Nagelkerke	McFadden
Persecución eficaz de los delitos cometido por la ciberdelincuencia.	0.686	0.818	0.635
Afectación económica	0.794	0.953	0.883
Afectación psicológica	0.595	0.712	0.501

A consecuencia de los resultados de la prueba de variabilidad del Pseudo R Cuadrado que se visualizan la dependencia de la variable persecución eficaz de los delitos cometido por la ciberdelincuencia por la persecución eficaz, donde la inestabilidad referida por el Nagelkerke es del 81,8% por los actos de investigación, asimismo la dependencia de la afectación económica es de 95,3% por los actos de investigación, y finalmente la inestabilidad de la afectación psicológico referida por el Nagelkerke es del 71,2% por los actos de investigación en el Distrito Fiscal de Lima, 2021.

Prueba de hipótesis general

H0: Los actos de investigación no inciden en la persecución de los delitos cometidos por la ciberdelincuencia en el Distrito Fiscal de Lima, 2021.

Ha: Los actos de investigación inciden en la persecución de los delitos cometidos por la ciberdelincuencia en el Distrito Fiscal de Lima, 2021

Tabla 9

Resultado del ajuste de los actos de investigación en la persecución de los delitos cometidos por la ciberdelincuencia.

Información de ajuste de los modelos

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	57,996			
Final	,000	57,996	2	,000

Función de enlace: Logit.

La derivación responde del ajuste de modelo los actos de investigación en la persecución de los delitos cometidos por la ciberdelincuencia que tiene un Chi cuadrado de 57,996y un P_valor de 0,000 frente, 0,001, lo que conllevó a rechazar la hipótesis nula, por lo que las variables no son independientes existe incidencia de la variable actos de investigación en la persecución de los delitos cometidos por la ciberdelincuencia en el Distrito Fiscal de Lima, 2021.

Tabla 10

Estimaciones de variabilidad de los actos de investigación en la persecución de los delitos cometidos por la ciberdelincuencia.

Estimaciones de parámetro

							Intervalo de confianza al 95%	
		Estimación	Error estándar	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[per_ef_delit_ciberd = 1]	-22,005	2355,745	,000	1	,993	-4639,180	4595,169
	[per_ef_delit_ciberd = 2]	-1,705	,544	9,836	1	,002	-2,770	-,639
Ubicación	[actos_invest=1]	-40,452	5586,630	,000	1	,994	-10990,046	10909,142
	[actos_invest=2]	-3,439	,829	17,203	1	,000	-5,065	-1,814
	[actos_invest=3]	0[a]	.	.	0	.	.	.

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

En relación a la prueba de hipótesis general se determina que las Los actos de investigación inciden en la persecución de los delitos cometidos por la ciberdelincuencia, por lo que el resultado de Wald es de 17,203 mayor al punto de corte que es 4 para el modelo; asimismo tiene una significancia de 0,000< α:0,001 donde conllevó al rechazo de la hipótesis nula por la innegable incidencia de la persecución de los delitos cometidos por la ciberdelincuencia en el Distrito Fiscal de Lima, 2021, que tiene un porcentaje Wald de 9,836> 4 con una significancia de 0,002< α:0,05, puesto que cuanto más regular sean los actos de investigación mucho más moderado será de la persecución de los delitos cometidos por la ciberdelincuencia.

Prueba de hipótesis específica 1

H0: Los actos de investigación no inciden en la afectación económica por la persecución de los delitos cometidos por la ciberdelincuencia en el Distrito Fiscal de Lima, 2021.

Ha: Los actos de investigación inciden en la afectación económica por la persecución de los delitos cometidos por la ciberdelincuencia en el Distrito Fiscal de Lima, 2021.

Tabla 11

Resultado del ajuste de los actos de investigación en la afectación económica

Información de ajuste de los modelos

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	78,961			
Final	,000	78,961	2	,000

Función de enlace: Logit.

Los resultados son del ajuste de modelo los actos de investigación en la afectación económica que tiene un Chi cuadrado de 78,971 y un P_valor de 0,000 frente, 0,001, lo que conllevó a rechazar la hipótesis nula, por lo que se muestra que las variables no son independientes existe incidencia de la variable actos de investigación en la afectación económica en el Distrito Fiscal de Lima, 2021.

Tabla 12

Estimaciones de variabilidad de los actos de investigación en la afectación económica

Estimaciones de parámetro

							Intervalo de confianza al 95%	
		Estimación	Error estándar	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[Afect_económ = 1]	-37,623	2119,006	,000	1	,986	-4190,797	4115,552
	[Afect_económ = 2]	-18,123	1690,005	,000	1	,991	-3330,472	3294,226
Ubicación	[actos_invest=1]	-55,114	3790,042	,000	1	,988	-7483,461	7373,232
	[actos_invest=2]	-20,320	1690,005	,000	1	,990	-3332,670	3292,029
	[actos_invest=3]	0[a]	.	.	0	.	.	.

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

En relación a la prueba de hipótesis específica 1 se determina que los actos de investigación inciden en la afectación económica, por lo que el resultado de Wald es de 3790,042 mayor al punto de corte que es 4 para el modelo; asimismo tiene una significancia de 0,000< α:0,001 donde conllevó al rechazo de la hipótesis nula

por la innegable incidencia de los actos de investigación en la afectación económica del distrito Fiscal de Lima, 2021, que tiene un porcentaje Wald de 2119,006> 4 con una significancia de 0,002< α:0,001, puesto que cuanto más malo sean los actos de investigación la afectación económica será más bajo.

Prueba de hipótesis específica 2

H0: Los actos de investigación no inciden en la afectación psicológica por la persecución de los delitos cometidos por la ciberdelincuencia en el Distrito Fiscal de Lima, 2021.

Ha: Los actos de investigación inciden en la afectación psicológica por la persecución de los delitos cometidos por la ciberdelincuencia en el Distrito Fiscal de Lima, 2021.

Tabla 13

Resultado del ajuste de los actos de investigación en la afectación psicológica

Información de ajuste de los modelos

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	45,200			
Final	,000	45,200	2	,000

Función de enlace: Logit.

Asimismo, las derivaciones son del ajuste de modelo los actos de investigación en la afectación psicológica que tiene un Chi cuadrado de 45,200 y un P_valor de 0,000 frente, 0,001, lo que conllevó a rechazar la hipótesis nula, por lo que se muestra que las variables no son independientes existe incidencia de la variable actos de investigación en la afectación económica en el Distrito Fiscal de Lima, 2021.

Estimaciones de parámetro

							Intervalo de confianza al 95%	
		Estimación	Error estándar	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[afec_psicolg = 1]	-20,087	1597,830	,000	1	,990	-3151,777	3111,603
	[afec_psicolg = 2]	-,470	,403	7,359	1	,004	-1,260	,320
Ubicación	[actos_invest=1]	-37,595	3547,922	,000	1	,992	-6991,394	6916,204
	[actos_invest=2]	-2,205	,745	8,763	1	,003	-3,664	-,745
	[actos_invest=3]	0[a]	.	.	0	.	.	.

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

En relación a la prueba de hipótesis específica 2 se determina que los actos de investigación inciden en la afectación psicológica, por lo que el resultado de Wald es de 8,763 mayor al punto de corte que es 4 para el modelo; asimismo tiene una significancia de 0,003< α:0,005 donde conllevó al rechazo de la hipótesis nula por la innegable incidencia de los actos de investigación en la afectación psicológica del distrito Fiscal de Lima, 2021, que tiene un porcentaje Wald de 7,359> 4 con una significancia de 0,004< α:0,001, puesto que cuanto más regular sean los actos de investigación la afectación psicológica será más moderada..

V. DISCUSIÓN

Al momento de efectuar la discusión, se debe precisar que los resultados deben ser contrastados con las bases teóricas y las investigaciones señalan lo siguiente:

En relación al objetivo general, se estableció que los actos de investigación durante la etapa de investigación preparatoria inciden significativamente en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, tal como se determinó, por lo que el resultado de Wald es de 17,203 mayor al punto de corte que es 4 para el modelo; asimismo tiene una significancia de 0,000< α:0,001 donde conllevó al rechazo de la hipótesis nula por la innegable incidencia de la persecución de los delitos cometidos por la ciberdelincuencia en el Distrito Fiscal de Lima, 2021, que tiene un porcentaje Wald de 9,836> 4 con una significancia de 0,002< α:0,05, puesto que cuanto más regular sean los actos de investigación mucho más moderado será de la persecución de los delitos cometidos por la ciberdelincuencia, ya que la mayoría de los encuestados respaldaron dicha afirmación, en ese sentido debemos destacar que ello fue corroborado por los sostenido por Ramírez y Castro (2018) quienes señalaron que para obtener un desarrollo en la sociedad las personas requieren estar a la vanguardia de las nuevas tecnologías, pues están proporcionan facilidades en cuanto a la relación humana y puestos laborales, lo cual los convierte en herramientas sumamente necesarias para el acceso a la información. Esta alta dependencia es lo que convierte a estos dispositivos en los blancos preferidos de ataques cibernéticos, pues en ellos se almacena información personal de carácter social, laboral y económico, con lo que es un importante bloque de información. Siendo así, producto del avance social el derecho se va adaptando a regular estos nuevos bienes y es que recoge el apartado de ciberdelincuencia, las conductas criminales destinadas al secuestro de información, extorsión, afección de la libertad y el acceso a las cuentas bancarias. Esto sirvió como precedente para el Ministerio de Telecomunicaciones en la creación de la Ley 1273 que se destina a facilitar tanto personal como tecnología para la cooperación con el Poder Judicial a fin de mantener un personal capacitado, este trabajo en conjunto desarrolló las cadenas de custodia, pues la información informática a diferencia de la física, puede ser

fácilmente manipulada por lo que, el valor probatorio de esta debe considerarse por encima de la física, lo que genera un tratamiento distinto y prioritario en las actuaciones, sin embargo, esta cooperación se limite a la misma, no extiende manual de procedimiento ni protocolos, por lo que, las cadenas de custodia van a depender mucho del personal a cargo y es posible prever comúnmente un deterioro o extravío de la evidencia.

Lo expuesto también se corrobora con lo señalado por Cárdenas (2008) quien afirmó como no existiría una lesión específica de un bien jurídico tutelado en los delitos informáticos, pues la informática vendría a ser la modalidad para la comisión del delito, donde es necesario únicamente valorar el resultado del daño y conceptuar el daño en los bienes jurídicos tradicionales como la privacidad o el patrimonio. Pudiendo entender ambas posturas teóricas, se considera importante valorar la posibilidad de la regulación del bien jurídico “seguridad en los medios informáticos” ya que, los delitos que emplean estos sistemas actúan en dos modos como parte de una conducta desagregada y posible a dividir en partes, donde en un primer momento se produce la violación de los sistemas informáticos y en un segundo, se accede al sistema a realizar la conducta criminal en la alteración, sustracción, manipulación, modificación o secuestro de la información. Este tratamiento exclusivo va a facilitar la creación de un marco legal ante el alarmante crecimiento de los delitos informáticos que permita actuar de manera oportuna y eficaz.

En relación al primer objetivo específico, se demostró que la recopilación de elementos de convicción por parte del fiscal incide negativamente en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, en el Distrito Fiscal de Lima, 2021, donde el 51.52% de los encuestados respaldaron la referida afirmación, debemos precisar que estos resultados, guardan relación con la investigación como Huarcaya (2021), quien señaló que el crimen informático organizado presenta una alta complejidad sobre el desarrollo de sus actividades, lo que impide una respuesta estatal efectiva, pues una posible intervención sería imposible de realizarse por el poco abordaje en la materia legal y encontraría conflictos con otros derechos. La falta de normas en este apartado genera un campo libre para el crecimiento de los crímenes organizados en materia informática, pues como principal objetivo se

tienen los datos personales, sin embargo, estos no son sustraídos, si no, copiados en un dispositivo de almacenamiento y empleando mecanismos como puertas bajas o puertos abiertos, no se considera para el país legalmente como una violación a alguna norma. Lo que podría generar un ilícito es la comercialización de la información y las extorsiones a las que deriven, ya que, estas conductas serían las únicas vistas como lesivas al ordenamiento jurídico.

Los resultados de la problemática advertida se sustentan como fuente teórica en Según la Ley Nº 30096, Ley de delitos informáticos se presenta como aquella que busca tanto la prevención como sanción de los ilícitos que empleos mecanismo tecnológicos, para el cumplimiento de este objetivo es que se desarrollan diez tipos penales. Asimismo, se destaca como primer artículo se encuentra el acceso ilícito, este articulo va a sancionar con uno a cuatro años a aquellos sujetos que realicen vulneraciones de seguridad a un "sistema informático." Además, en la normativa se regula la sanción para aquel que altera datos de sistemas informáticos, del mismo modo la proposición de actos sexuales contra menores en uso de medios tecnológicos y la interceptación de los datos informáticos, este mantiene verbos rectores muy distantes a las acciones de las prácticas comunes, se regula la interceptación de datos y las emisiones en fuentes electromagnéticas. Sobre la interceptación se puede hacer una precisión, está en la práctica no puede ser entendida como una interceptación, principalmente porque el acceso a los datos suele darse cuando estos ya se encuentren alojados en un servidor y respaldados para poder ser copiados, pues la interceptación haría referencia a una conducción de la información hacia una fuente distinta durante la emisión.

Con relación al segundo objetivo específico, se demostró que la recopilación de elementos de convicción por parte de la policía incide negativamente en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, en el Distrito Fiscal de Lima, 2021, habiendo obtenido un respaldo de los encuestados en un (41.73%).

Los resultados también guardan relación con las investigaciones realizado por Nobles et al (2020) quien señaló como las actuaciones durante los actos de investigación deben considerarse que esta tendrá un valor informático, es decir,

conceptúa a la prueba electrónica por lo que el enfoque en relación a las pericias normales debe cambiar sus planteamientos, principalmente desde el apartado metodológico, la recolección de esta información va a referirse a los criterios que se emplearan para lo mismo, la definición y conceptualización serán elementos principales para mantener una autenticidad en unos datos tan frágiles, la confianza de la fuente de la información y la necesidad de relación con el suceso para poder fundar una hipótesis y demostrarla. Estos resultados también guardan relación con la investigación de Quispe et al., (2019) quienes mencionaron que las practicas forenses en informática deberán analizar la información con un backup a fin de mantener un respaldo original y no deteriorar la información como poder visualizar en un futuro el estado intacto de lo encontrado para contrastarlo, principalmente se requiere esto debido a que, cuando se realiza la apertura de archivos estos suelen registrar hora y fecha de su acceso, entonces después de una pericia sin un backup genera un deterioro completo de la prueba, tanto en su originalidad como en su credibilidad, pues el solo acceso posterior ya podría ser suficiente como para aducir a una modificación del contenido de los archivos, siendo esto en materia legal un motivo suficiente para restar credibilidad y cuestionar la prueba.

Estos resultados tienen como fuente teórica lo señalado por Del Río (2006) quien explicó cómo la policía actúa directamente en recoger testimonio y realizar peritaje sobre el material tecnológico que no contemple un acceso dificultoso y se limite a la observación del contenido y estado, sin embargo, menciona como es normal encontrarse con un lenguaje extraño en la informática y donde en materia de criminal el lenguaje predominante es el inglés con un abundante número de contracciones, lo que para la labor se considera una brecha no solo de conocimiento, si no también, de comunicación y preparación pues las actividades tendrán que ser trasladas a la fiscalía para actuar con mayor especialidad y conocimiento. Como se ha señalado se menciona como es de preocupación que, las comisarias que cuentan con personal policial especializado en materia informática son muy escasas, por lo que, el funcionamiento de su actuar no es suficiente para realizar una adecuada gestión de la información como del estado en el que se encuentra y ante una posible manipulación inadecuada que pueda deteriorar completamente su valor probatorio como su contenido.

Con relación al tercer objetivo específico, se determinó que la recopilación de elementos de convicción por parte del fiscal incide en el patrimonio de las víctimas en los delitos cometidos por la ciberdelincuencia, tal como se determinó, por lo que el resultado de Wald es de 3790,042 mayor al punto de corte que es 4 para el modelo; asimismo tiene una significancia de 0,000< α:0,001 donde conllevó al rechazo de la hipótesis nula por la innegable incidencia de los actos de investigación en la afectación económica del distrito Fiscal de Lima, 2021, que tiene un porcentaje Wald de 2119,006> 4 con una significancia de 0,002< α:0,001, puesto que cuanto más malo sean los actos de investigación la afectación económica será más bajo,ya que la mayoría de los encuestados respaldaron tal afirmación.

Los resultados guarda relación con lo afirmado por considera a Olivera (2012) quien mencionó que en los delitos informáticos que afectan al patrimonio y este se encuentre al interior de cuentan bancarias, solo se logra recuperar el dinero del cincuenta y cuatro por ciento de los casos, lo que genera preocupación en cuanto a la eficiencia del derecho en este campo, por ello, se estima que son alrededor de 4 millones de dólares en pérdidas para la región latinoamericana y únicamente sobre los casos denunciados, esta falta de denuncia por las personas evidencia que, el actuar de las autoridades no siempre suele ser eficiente y renuncian a formalizar una denuncia. De acuerdo al marco normativo: se tiene en cuenta El convenio Budapest, Conocido como el convenio sobre la ciberdelincuencia, realizado en el 2001 por iniciativa de la OCDE, sentó las principales bases legislación peruana en los delitos informáticos.

Con relación al cuarto objetivo específico, se demostró que la recopilación de elementos de convicción por parte de la policía incide en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, tal como se determinó por lo que el resultado de Wald es de 8,763 mayor al punto de corte que es 4 para el modelo; asimismo tiene una significancia de 0,003< α:0,005 donde conllevó al rechazo de la hipótesis nula por la innegable incidencia de los actos de investigación en la afectación psicológica del distrito Fiscal de Lima, 2021, que tiene un porcentaje Wald de 7,359> 4 con una significancia de 0,004< α:0,001, puesto que cuanto más regular sean los actos de investigación la afectación psicológica será más

moderada.ya que la mayoría de los encuestados respaldaron tal afirmación, ya que la mayoría de los encuestados respaldaron tal afirmación.

Los resultado guardan relación con lo señalado por la Federal Trade Commission (2012) quien señaló cómo las personas afectas por delitos informáticos en gran parte comprometieron su información personal y ante la imposibilidad de poder actuar la autoridad rápidamente debido a la alta carga de casos complejos se pudo determinar cómo generó daños al honor de las personas, la imagen pública de algunos e integridad lo que evidenciaría una alteración a la estabilidad psicológica de las personas, pues los ataques de pánico y ansiedad suelen ser figuras muy repetitivas en los casos.

VI. CONCLUSIONES

Primera: Respecto al objetivo general, se logró establecer que los actos de investigación durante la etapa de investigación preparatoria inciden en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, Distrito Fiscal de Lima, 2021, debido a que resultados de la prueba de bondad de ajuste señalan un Chi cuadrado de 2,191 donde el rechazo es de la hipótesis alterna y aceptar la nula, tal es así que es posible referirse que el modelo empleado para la prueba estadística con es la regresión logística ordinal es acertada para la prueba de hipótesis

Segunda: Respecto al primer objetivo específico, se estableció que la incorporación de la recopilación de elementos de convicción por parte del fiscal incide en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, Distrito Fiscal de Lima, 2021. Identificación de la dirección IP (internet Protocolo) de dispositivos informáticos siendo el indicador Visualización de los mensajes de redes sociales (43.86%) y la Visualización de los mensajes correos electrónicos (65.21%).

Tercera: Respecto al segundo objetivo específico, se estableció que la incorporación la recopilación de elementos de convicción por parte de la policía incide en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, Distrito Fiscal de Lima, 202, siendo los indicadores que fueron respaldados Peritajes sobre equipos celulares (48.21%), Pericia informática forense (53.29%) y Peritajes sobre otros equipos de informática (64.83%).

Cuarta: Respecto al tercero objetivo específico, se estableció que la recopilación de elementos de convicción por parte del fiscal incide en el patrimonio de las víctimas en los delitos cometidos por la ciberdelincuencia en el Distrito Fiscal de Lima, debido a que esto debido a que son del ajuste de modelo los actos de investigación en la afectación económica que tiene un Chi cuadrado de 78,971 y un P_valor de 0,000 frente, 0,001, lo que conllevó a rechazar la hipótesis

nula, por lo que se muestra que las variables no son independientes existe incidencia de la variable actos de investigación en la afectación económica en el Distrito Fiscal de Lima

Quinta: Respecto al cuarto objetivo específico, se estableció la manera en que la recopilación de elementos de convicción por parte de la policía incide en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, que las derivaciones son del ajuste de modelo los actos de investigación en la afectación psicológica que tiene un Chi cuadrado de 45,200 y un P_valor de 0,000 frente, 0,001, lo que conllevó a rechazar la hipótesis nula, por lo que se muestra que las variables no son independientes existe incidencia de la variable actos de investigación en la afectación psicológica

VII. RECOMENDACIONES

Primera: Al Ministerio de Economía y Finanzas, estando que los actos de investigación durante la etapa de investigación preparatoria inciden negativamente en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, es que se requiere mayor presupuesto para la cartera del Ministerio del Interior y Ministerio Público a efectos de dotar logísticamente a dichas áreas, de tal manera que permita llevar una actividad de investigaciones eficaz.

Segunda: Al Ministerio público, realizar capacitaciones a los fiscales penales y fiscalías especializadas en delitos de ciberdelincuencia ya sea a través de la escuela del Ministerio Público y cualquier otra entidad de alta acreditación en tecnología, con la finalidad de profundizar el estudio del manejo de técnicas de investigación, lo cual permitir realizar una actividad probatoria prolija de cara a la identificación de los autores.

Tercero: Al Ministerio del interior, realizar capacitaciones a los efectivos policiales por la escuela de capacitación de la Policía Nacional del Perú, por parte de peritos especializados en el manejo de técnicas de investigación en el área cibernético, lo cual permitir realizar un menor manejo de las pesquisas.

Cuarta: A la Superintendencia de Banca y Seguros, emitir directivas para que los Bancos puedan mejorar sus estándares de seguridad de las páginas electrónicas, de tal manera que no se de vulnerabilidad a los clientes, ya que se ha demostrado que los ciberdelincuentes apuntan a esas páginas web.

Quinta: Al Ministerio Público, efectuar charlas de concientización a la ciudadanía en colaboración con las Municipalidades, a efectos de concientizar el manejo de las herramientas informáticas, con la finalidad de prevenir el acceso a ella de manera responsable en aras de resguardar su información personal

REFERENCIAS

Avast Academy (2020). Qué es el spam: guía esencial para detectar y prevenir el spam.

Canedo, A. (2010). La informática forense y los delitos informáticos. Revista Pensamiento Americano.

Cámara de Diputados. (2011). Boletín 4520: El robo de identidad origina en México pérdidas anuales por 9 millones de dólares.

Cárdenas, C. (2008). El lugar de comisión de los denominados ciberdelitos. Política Criminal.

Congreso de Naciones Unidas sobre Prevención del delito y Tratamiento del delincuente. (2000).

Del Río, C. (2006). La persecución y sanción de los delitos informáticos.

Federal trade commission. (2012). FTC Issues final commission report of protecting consumer privacy.

Fernandez, J. (2011). Derecho penal e internet. Lex Nova.

Grispo, M. (2017). Derecho internacional y seguridad cibernética. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

González, J. (2014). Un nuevo bien jurídico protegido en el uso y disfrute de la tecnología. La Ley Penal.

INTEL (2021). Sistemas y dispositivos informáticos con tecnología INTEL.

Kaspersky. (2020). Dirección IP: definición y explicación.

Mayer, K. (2017). Protección a los bienes jurídicos protegidos. Revista Chilena de Derecho.

Medina, G. (2014). *Estructura típica del delito de intromisión informática*. Revista Chilena de Derecho.

Mata, R. (2007). Delitos cometidos mediante sistemas informáticos. Universidad de Deusto.

Ministerio del Interior. (2019). Manual para el recojo de evidencia digital.

Ministerio Público. (2018). Investigación Preparatoria.

Ministerio Público. (2020). Ciberdelincuencia en el Perú: Pautas para una rápida investigación fiscal especializada.

Ministerio Público. (2021). Informe de análisis 04 ciberdelincuencia en el Perú: pautas para una investigación especializada.

Moreno, J. (2017). Los elementos de convicción graves y fundados en la medida de prisión preventiva. Comunicaciones telefónicas y testigos protegidos. SAPERE USMP.

Nobles, J. Et al. (2020). Ámbito de valides de la prueba electrónica en los delitos informáticos.

Olivera, N. (2012). Simposio argentino de informática y derecho. JAIIO.

Pastor, E. (2020). Modelo de gestión del análisis forense de hechos delictivos informáticos en el marco del sistema de justicia peruano [Tesis doctoral, Universidad Nacional Federico Villareal].

Panda Security. (2020). ¿Qué es el Phishing?

Proaño, R y Gavilanes, A. (2018). Estrategia para responder a incidentes de inseguridad informática ambientado en la legalidad ecuatoriana. Enfoque UTE.

Quispe, et al. (2019). Asegurándose contra delitos informáticos. Revista de información, tecnología y sociedad.

Rouse, M. (2019). Copia de seguridad o respaldo. TechTarget.

Sundt, C. (2006). Information security and the law. Information Security Technica

Sampaoli, J. (2018). Peritaje informático: Marco teórico – práctico [Tesis de pregrado, Universidad Católica de Argentina].

Téllez, J. (2009). Derecho informático. McGrawHill.

Temperini, I. (2013). Delitos informáticos en Latinoamérica: Un estudio de derecho comparado. CONICET.

Temperini. I. (2014). Suplantación de identidad digital como delito informático en Argentina.

Tori, C. (2008). Hacking ético.

ANEXOS

Anexo 1: Matriz de operacionalización de las variables.

Preguntas de Investigación	Objetivos	Hipótesis	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición
1.- La identificación de la dirección IP (internet Protocolo) de dispositivos informáticos resulta fundamental para combatir la ciberdelincuencia. 2.- La Visualización de los mensajes de redes sociales resulta fundamental para combatir la ciberdelincuencia. 3.- La Visualización de los mensajes correos electrónicos resulta fundamental para combatir la ciberdelincuencia. 4.- La recuperación de archivos eliminados o borrados resulta fundamental para combatir la ciberdelincuencia. 5.- La recuperación de archivos borrados resulta fundamental para combatir la ciberdelincuencia. 6.- La recuperación de mensajes de aplicativos resulta fundamental para combatir la ciberdelincuencia. DIMENSIÓN: Recopilación de elementos de convicción por parte de la policía. 7.- Los Peritajes sobre equipos celulares resulta fundamental para combatir la ciberdelincuencia. 8.- La Pericia informática forense resulta fundamental para combatir la ciberdelincuencia.	Objetivo general Establecer los actos de investigación durante la etapa de investigación preparatoria incide en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, en el Distrito Fiscal de Lima, 2021 2. Objetivos específicos Primer objetivo especifico Determinar la manera en que la recopilación de elementos de convicción por parte del fiscal incide en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, en el Distrito Fiscal de Lima, 2021 Segundo objetivo especifico Establecer la manera en que la recopilación de elementos de convicción por parte de la policía incide en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, en el Distrito Fiscal de Lima, 2021 Tercer objetivo especifico Determinar la manera en que la recopilación de elementos de	**Actos de investigación**	Actuaciones que permite recabar pruebas en la etapa de investigación preparatoria.	(ROSAS, 2012) Los actos de investigación son todos los actos procesales que realiza el fiscal y la policía en procura de recabar o recopilar los elementos de prueba o de convicción que lleven a esclarecer debidamente los hechos.	Recopilar elementos de convicción por parte del fiscal.	• Identificación de la dirección IP (internet Protocolo) de dispositivos informáticos • Visualización de los mensajes de redes sociales • Visualización de los mensajes correos electrónicos. • La recuperación de archivos eliminados o borrados • La recuperación de archivos borrados • La recuperación de mensajes de aplicativos	Totalmente en desacuerdo En desacuerdo Ni de acuerdo ni en desacuerdo De acuerdo Totalmente de acuerdo

9.- Los Peritajes sobre otros equipos de informática resulta fundamental para combatir la ciberdelincuencia. 10.- Peritajes sobre computadoras resulta fundamental para combatir la ciberdelincuencia. 11.- Peritajes sobre Tablets resulta fundamental para combatir la ciberdelincuencia. 12.- Peritaje sobre dispositivos USB resulta fundamental para combatir la ciberdelincuencia.	convicción por parte del fiscal incide en el patrimonio de las víctimas en los delitos cometidos por la ciberdelincuencia en el Distrito Fiscal de Lima, 2021 Cuarto objetivo especifico Establecer la manera en que la recopilación de elementos de convicción por parte de la policía incide en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, en el Distrito Fiscal de Lima, 2021						
					Recopilar elementos de convicción por parte de la policía.	• Peritajes sobre equipos celulares • Pericia informática forense • Peritajes sobre otros equipos de informática • Peritajes sobre computadoras • Peritajes sobre Tablet • Peritaje sobre dispositivos USB	

13.- Los actos de investigación permiten proteger las Cuentas bancarias. 14.- Los actos de investigación permiten proteger la información de contenido patrimonial. 15.- Los actos de investigación permiten proteger las Claves. 16.- Los actos de investigación permiten proteger las contraseñas. 17.- Los actos de investigación permiten proteger la información financiera. 18.- Los actos de investigación permiten proteger información contable. DIMENSIÓN: Afectación psicológica 19.- Los actos de investigación generan afectación a la intimidad. 20.- Los actos de investigación generan afectación a la moral. 21.- Los actos de investigación generan vulneración al secreto de las comunicaciones. 22.- Los actos de investigación generan afectación a la psique. 23.- Los actos de investigación generan vulneración a la correspondencia. 24.- Los actos de investigación generan vulneración a las conversaciones. 25.- Los actos de investigación generan vulneración a la privacidad de los documentos.		**Persecución eficaz en los delitos de Ciberdelincuencia**	Persecución eficaz en los delitos de Ciberdelincuencia surge una protección a los bienes jurídicos protegidos.	(Ministerio Publico 2020) La afectación de la víctima depende de la modalidad del delito informático; es así que la afectación puede ser económica o patrimonial, pero también puede ser moral o psicológica. En este último caso, la afectación también podría estar generada por la pérdida de sus cuentas en redes sociales y por la frustración al no poder identificar a los autores de los delitos.	Afectación económica	• Cuentas bancarias • Información de contenido patrimonial • Claves • Contraseñas • Información financiera • Información contable	
					Afectación psicológica	• Afectación a la intimidad • Afectación a la moral • Vulneración al secreto de las comunicaciones • Afectación a la psique • Vulneración a la correspondencia. • Vulneración a las conversaciones • Vulneración a la privacidad de los documentos	

Anexo 2: Instrumentos de recolección de datos

Cuestionario para medir Actos de investigación

I.Introducción:

Estimado informante el presente documento tiene por objeto conocer su opinión sobre la ACTOS DE INVESTIGACIÓN Y SU INCIDENCIA EN LA PERSECUCIÓN EFICAZ DE LOS DELITOS COMETIDOS POR LA CIBERDELINCUENCIA, DISTRITO FISCAL DE LIMA, 2021, dicha información es completamente anónima y confidencial, por lo que solicito responder las interrogantes con sinceridad y de acuerdo a su propia expectativa.

II. Indicaciones

A continuación, se le presenta una serie de preguntas las cuales deberá responder marcando con una (X) la respuesta que considere pertinente y de acuerdo a escala, solo debe marcar una opción.

A	Totalmente en desacuerdo	1
B	En desacuerdo	2
C	Ni de acuerdo ni en desacuerdo	3
D	De acuerdo	4
E	Totalmente de acuerdo	5

ÍTEMS	APRECIACIÓN				
	1	2	3	4	5
DIMENSIÓN: Recopilación de elementos de convicción por parte del fiscal					
1.- La identificación de la dirección IP (internet Protocolo) de dispositivos informáticos resulta fundamental para combatir la ciberdelincuencia.					
2.- La Visualización de los mensajes de redes sociales resulta fundamental para combatir la ciberdelincuencia.					
3.- La Visualización de los mensajes correos electrónicos resulta fundamental para combatir la ciberdelincuencia.					
4.- La recuperación de archivos eliminados o borrados resulta fundamental para combatir la ciberdelincuencia.					
5.- La recuperación de archivos borrados resulta fundamental para combatir la ciberdelincuencia.					
6.- La recuperación de mensajes de aplicativos resulta fundamental para combatir la ciberdelincuencia.					
DIMENSIÓN: Recopilación de elementos de convicción por parte de la policía.					
7.- Los Peritajes sobre equipos celulares resulta fundamental para combatir la ciberdelincuencia.					
8.- La Pericia informática forense resulta fundamental para combatir la ciberdelincuencia.					
9.- Los Peritajes sobre otros equipos de informática resulta fundamental para combatir la ciberdelincuencia.					
10.- Peritajes sobre computadoras resulta fundamental para combatir la ciberdelincuencia.					
11.- Peritajes sobre Tablets resulta fundamental para combatir la ciberdelincuencia.					
12.- Peritaje sobre dispositivos USB resulta fundamental para combatir la ciberdelincuencia.					

Cuestionario para medir la Persecución eficaz de los delitos cometido por la ciberdelincuencia

I.Introducción:

Estimado informante el presente documento tiene por objeto conocer su opinión sobre la ACTOS DE INVESTIGACIÓN Y SU INCIDENCIA EN LA PERSECUCIÓN EFICAZ DE LOS DELITOS COMETIDOS POR LA CIBERDELINCUENCIA, DISTRITO FISCAL DE LIMA, 2021, dicha información es completamente anónima y confidencial, por lo que solicito responder las interrogantes con sinceridad y de acuerdo a su propia expectativa.

II. Indicaciones:

A continuación, se le presenta una serie de preguntas las cuales deberá responder marcando con una (X) la respuesta que considere pertinente y de acuerdo a escala, solo debe marcar una opción.

A	Totalmente en desacuerdo	1
B	En desacuerdo	2
C	Ni de acuerdo ni en desacuerdo	3
D	De acuerdo	4
E	Totalmente de acuerdo	5

ÍTEMS	APRECIACIÓN				
	1	2	3	4	5
DIMENSIÓN: Afectación económica					
13.- Los actos de investigación permiten proteger las Cuentas bancarias.					
14.- Los actos de investigación permiten proteger la información de contenido patrimonial.					
15.- Los actos de investigación permiten proteger las Claves.					
16.- Los actos de investigación permiten proteger las contraseñas.					
17.- Los actos de investigación permiten proteger la información financiera.					
18.- Los actos de investigación permiten proteger información contable.					
DIMENSIÓN: Afectación psicológica					
19.- Los actos de investigación generan afectación a la intimidad.					
20.- Los actos de investigación generan afectación a la moral.					
21.- Los actos de investigación generan vulneración al secreto de las comunicaciones.					
22.- Los actos de investigación generan afectación a la psique.					
23.- Los actos de investigación generan vulneración a la correspondencia.					
24.- Los actos de investigación generan vulneración a las conversaciones.					
25.- Los actos de investigación generan vulneración a la privacidad de los documentos.					

Anexo 3: Instrumentos de validación – Juicio de experto

OPERACIONALIZACIÓN DE LA VARIABLE

Experto 1

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE……

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: ACTOS DE INVESTIGACIÓN	Sí	No	Sí	No	Sí	No	
1	La identificación de la dirección IP (internet Protocolo) de dispositivos informáticos resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
2	La Visualización de los mensajes de redes sociales resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
3	La Visualización de los mensajes correos electrónicos resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
4	La recuperación de archivos eliminados o borrados resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
5	La recuperación de archivos borrados resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
6	La recuperación de mensajes de aplicativos resulta fundamental para combatir la ciberdelincuencia.	X		X		X		

7	Los Peritajes sobre equipos celulares resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
8	La Pericia informática forense resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
9	Los Peritajes sobre otros equipos de informática resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
10	Peritajes sobre computadoras resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
	DIMENSIÓN 2: Formulación y evacuación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	Peritajes sobre Tablets resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
12	Peritaje sobre dispositivos USB resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
13								

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE……

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN2: PERSECUCIÓN EFICAZ DE LOS ELITOS COMETIDO POR LA CIBERDELINCUENCIA	Sí	No	Sí	No	Sí	No	
1	Los actos de investigación permiten proteger las Cuentas bancarias.	X		X		X		
2	Los actos de investigación permiten proteger la información de contenido patrimonial.	X		X		X		
3	Los actos de investigación permiten proteger las Claves.	X		X		X		
4	Los actos de investigación permiten proteger las contraseñas.	X		X		X		
5	Los actos de investigación permiten proteger la información financiera.	X		X		X		
6	Los actos de investigación permiten proteger información contable.	X		X		X		
7	Los actos de investigación generan afectación a la intimidad.	X		X		X		
8	Los actos de investigación generan afectación a la moral.	X		X		X		
9	Los actos de investigación generan vulneración al secreto de las comunicaciones.	X		X		X		

10	Los actos de investigación generan afectación a la psique.	X		X		X		
	DIMENSIÓN 3: Formulación y evacuación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	Los actos de investigación generan vulneración a la correspondencia.	X		X		X		
12	Los actos de investigación generan vulneración a las conversaciones.	X		X		X		
13	Los actos de investigación generan vulneración a la privacidad de los documentos.	X		X		X		

Observaciones (en caso existan):

_____

Opinión de aplicabilidad:

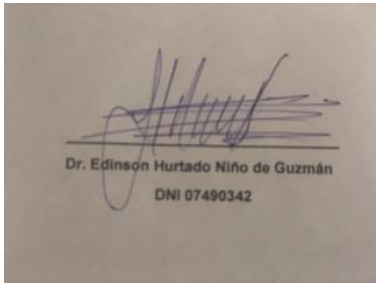
Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador Dr. / Mg: Edinson Wilber Hurtado Niño de Guzman

DNI: 07490342

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

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



Firma del experto informante

15 de diciembre de 2021

Experto 2

OPERACIONALIZACIÓN DE LA VARIABLE

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE……

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: ACTOS DE INVESTIGACIÓN	Sí	No	Sí	No	Sí	No	
1	La identificación de la dirección IP (internet Protocolo) de dispositivos informáticos resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
2	La Visualización de los mensajes de redes sociales resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
3	La Visualización de los mensajes correos electrónicos resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
4	La recuperación de archivos eliminados o borrados resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
5	La recuperación de archivos borrados resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
6	La recuperación de mensajes de aplicativos resulta fundamental para combatir la	X		X		X		

	ciberdelincuencia.							
7	Los Peritajes sobre equipos celulares resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
8	La Pericia informática forense resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
9	Los Peritajes sobre otros equipos de informática resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
10	Peritajes sobre computadoras resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
	DIMENSIÓN 2: Formulación y evacuación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	Peritajes sobre Tablets resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
12	Peritaje sobre dispositivos USB resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
13								

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE……

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: PERSECUCIÓN EFICAZ DE LOS DELITOS COMETIDO POR LA CIBERDELINCUENCIA	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	Los actos de investigación permiten proteger las Cuentas bancarias.	X		X		X		
2	Los actos de investigación permiten proteger la información de contenido patrimonial.	X		X		X		
3	Los actos de investigación permiten proteger las Claves.	X		X		X		
4	Los actos de investigación permiten proteger las contraseñas.	X		X		X		
5	Los actos de investigación permiten proteger la información financiera.	X		X		X		
6	Los actos de investigación permiten proteger información contable.	X		X		X		
7	Los actos de investigación generan afectación a la intimidad.	X		X		X		
8	Los actos de investigación generan afectación a la moral.	X		X		X		
9	Los actos de investigación generan vulneración al secreto de las comunicaciones.	X		X		X		
10	Los actos de investigación generan afectación a la psique.	X		X		X		
	DIMENSIÓN 2: Formulación y evacuación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	Los actos de investigación generan vulneración a la correspondencia.	X		X		X		

12	Los actos de investigación generan vulneración a las conversaciones.	X		X		X		
13	Los actos de investigación generan vulneración a la privacidad de los documentos.	X		X		X		

Observaciones (en caso existan):

Opinión de aplicabilidad:

Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador Dr. / Mg: JOSE OSWALDO CARRETERO GAVANCHO

DNI: 09008286

15 de diciembre de 2021

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

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

Firma del Experto Informante.
JOSE CARRETERO GAVANCHO
Doctor en Derecho

Firma del experto informante

Experto 3

OPERACIONALIZACIÓN DE LA VARIABLE

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE……

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: ACTOS DE INVESTIGACIÓN	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	La identificación de la dirección IP (internet Protocolo) de dispositivos informáticos resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
2	La Visualización de los mensajes de redes sociales resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
3	La Visualización de los mensajes correos electrónicos resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
4	La recuperación de archivos eliminados o borrados resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
5	La recuperación de archivos borrados resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
6	La recuperación de mensajes de aplicativos resulta fundamental para combatir la	X		X		X		

	ciberdelincuencia.							
7	Los Peritajes sobre equipos celulares resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
8	La Pericia informática forense resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
9	Los Peritajes sobre otros equipos de informática resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
10	Peritajes sobre computadoras resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
	DIMENSIÓN 2: Formulación y evacuación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	Peritajes sobre Tablets resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
12	Peritaje sobre dispositivos USB resulta fundamental para combatir la ciberdelincuencia.	X		X		X		
13								

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE……

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: PERSECUCIÓN EFICAZ DE LOS DELITOS COMETIDO POR LA CIBERDELINCUENCIA	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	Los actos de investigación permiten proteger las Cuentas bancarias.	X		X		X		
2	Los actos de investigación permiten proteger la información de contenido patrimonial.	X		X		X		
3	Los actos de investigación permiten proteger las Claves.	X		X		X		
4	Los actos de investigación permiten proteger las contraseñas.	X		X		X		
5	Los actos de investigación permiten proteger la información financiera.	X		X		X		
6	Los actos de investigación permiten proteger información contable.	X		X		X		
7	Los actos de investigación generan afectación a la intimidad.	X		X		X		
8	Los actos de investigación generan afectación a la moral.	X		X		X		
9	Los actos de investigación generan vulneración al secreto de las comunicaciones.	X		X		X		
10	Los actos de investigación generan afectación a la psique.	X		X		X		
	DIMENSIÓN 2: Formulación y evacuación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	Los actos de investigación generan vulneración a la correspondencia.	X		X		X		
12	Los actos de investigación generan vulneración	X		X		X		

	a las conversaciones.							
13	Los actos de investigación generan vulneración a la privacidad de los documentos.	X		X		X		

Observaciones (en caso existan):

Opinión de aplicabilidad:

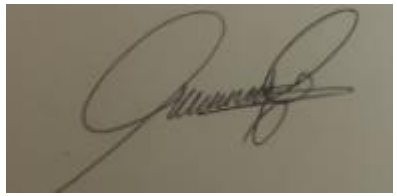
Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador Dr. / Mg: LEYLA CARUAJULCA AGUILAR
DNI: 40744495

15 de diciembre de 2021

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

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



Firma del experto informante

Anexo 4: Análisis de base de datos

Actos de investigación

PREG1	PREG2	PREG3	PREG4	PREG5	PREG6	PREG7	PREG8	PREG9	PREG10	PREG11	PREG12	PREG13
3	5	3	3	3	3	3	5	3	3	3	3	3
5	5	3	3	5	3	5	5	3	3	5	3	5
5	2	5	5	5	3	5	2	5	5	5	3	5
5	3	3	5	3	3	5	3	3	5	3	3	5
5	5	5	5	5	4	5	5	5	5	5	4	5
4	5	2	3	3	4	4	5	2	3	3	4	4
4	5	5	5	5	4	4	5	5	5	5	4	4
4	5	5	5	5	5	4	5	5	5	5	5	4
4	2	1	1	1	1	4	2	1	1	1	1	4
4	5	5	3	5	4	4	5	5	3	5	4	4
3	2	2	5	5	5	3	2	2	5	5	5	3
4	3	2	5	3	3	4	3	2	5	3	3	4
4	5	5	5	2	3	4	5	5	5	2	3	4
4	3	3	2	5	3	4	3	3	2	5	3	4
3	3	5	3	3	3	3	3	5	3	3	3	3
3	3	3	3	2	3	3	3	3	3	2	3	3
4	4	3	4	3	4	4	4	3	4	3	4	4
3	5	3	4	2	5	3	5	3	4	2	5	3
4	4	3	4	5	3	4	4	3	4	5	3	4
5	5	4	3	5	3	5	5	4	3	5	3	5
1	1	1	1	1	1	1	1	1	1	1	1	1
4	4	4	3	3	1	4	4	4	3	3	1	4
5	5	4	5	3	4	5	5	4	5	3	4	5
2	2	2	2	2	2	2	2	2	2	2	2	2
1	5	4	5	3	4	1	5	4	5	3	4	1
2	3	3	3	3	3	2	3	3	3	3	3	2
3	3	3	3	3	3	3	3	3	3	3	3	3
2	3	5	3	3	3	2	3	5	3	3	3	2
3	4	3	3	3	5	3	4	3	3	3	5	3
5	2	5	3	3	5	5	2	5	3	3	5	5
3	5	5	3	1	2	3	5	5	3	1	2	3
2	2	2	4	4	5	2	2	2	4	4	5	2
3	5	5	3	5	1	3	5	5	3	5	1	3
5	5	4	5	5	5	5	5	4	5	5	5	5
5	5	4	4	1	3	5	5	4	4	1	3	5
4	5	5	5	5	5	4	5	5	5	5	5	4
1	2	1	1	1	1	1	2	1	1	1	1	1
4	5	5	3	5	4	4	5	5	3	5	4	4
3	2	2	5	5	5	3	2	2	5	5	5	3
4	2	2	5	3	4	4	2	2	5	3	4	4
4	5	5	5	2	3	4	5	5	5	2	3	4
4	3	2	2	5	4	4	3	2	2	5	4	4
4	3	5	3	3	3	4	3	5	3	3	3	4
3	3	2	3	2	4	3	3	2	3	2	4	3
4	4	3	4	3	4	4	4	3	4	3	4	4
5	3	4	4	2	5	5	3	4	4	2	5	5
4	3	4	4	5	3	4	3	4	4	5	3	4
5	4	4	3	5	3	5	4	4	3	5	3	5
4	4	3	4	5	2	4	4	3	4	5	2	4
4	4	4	3	3	1	4	4	4	3	3	1	4

Anexo 5: Análisis de base de datos

Delitos cibernéticos

PREG14	PREG15	PREG16	PREG17	PREG18	PREG19	PREG20	PREG21	PREG22	PREG 23	PREG 24	PREG25
5	3	3	3	3	3	5	3	3	3	3	3
5	3	3	5	3	5	5	3	3	5	3	3
2	5	5	5	3	5	2	5	5	5	3	3
3	3	5	3	3	5	3	3	5	3	3	3
5	5	5	5	4	5	5	5	5	5	4	4
5	2	3	3	4	4	5	2	3	3	4	4
5	5	5	5	4	4	5	5	5	5	4	4
5	5	5	5	5	4	5	5	5	5	5	5
2	1	1	1	1	4	2	1	1	1	1	1
5	5	3	5	4	4	5	5	3	5	4	4
2	2	5	5	5	3	2	2	5	5	5	5
3	2	5	3	3	4	3	2	5	3	3	3
5	5	5	2	3	4	5	5	5	2	3	4
3	3	2	5	3	4	3	3	2	5	3	4
3	5	3	3	3	3	3	5	3	3	3	4
3	3	3	2	3	3	3	3	3	2	3	4
4	3	4	3	4	4	4	3	4	3	4	4
5	3	4	2	5	3	5	3	4	2	5	4
4	3	4	5	3	4	4	3	4	5	3	5
5	4	3	5	3	5	5	4	3	5	3	5
1	1	1	1	1	1	1	1	1	1	1	1
4	4	3	3	1	4	4	4	3	3	1	1
5	4	5	3	4	5	5	4	5	3	4	4
2	2	2	2	2	2	2	2	2	2	2	2
5	4	5	3	4	1	5	4	5	3	4	4
3	3	3	3	3	2	3	3	3	3	3	3
3	3	3	3	3	3	3	3	3	3	3	3
3	5	3	3	3	2	3	5	3	3	3	3
4	3	3	3	5	3	4	3	3	3	5	5
2	5	3	3	5	5	2	5	3	3	5	5
5	5	3	1	2	3	5	5	3	1	2	2
2	2	4	4	5	2	2	2	4	4	5	5
5	5	3	5	1	3	5	5	3	5	1	1
5	4	5	5	5	5	5	4	5	5	5	5
5	4	4	1	3	5	5	4	4	1	3	3
5	5	5	5	5	4	5	5	5	5	5	5
2	1	1	1	1	1	2	1	1	1	1	1
5	5	3	5	4	4	5	5	3	5	4	4
2	2	5	5	5	3	2	2	5	5	5	5
2	2	5	3	4	4	2	2	5	3	4	4
5	5	5	2	3	4	5	5	5	2	3	3
3	2	2	5	4	4	3	2	2	5	4	4
3	5	3	3	3	4	3	5	3	3	3	3
3	2	3	2	4	3	3	2	3	2	4	4
4	3	4	3	4	4	4	3	4	3	4	4
3	4	4	2	5	5	3	4	4	2	5	5
3	4	4	5	3	4	3	4	4	5	3	3
4	4	3	5	3	5	4	4	3	5	3	3
4	3	4	5	2	4	4	3	4	5	2	2
4	4	3	3	1	4	4	4	3	3	1	1

UNIVERSIDAD CÉSAR VALLEJO

RESOLUCIÓN JEFATURAL N° 5021-2021-UCV-VA-EPG-F05L01/J-INT

Los Olivos, 31 de diciembre de 2021

VISTO:

El informe presentado por el (la) docente Mtro(a). Dr. (a) **Menacho Rivera Alejandro Sabino** de la Experiencia Curricular **"Diseño y Desarrollo del Trabajo de Investigación"** del programa de **Maestría en Derecho Penal y Procesal Penal**, grupo **A1**, a la Jefatura de la Escuela de Posgrado de la Filial Lima Norte de la Universidad César Vallejo, solicitando la inscripción del proyecto de investigación:

"ACTOS DE INVESTIGACIÓN EN LA PERSECUSION EFICAZ DE LOS DELITOS COMETIDOS POR LA CIBERDELINCUENCIA, DISTRITO FISCAL DE LIMA, 2021"

presentado por el (la) estudiante:

Karina Usaqui Barbaran

CONSIDERANDO:

Que, el artículo 7° del Reglamento de Investigación de Posgrado indica: *"El sistema de Evaluación de la investigación implica el seguimiento de los trabajos de investigación, desde su concepción hasta su obtención de los resultados para su sustentación y publicación"*.

Que, el artículo 14° del Reglamento de Investigación de Posgrado indica: *"La vigencia del proyecto es un año. En caso de exceder el tiempo considerado, el interesado deberá remitirse a los procedimientos de investigación de la Escuela de Posgrado"*.

Que, el artículo 17° del Reglamento de Investigación de Posgrado indica: *"El proyecto de tesis es elaborado por un estudiante bajo la asesoría del docente metodólogo, dentro del cronograma y normatividad académica establecida y culmina, previa evaluación, con opinión favorable del docente metodólogo y la obtención de la resolución del proyecto"*.

Que, el artículo 35° del Reglamento de Investigación de Posgrado indica: *"El docente se constituye en asesor metodólogo, responsable del monitoreo y evaluación del diseño y desarrollo del proyecto de tesis"*.

Que, el (la) estudiante ha cumplido con todos los requisitos académicos y administrativos necesarios para inscribir su proyecto de tesis.

Que, el proyecto de investigación cuenta con la opinión favorable del docente metodólogo de la experiencia curricular de **"Diseño y Desarrollo del Trabajo de Investigación"**.

Que, estando a lo expuesto y de conformidad con las normas estatutarias y reglamento vigente;

SE RESUELVE:

Art. 1°.- Aprobar el proyecto de tesis: **"ACTOS DE INVESTIGACIÓN EN LA PERSECUSION EFICAZ DE LOS DELITOS COMETIDOS POR LA CIBERDELINCUENCIA, DISTRITO FISCAL DE LIMA, 2021"**, presentado por el (la) estudiante **Karina Usaqui Barbaran**, con Código: **7002537207**, el mismo que contará con un plazo máximo de un año para su ejecución.

UNIVERSIDAD CÉSAR VALLEJO

Art. 2°.- Registrar el proyecto de tesis dentro del archivo de la línea de investigación: **DERECHO PENAL Y PROCESAL PENAL,** correspondiente al Programa de **Maestría en Derecho Penal y Procesal Penal,** grupo **A1.**

Art. 3°.- Designar al Mtro(a). Dr(a). **Menacho Rivera Alejandro Sabino** como asesor metodólogo del proyecto de tesis: **"ACTOS DE INVESTIGACIÓN EN LA PERSECUSION EFICAZ DE LOS DELITOS COMETIDOS POR LA CIBERDELINCUENCIA, DISTRITO FISCAL DE LIMA, 2021".**

Regístrese, comuníquese y archívese.

Ormeño Trinidad Vargas, MBA
Jefe (e)
Escuela de Posgrado - Campus Lima Norte