UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Derecho Penal y Procesal Penal

AUTOR:

Chavarría Velasquez, Gustavo Rafael (orcid.org/0000-0003-2318-9101)

ASESORES:

Dra. Alva Diaz, Lyda Palmira (orcid.org/0000-0002-3230-2981)

Dr. Vasquez Castro, Miguel Angel (orcid.org/0000-0002-2141-1568)

LÍNEA DE INVESTIGACIÓN:

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

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía.

CHIMBOTE – PERÚ

2023

DEDICATORIA

A Dios, quien me ha otorgado la vida, y me ha brindado salud y sabiduría en el desarrollo de la presente tesis.

A mi mamá y mi familia, por siempre apoyarme y motivarme en todo lo que me propongo. Gracias por enseñarme a nunca rendime.

Gustavo Rafael Chavarría Velásquez

AGRADECIMIENTO

A Dios, quien forja mi camino y siempre me guía por el sendero correcto, y por haberme permitido ser capaz de concluir esta investigación.

Gustavo Rafael Chavarría Velásquez

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Declaratoria de Autenticidad de los Asesores

Nosotros, ALVA DIAZ LYDA PALMIRA,VASQUEZ CASTRO MIGUEL ANGEL, docente de la ESCUELA DE POSGRADO MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL de la UNIVERSIDAD CÉSAR VALLEJO SAC - CHIMBOTE, asesores de Tesis titulada: "Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú", cuyo autor es CHAVARRÍA VELÁSQUEZ GUSTAVO RAFAEL, constato que la investigación tiene un índice de similitud de 7.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

CHIMBOTE, 30 de Agosto del 2023

Apellidos y Nombres del Asesor:	**Firma**
ALVA DIAZ LYDA PALMIRA,VASQUEZ CASTRO MIGUEL ANGEL **DNI:** 06240404 **ORCID:** 0000-0002-3230-2981	Firmado electrónicamente por: ADIAZLP el 30-08-2023 22:51:12
ALVA DIAZ LYDA PALMIRA,VASQUEZ CASTRO MIGUEL ANGEL **DNI:** 03700347 **ORCID:** 0000-0002-2141-1568	Firmado electrónicamente por: VCASTROMA el 31-08-2023 17:55:06

Código documento Trilce: TRI - 0650450

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Declaratoria de Originalidad del Autor

Yo, CHAVARRÍA VELÁSQUEZ GUSTAVO RAFAEL estudiante de la ESCUELA DE POSGRADO MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL de la UNIVERSIDAD CÉSAR VALLEJO SAC - CHIMBOTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

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

Nombres y Apellidos	**Firma**
GUSTAVO RAFAEL CHAVARRÍA VELÁSQUEZ **DNI:** 71587202 **ORCID:** 0000-0003-2318-9101	Firmado electrónicamente por: GCHAVARRIAVEL el 01-08-2023 21:45:02

Código documento Trilce: TRI - 0635484

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

RESUMEN

La presente investigación fue realizada con el objetivo de determinar la implicancia existente entre los delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público del Perú. Fue elaborada desde un enfoque cualitativo, usando un tipo de investigación básica y un diseño de teoría fundamentada. Además, la entrevista se usó como técnica de recolección de datos y la guía de entrevista como su instrumento, siendo esta aplicada a cinco abogados en ejercicio en el área penal en el Distrito Judicial del Santa. Se obtuvo como resultado que la Unidad Fiscal Especializada en Ciberdelincuencia fue implementada para acompañar – de manera técnica – en la identificación, investigación y sanción de los delitos informáticos a los fiscales mediante el uso de recursos tecnológicos. Además, se requiere la elaboración de doctrina y teorías jurídicas, una ampliación de funciones siguiendo modelos internacionales y la implementación de fiscalías especializadas en ciberdelincuencia que hagan frente a los ciberdelitos en los distritos fiscales. Por lo tanto, se concluyó que sí existe implicancia entre esta clase de delitos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia.

Palabras clave: Delitos informáticos, ciberdelincuencia, ciberdelitos, Unidad Fiscal Especializada en Ciberdelincuencia.

ABSTRACT

The present investigation was carried out with the objective of determining the existing implication between computer crimes and the implementation of the Specialized Fiscal Unit in Cybercrime of the Public Ministry of Peru. It was elaborated from a qualitative approach, using a type of basic research and a grounded theory design. In addition, the interview was used as a data collection technique and the interview guide as its instrument, being applied to five lawyers practicing in the criminal area in the Judicial District of Santa. It was obtained as a result that the Specialized Fiscal Unit in Cybercrime was implemented to accompany - in a technical way - in the identification, investigation and punishment of computer crimes to prosecutors through the use of technological resources. In addition, it is required the elaboration of legal doctrine and theories, an expansion of functions following international models and the implementation of specialized cybercrime prosecutor's offices that deal with cybercrime in tax districts. Therefore, it was concluded that there is an implication between this class of crimes and the implementation of the Specialized Fiscal Unit in Cybercrime.

Keywords: Computer crimes, cybercrime, cybercrime, Specialized Fiscal Unit in Cybercrime.

I. INTRODUCCIÓN

La globalización es un fenómeno que ha coadyuvado al desarrollo y expansión de la tecnología, proporcionando herramientas digitales que han modificado los modos en como se realizan las actividades. Estas herramientas también han sido implementadas por parte de los gobiernos – aplicándolas a través de los diferentes ámbitos de la gestión pública e instituciones – en aras de efectivizar la administración pública (Leyva, 2021).

Asimismo, grandes y modernos cambios tecnológicos han sido generados e implementados en los últimos años, producto de la pandemia de la COVID-19. Este hecho ha logrado que las comunicaciones sean más eficaces y que las actividades se desarrollen con mayor agilidad; sin embargo, también han fomentado el riesgo de que se vulneren los bienes jurídicos expuestos en el mundo digital. El desarrollo de la tecnología no solo ha traído grandes ventajas, sino también nuevas formas y modalidades delictivas.

> Las fuerzas del orden público de todo el mundo han sido testigos de primera mano de los aspectos delictivos únicos que generaba la pandemia de la COVID-19, especificamente la diversificación y el creciente impacto de la ciberdelincuencia. Este fenómeno nos ha hecho repensar nuestra respuesta global y reorientar nuestra red mundial de aplicación de la ley. (INTERPOL – International Criminal Police Organization –, 2021, p. 3)

Además, la INTERPOL (2021) refiere que un informe suyo – que estudió el impacto de la COVID-19 en el panorama global de ciberamenazas – identificó las estrategias nacionales contra el ciberdelito como una forma de desarrollar la resiliencia de la infraestructura y los servicios nacionales, ayudando a los países a contrarrestar las ciberamenazas de manera efectiva y proteger a las comunidades de los ciberataques durante la pandemia y más allá.

Según el Observatorio Español de Delitos Informáticos (2021), se cometieron 287, 963 y 305, 477 delitos informáticos durante el 2020 y 2021 – respectivamente – en España. Morón (2016) informó que como medida para contrarrestar los delitos informáticos en República Dominicana, ha sido incorporada una regulación específica en una ley especial. Por otro lado, en países como Panamá o Colombia, las regulaciones sobre delitos informáticos han sido incorporadas en sus Códigos Penales.

Esta diferencia entre los cuerpos normativos es una muestra de que hay varios caminos para combatir la ciberdelincuencia; no obstante, es necesario que la normativa esté actualizada a los cambios y avances que se den en los medios informáticos.

En esa misma línea, es indispensable que existan herramientas normativas internacionales que brinden parámetros generales para cada Estado sobre los delitos informáticos, toda vez que la realización de estos – producto de la red global del internet – pueden trascender fronteras e involucrar a más de un Estado. De manera global, el jefe de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) comunica que la ciberdelincuencia produce pérdidas anuales aproximadas de $ 12, 500 millones (Alva y Collave, s.f.). Por lo que, Vinelli (2021) informa que los Estados están de acuerdo en que los delitos informáticos deben ser investigados y sus autores, enjuiciados; sin embargo, esto es obstaculizado debido a la diparidad entre la escasa cooperación internacional y la diparidad normativa.

El 8 de noviembre de 2001, frente a esta necesidad, fue aprobado el Convenio de Budapest, brindando protección internacional frente a la ciberdelincuencia. Al respecto, Perú ratificó su adhesión el 9 de marzo de 2019. Si bien este Convenio fue un gran acierto, ya han transcurrido más de 20 años desde su dación; por lo que, es algo notable el hecho de que no haya un nuevo convenio con un contenido actualizado.

Por consiguiente, en los últimos años se han promovido cooperaciones transnacionales con el objetivo de combatir la ciberdelincuencia. En Sudamérica,

existen dos pronunciamientos iberoamericanos resaltantes. Por un lado, el Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia. Por otro lado, la Recomendación de la Conferencia de Ministros de Justicia de los Países Iberoamericanos relativa a la tipificación y sanción de la ciberdelincuencia. Estas herramientas – promulgadas en 2014 – han brindado criterios básicos en aras de la prevensión y batalla contra la ciberdelincuencia, sin dejar de lado las legislaciones nacionales de cada país.

En cuanto a nuestra situación nacional, según las estadísticas recabadas por la Oficina de Racionalización y Estadística (ORACE) del Ministerio Público (2021), – en el periodo abarcado desde octubre de 2013 hasta julio de 2020 – 21, 687 denuncias sobre delitos informáticos fueron reportadas. Como era de esperarse, el pico de denuncias se dio durante la emergencia sanitaria por la COVID-19, dado que esta coyuntura impulsó el uso masivo del e-commerce. Para combatir este gran problema, existen las siguientes normas nacionales: la Ley N.° 30999 y la Ley N.° 30096.

El 30 de diciembre de 2020, como respuesta a esta situación, una Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público fue implementada, siendo esto un gran avance que lleva a la especialización como forma efectiva de combatir los delitos informáticos y, asimismo, engloba una materia compleja que afecta a todas las formas de delincuencia. Sumado a ello, se implementó – a nivel nacional – una red de fiscales en ciberdelincuencia, integrado por 64 fiscales, quienes serán los intermediarios entre esta nueva unidad y los distritos fiscales (Ministerio Público, 2021).

En ese sentido, este es un problema internacional que requiere soluciones desde el plano internacional y primordiamente, desde el plano nacional; por lo cual, diversos países han creado unidades especializadas en combatir la ciberdelincuencia. Esto ha incentivado a que el Perú – por recomendaciones y con apoyo – se decida a crear una unidad enfocada a identificar, investigar y sancionar los delitos informáticos, siendo esta la institución objeto de estudio.

Además, bajo recomendación de esta unidad, a mediados del 2021, se implementó la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, teniendo competencia sobre 16 distritos capitalinos para conocer e investigar los delitos informáticos regulados por ley (Defensoría del Pueblo, 2023). En datos actuales, la DIVINDAT informó que 3, 946 delitos informáticos fueron denunciados en todo el 2022 (Pichihua, 2023).

Es evidente que el Ministerio Público ha tomado medidas en aras de combatir la ciberdelincuencia. Frente a esta situación, se planteó la siguiente interrogante: ¿Cuál es la implicancia de los delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú?

La importancia de la presente tesis se fundamentó en la gran problemática que representan los delitos informáticos para el Estado, debido a sus constantes cambios con nuevas formas delictivas.

Frente a estos cambios, el Perú ha respondido implementando una Unidad Fiscal Especializada en Ciberdelincuencia. Esta tesis aportará conocimientos teóricos y prácticos sobre los delitos informáticos y la unidad antes mencionada; además, dará alcances sobre las nuevas magnitudes que están alcanzando los delitos informáticos.

Lo novedoso radica en que la institución objeto de estudio ha sido creada finalizando el 2020 y no hay tesis precedentes que la hayan abordado, debido a que es un proyecto piloto por parte del Ministerio Público. Por lo mencionado, la presente tesis fue viable y es de gran utilidad para la sociedad peruana.

Al respecto, es pertinente hacer referencia a los objetivos. El objetivo general es determinar la implicancia existente entre los delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú.

Asimismo, el objetivo específico 1: identificar si existen doctrinas y teorías modernas suficientes sobre los delitos informáticos.

El objetivo específico 2 es: comparar la Unidad Fiscal Especializada en Ciberdelincuencia con sus similares en otros países.

Y el objetivo específico 3 es: analizar el avance en la identificación, investigación y sanción de los delitos informáticos tras la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia en el Perú

II. MARCO TEÓRICO

En el plano internacional, Rivera (2020) concluyó que para establecer la constitución de un delito informático, este debe ser estudiado desde la perpectiva de la teoría del delito, dado que esta es procedente para todas las formas delictivas encausadas. Asimismo, afirma que en el futuro existirán nuevos delitos informáticos que serán excluidos dentro del estudio penal; sin embargo, cuando estos sean tipificados, el legislador deberá poseer mayores estudios sobre la realización de estos tipos de delitos sin dejar de lado los fundamentos y la base del derecho penal.

Aunado a ello, Habirovs (2018) concluyó que es importante reconocer que el ciberespacio es un entorno que cambia extraordinariamente rápido; por lo que, los estudios realizados en este campo pueden quedar obsoletos en unos pocos años a medida que avanza el progreso tecnológico y, los métodos de ciberataque y las técnicas de protección contra el cibercrimen cambian con él. Además, concluye que la tergiversación del estado de la ciberdelincuencia real puede generar un mayor temor a esta y – en consecuencia – provocar un uso excesivo de medidas de prevneción inncesarias; por lo que, revelar datos reales sobre la victimización en el ciberespacio y demostrar que es mucho más seguro de lo que se percibe, podría reducir el miedo al ciberdelito en la población en general.

En esa misma línea, Graham (2023) concluyó que los delitos informáticos representan una series de desafíos únicos para los legisladores y, otros actores públicos y privados relevantes; además, el panorama tecnológico en continuo desarrollo presenta desafíos únicos para la aplicación de la ley y los intentos de regulación en este espacio. Además, concluye que la naturaleza cambiante del delito cibernético y el delito habilitado por la tecnología presentan dificultades significativas para garantizar que la ley siga efectiva y aplicable.

En el plano nacional, Bernal y Menacho (2021) concluyeron que las instituciones administradoras de justicia peruanas actuales no son adecuadas

para investigar y sancionar la comisión tanto de delitos informáticos como tradicionales, realizados haciendo uso de medio tecnológicos, porque existe insuficiencia en la logística, la infraestructura y el personal. Además, añaden que una Fiscalía Especializada en Ciberdelincuencia que no esté integrada de personal que cuente tanto con conocimientos de derecho como de tecnología, enfocada – de manera exclusiva – en la solución de delitos informáticos y tradicionales – realizados haciendo uso de medio tecnológicos –, impacta de manera negativa en los procesos de investigación fiscal, impidiendo una protección ideal y provocando desconfianza en las víctimas.

Por su parte, Huamán (2020) concluyó que la problemática presente – producto de la ciberdelincuencia en el Perú – está en aumento y, guarda relación con la accesibilidad y uso de diferentes y modernos aparatos digitales por parte de los delincuentes cibernéticos, generando trabas en su identificación y localización. Sumado a ello, informa que en 2017, el Perú fue el país más afectado de América Latina con los programas ransomware (secuestro de datos), representando el 25.1% del total de casos presentados; consecuentemente, en 2019, nuestro país ocupó el tercer lugar de los países más afectados con programas spyware en América Latina, presentandose ese mismo año un total de 247 denuncias por suplantación de identidad y 3, 012 denuncias por fraude informático en la DIVINDAT. Por último, realzan el problema que representa la falta de presupuesto dirigido a contar con tecnología de última generación para combatir los delitos informáticos.

Asimismo, Carrera (2021) concluyó que los aspectos negativos en la investigación fiscal son resultado de la nula capacidad operativa por parte de la DIVINDAT y la gran cantidad de casos en las oficinas de los agentes de justicia; en consecuencia, provocan que las investigaciones por delitos informáticos no se lleven a cabo de manera efectiva. Además, concluye que debido a los avances tecnologícos, nuevos tipos penales que no están regulados por ley son generados y, muchas veces por falta de conocimiento, no se logra combatir efectivamente la criminalidad informática, ni tampoco identificar la clase de comportamiento del perpetrador.

Por otro lado, Valarezo, Valarezo y Duran (2019) han explicado que la teoría clásica del delito constituye una herramienta que analiza el comportamiento humano de manera científica con el objetivo de identificar la existencia del tipo penal; en consecuencia, representa un sistema de ordenación secuenciada y categorizada de todos los elementos cuya concurrencia es menester corroborar con el fin de establecer la culpabilidad de una persona. Además, precisó que esta teoría exije el cumplimiento de juicios sucesivos: acción, tipicidad, antijuricidad y culpabilidad.

Respecto a las teorías sobre delitos informáticos, Palmieri y Shortland (2021) han afirmado que el internet ha brindado a las personas una multitud de oportunidades para participar en delitos y desviaciones en línea. A pesar de los esfuerzos de investigaciones recientes, la aplicación de teorías criminológicas al tema del delito cibernético ha arrojado resultados mixtos. Además, ningún estudio hasta la fecha ha tratado de examinar el efecto de la personalidad – en las diferencias individuales – en las motivaciones para participar en el delito cibernético.

> No existe una sola perspectiva teórica que haya recibido un amplio apoyo para explicar estos tipos penales; además, las evaluaciones empíricas que aplican las teorías criminológicas tradicionales al estudio de la ciberdelincuencia han proporcionado un apoyo mixto. Sin embargo, lo que está claro es que una teoría del delito informático debe abarcar a un delincuente motivado, en el que la motivación se ve influida interna y externamente. Por lo tanto, para el estudio de los delitos informáticos, es importante que los académicos observen las teorías de la motivación en lugar de solo las teorías tradicionales del delito. (Palmieri y Shortland, 2021, p. 2)

En ese sentido, Barn y Barn (2016) han propuesto una taxonomía que luego fue desarrollada como ontología con el propósito de clasificar los ciberdelitos. Los principales conceptos presentados en su ontología son: acción, agente, contacto, observador externo, impacto, ubicación, motivación, acto de ingeniería social, objetivo, rol tecnológico y punto de vista. La ontología presentada es

informativa ya que ofrece varias características con las que clasificar los delitos cibernéticos, intentando una visión integrada de estos. Además, se identifican formalmente características adicionales que se pueden incorporar en trabajos futuros.

Por su parte, Applegate y Stavrou (2013) han propuesto una taxonomía de delitos informáticos para describir los eventos de la ciberdelincuencia y se divide en dos grupos principales: categorías y sujetos. Los sujetos son entidades o eventos, y representan los eventos de conflicto cibernético del mundo real y sus participantes; es decir, individuos, organizaciones o estados. Las categorías se utilizan para clasificar los sujetos a través de dos subcategorías: acciones y actores; y cada subcategoría se subdivide en subcategorías específicas cada vez mayores que se utilizan para describir los sujetos.

Al respecto, Chandra y Snowe (2020) también han desarrollado una teoría de ciberdelincuencia basada en una taxonomía. Esto surge debido a la falta de una definición y estándares para medir y gestionar la ciberdelincuencia; por consiguiente, definen el delito informático como un acto que utiliza la tecnología informática para cometer un delito. Su taxonomía propuesta está basada en cuatro componentes básicos: exclusividad mutua, estructura, exhaustividad y categorías bien definidas.

> En primer lugar, la condición de exclusividad mutua garantiza que dos elementos de la taxonomía no tengan características comunes; es decir, diferencia la modalidad virtual de la criminalidad tradicional. En segundo lugar, el componente estructura reduce la complejidad al limitar los niveles jerárquicos, agrupando ampliamente los elementos dentro de categorías bien definidas, dado que estos brindarán uniformidad y eficiencia. En tercer lugar, la condición de exhaustividad requiere la inclusión de todas las características para describir un elemento en la taxonómia; por lo tanto, se consideran todas las posibilidades para describir un delito cibernético. Por último, la condición de categorías bien definidas garantiza que cada delito cibernético se identifique con claridad y especificidad, con los detalles efectivos necesarios para su adecuada asignación dentro de la taxonomía.

> Estos cuatro componentes permiten la identificación y categorización de un delito informático único – cada uno con características distintas – para la determinación de su lugar apropiado en la taxonomía y para la identificación proactiva de sus nuevas variaciones. Asimismo, su taxonomía tiene implicaciones para que – en primer lugar – cada gestión diseñe controles internos apropiadas para cada categoría de delito informático y – en segundo lugar –, para que los órganos de gobierno instituyan estándares y procesos para monitorear su cumplimiento. Por último, manifiestan que el sistema judicial y penal puede beneficiarse de la claridad conceptual de su taxonomía para juzgar los delitos informáticos. (Chandra y Snowe, 2020, p. 5)

En cuanto al enfoque conceptual, Donalds y Osei-Bryson (2019) señalaron que los delitos informáticos abarcan una gran cantidad de actos, delitos o conductas ilícitas perpetradas por individuos o grupos contra computadoras, dispositivos relacionados con computadoras o redes de tecnología de la información; del mismo modo, delitos tradicionales que son facilitados o mantenidos por el uso del internet y/o tecnología de la información.

En cuanto a estudios sobre la ciberdelincuencia, Donalds y Osei-Bryson (2019) refirieron que los esquemas de clasificación en trabajos anteriores son insuficientes, dado que tienen un alcance limitado y cada uno aborda solo unas pocas perspectivas; es decir, están fragmentados y – a menudo – son incompatibles. Además, son incapaces de clasificar a los delitos informáticos de manera efectiva. No obstante, la clasificación consistente y repetible es importante para el dominio del problema, dado que los investigadores podrían clasificar el mismo delito cibernético de manera diferente, lo que resultaría en una identificación inexacta de sus tendencias y patrones.

> El trabajo policial se ha establecido como centrado en el conocimiento; por ejemplo, las investigaciones penales suelen incluir actividades como el procesamiento de la escena del crimen o la recopilación de pruebas. Esta naturaleza centrada de los delitos cibernéticos muestra claramente la necesidad de sistemas y aplicaciones basados en el conocimiento; por lo

que, existe una escasez de desarrollo basado en el conocimiento. (Donalds y Osei-Bryson, 2019, p. 405)

En ese sentido, Goni, Ali, Showrov, Alam y Shameem (2022) refirieron que el término ciberdelito es utilizado para describir – de manera general – el tipo penal donde las redes informáticas o computadoras son los medios, objetivos o lugar de comisión del delito, e incluye diversas cosas, como los ataques de craqueo electrónico. Explican su preocupación de que la ciberdelincuencia está creciendo y los modelos técnicos actuales para abordarlo son ineficientes; por lo que, existe la necesidad de más estrategias preventivas para reducir esta problemática.

Por su parte, Puchkov (2021) indicó que incluso si existe un acuerdo general entre la mayoría de los países sobre la importancia y relevancia de la lucha contra la ciberdelincuencia, lo que presupone una respuesta constante y coordinada; por lo que, este problema como tal no puede ser descrito dentro de límites cuantitativos, dado que diferentes modalidades de delitos informáticos tampoco pueden ser descritos. Por lo tanto, esta problemática presenta hoy desafíos únicos y requiere de una necesidad especial de cooperación internacional. Añade que a pesar de que ya existen y están en vigor una serie de acuerdos sobre asistencia legal recíproca, existe una necesidad apremiante de mejorar los procedimientos para una respuesta adecuada a los actos de ciberdelincuencia – especialmente a nivel internacional – y; en consecuencia, se genere una cooperación internacional ideal.

Según Rodriguez (citado por Barrios, 2017), los delitos informáticos representan una acción cuyos requisitos configuran un delito, consumándose con el uso de un aparato tecnológico o violentando los derechos del titular de uno, indistintamente de si es hardware o software.

En cuanto a la naturaleza del delito cibernético, la Office of Civil and Criminal Justice Reform (2017) señaló que es importante contar con una base jurisdiccional amplia para tales delitos, ya que a menudo los actos cometidos en el territorio de una jurisdicción pueden tener un impacto sustancial en otras.

Añade que algunos países pueden abordar este problema a través de la jurisprudencia que interpreta la jurisdicción territorial de manera amplia para incluir situaciones en las que existe un vínculo real y sustancial con esa juridicción, aunque los elementos del delito puedan haberse cometido en otro lugar.

> En otros países, la legislación establece específicamente que la jurisdicción puede asumirse cuando existe un vínculo sustancial con el país, término que se define en sentido amplio. Por lo tanto, cualquiera sea el enfoque que se adopte, es importante que los países consideren cuidadosamente la cuestión de la jurisdicción y adopten disposiciones que aseguren que no haya refugio seguro para quienes cometan delitos cibernéticos. (La Office of Civil and Crimminal Justice Reform, 2017, p. 7)

La OFAEC – Oficina de Análisis Estratégico contra la Criminalidad – (2021) refirió que la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público es un Piloto de Fiscalía Especializada que posee competencia a nivel nacional y, es dependiente de la Fiscalía de la Nación en los aspectos administrativos y funcionales.

Finalmente, con todo lo desarrollado, se debe tener claro que los delitos informáticos son actos delictivos que son realizados haciendo uso de medios tecnológicos. Las diferentes modalidades que existen y surgirán con el tiempo están en función al desarrollo y evolución de la tecnología, toda vez que cuando existen nuevos medios de interacción, también existirán nuevos delitos y nuevas formas de llevar a cabo los delitos tradicionales.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

La presente tesis ha sido desarrollada desde un enfoque cualitativo. Al respecto, Nizama y Nizama (2020), explicaron que este enfoque se centra en la coexistencia de los seres humanos en escenarios reales y naturales; además, prioriza el análisis y la práctica de los valores, debido a que afectan la interpretación de problemas.

Asimismo, el enfoque cualitativo busca estudiar fenómenos de forma ordenada y metódica; por lo que, inicia indagando los hechos y revisando los estudios anteriores de manera simultánea, con el objetivo de desarrollar una teoría congruente con la realidad problemática (Hernández-Sampieri y Mendoza, 2018).

Por otra parte, el tipo de investigación fue básica. Al respecto, Alvarez (2020) explicó que la investigación es básica cuando está enfocada en obtener conocimientos novedosos de manera sistemática, en aras de incrementar el bagaje cognitivo de una problemática en concreto.

Nicomedes (2018) explicó que la investigación básica, también llamada sustantiva, recibe esos nombres porque se interesa en la búsqueda de nueva sabiduría; por lo que, buscar plantar nuevos cimientos para la investigación tecnológica o aplicada.

El tipo de diseño fue de teoría fundamentada. Este diseño busca información sobre nuevos conceptos en patrones unificados y categorizados, realizando un análisis – a través de pasos rigurosos – y haciendo una comparación constante; por lo que, está diseñado para producir conceptos y teorías basadas en datos (De la Espriella y Gómez, 2020).

3.2. Categorías, subcategorías y matriz de categorización

Categoría 1:

Delitos informáticos. “Son actividades delictivas que crean perturbaciones en la red; por ejemplo, robando datos privados de gran importancia, o pirateando información bancaria y transfiriendo dinero ajeno” (Goni, Ali, Showrov, Alam y Shameem, 2022, p. 29).

Las definiciones de delitos informáticos afectan las estimaciones sobre el alcance de la ciberdelincuencia, las políticas para responder al problema, las estrategias para prevenirlo y las teorías usadas para explicar el comportamiento, demostrándose que los delitos informáticos pueden conceptualizarse – de manera tradicional – como una conducta desviada, una cuestión legal, el producto de una construcción social o un problema tecnológico. Esta precisión está guiada por el reconocimiento de que la ciberdelincuencia es de naturaleza global, cometida en la vasta área llamada ciberespacio, diferente de muchos otros delitos, poco estudiado en justicia penal, y mejor entendido a través de una lente multidisciplinaria (Payne, 2020).

Subcategorías:

Globalización. Kasych y Vochozka (2019) han explicado que durante el proceso de la globalización – como característica clave – debe tenerse en cuenta que “la falta de control y la incertidumbre dan testimonio de la incapacidad de cualquier institución y sistema para proporcionar regulación y ajuste de procesos en la dirección requerida” (p. 6).

Asimismo, Siregar y Sinaga (2021) han precisado que la globalización hace que el mundo no tenga fronteras, los países compiten libremente en varios campos y – en ocasiones – traspasan los límites jurisdiccionales de un país; en consecuencia, la superación del ciberdelito en la legislación es absolutamente necesaria. Por lo tanto, relacionado con la jurisdicción de este delito que es global, es necesario contar con una ley separada que lo regule.

Normativa penal. Villavicencio (2019) ha referido que el poder penal consiste en aplicar la coerción estatal haciendo uso del sistema penal, el cual está compuesto por un grupo de agencias y actividades – que participan en la formación y aplicación de la normativa penal –; y además, por instituciones de control penal.

Categoría 2:

Unidad Fiscal Especializada en Ciberdelincuencia. Es un piloto de Fiscalía Especializada en ciberdelincuencia que fue implementada a finales de 2020 y cuenta con competencia a nivel nacional (OFAEC, 2021).

Subcategorías:

Derecho Comparado. Villanueva (2023) ha indicado que la comprensión normativa del derecho frecuentemente pasa por alto cuestiones fácticas igualmente importantes para proporcionar una respuesta coherente más allá de la mera intuición; por lo que, el derecho comparado ha sido una herramienta consuetudinaria para generaciones de estudiosos del derecho. El enfoque del derecho comparado fue más allá del estudio del derecho, involucrando la historia, los eventos sociales, el idioma y la cultura del sistema bajo investigación.

Aunado a ello, Siems (2022) ha señalado que el derecho comparado ofrece una base sólida en el tema para estudiantes y académicos por igual, que cubre discusiones académicas esenciales y metodología del derecho comparado; además, debate críticamente los enfoques tradicionales y modernos de la disciplina, utilizando ejemplos de una variedad de jurisdicciones para brindar al lector una perspectiva verdaderamente global.

Ministerio Público. La Autoridad Nacional del Servicio Civil (2021) ha comentado que el Ministerio Público es una institución autónoma, cuyo propósito principal es perseguir y prevenir los delitos; y salvaguardar los derechos de la población, el interés público tutelado por norma y la legalidad.

3.3. Escenario de estudio

La presente tesis ha sido llevada a cabo en el Distrito Judicial del Santa, donde los participantes contribuyeron con su bagaje cognitivo, producto de su formación y vivencias profesionales. En paralelo, se utilizó doctrina nacional y – principalmente – extranjera como fuente de información, lo que ha sido el sustento para el presente trabajo.

3.4. Participantes

Debiendo ser personas expertas en la materias, los participantes han sido cinco abogados en ejercicio en el área penal en el Distrito Judicial del Santa, dado que en su labor diaria, son testigos de la comisión de diversos tipos penales, entre ellos, los delitos informáticos.

3.5. Técnicas e instrumentos de recolección de datos

En primer lugar, la entrevista fue la técnica usada con los participantes de la tesis. Según Feria, Matilla y Mantecón (2020), es una forma de indagación de nivel empírico y de índole administrativo, haciendo uso de una comunicación interactiva con diversos participantes, con el objetivo de recabar – mediante un cuestionario o una guía – sus puntos de vista respecto a una problemática en particular.

En segundo lugar, la guía de entrevista fue el instrumento que se utilizó para obtener los datos. Haciendo uso de este, se buscó que los participantes plasmen sus respuestas de manera libre; por lo que, las preguntas fueron de forma abierta, guardando relación tanto con el objetivo general como con los específicos.

Por último, la guía de entrevista estuvo compuesta por doce preguntas y todas fueron de tipo ensayo. Además, en la guía se especificó a que objetivo guarda relación cada pregunta. Sumado a ello, previo a las preguntas, se describió el propósito de la guía y el título de la presente tesis.

3.6. Procedimiento

En primer lugar, se elaboró la guía de entrevista. Posterior a ello, se buscó a sujetos que cumplan con las características específicadas. Una vez que se seleccionó a los participantes – y estos aceptaron –, se coordinó una visita, en la cual se les facilitó la hoja de consentimiento informado, para que de manera formal muestren su conformidad. Acto siguiente, se realizó la entrevista, haciendo uso de la guía de entrevista. En algunos casos, el proceso se realizó de manera virtual. Finalmente, se guardaron los datos recabados para su análisis en la etapa respectiva.

3.7. Rigor científico

La National Library of Medicine (citado por Hofseth, 2017) lo definió como la aplicación meticulosa de la técnica científica para garantizar un diseño experimental y una metodología; además, busca que el informe de resultados sea neutral, producto de un buen análisis e interpretación. Asimismo, precisa que esto incluye total transparencia en el informe para que otros puedan tener acceso a esta y amplíen los hallazgos.

En primer lugar, el presente trabajo contó con credibilidad, dado que la información que se obtuvo de la recolección de datos son verdaderos y, muestran una imagen representativa y fiel de la realidad problemática que se estudió.

Y en segundo lugar, el presente trabajo contó con confirmabilidad, dado que se registró de manera completa y detallada todas las actividades realizadas respecto al objeto de estudio. En consecuencia, me permitió examinar la información obtenida y arribar a resultados análogos.

3.8. Método de análisis de datos

Rojas (2023) comentó que es un proceso complejo, cuyo fin es conseguir un resultado sobre la base de los objetivos planteados inicialmente, sometiendo a análisis los datos recabados.

El método cualitativo fue el que se utilizó, dado que me permitió obtener conclusiones de información que no son expresadas de forma cuantificable; para lo cual, hice uso de la entrevista.

3.9. Aspectos éticos

La presente tesis ha sido desarrollada respetando todos los principios, la ética y la moral. Toda la información ha sido obtenida de manera honesta y legal, respetando la propiedad intelectual de los trabajos que han sido citados y referenciados siguiendo la normas APA actuales; por lo que, todo es verídico. Además, la información y datos recabados mediante las entrevistas han sido utilizados con la reserva debida y solo para fines académicos.

IV. RESULTADOS Y DISCUSIÓN

Objetivo General: Determinar la implicancia existente entre los delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público del Perú.

Tabla 1 : Opinión respecto si la ciberdelincuencia es un problema jurídico actual

Pregunta 1				
¿Considera que la ciberdelincuencia es un problema jurídico actual? ¿Por qué?				
Entrevistado 1	Entrevistado 2	Entrevistado 3	Entrevistado 4	Entrevistado 5
Sí, porque a pesar de que hay leyes que castigan penalmente, aún existen personas inescrupulosas que aún lo hacen.	Porque cada vez existe mayor manejo de la virtualidad para realizar las labores cotidianas, y la delincuencia no se queda atrás.	Sí.	Sí, un arma más accesible y concurrida para la criminalidad.	Sí, porque actualmente en el siglo XXI se han incrementado los ataques cibernéticos, como por ejemplo: la clonación, cuentas bancarias, robo de datos personales, hackeos cibernéticos de las redes sociales.

Fuente: Elaboración propia (2023).

Respecto a la primera pregunta, todos los participantes han coincidido en su respuesta y consideran a la ciberdelincuencia como un problema jurídico actual. Cuatro de los participantes sustentaron su respuesta y – tomando todo en cuenta – señalaron que los delincuentes se aprovechan de los avances tecnológicos para cometer delitos; por lo que, se han incrementado los ataques cibernéticos.

Al respecto, Huamán (2020) ha referido que la accesibilidad cada vez más común al ciberespacio, sumado a la facilidad de acceder a internet, a las redes sociales, entre otros, ha facilitato las actividades de los seres humanos; no obstante, representa un herramienta cómoda para los delincuentes cibernéticos, quienes encuentran un medio accesible y sin fronteras para cometer delitos informáticos.

El investigador comparte la opinión de los participantes, es claro que la ciberdelincuencia es un problema jurídico actual que requiere una atención inmediata, dado que estamos adentrándonos cada vez más a un mundo digital, y esto no puede ser motivo para que se cometan delitos informáticos con más facilidad, dado que según la Divindat (citado por Pichihua, 2023), en 2022 se recibieron 3, 946 denuncias por delitos informáticos.

Tabla 2 : Opinión respecto si la normativa nacional – Ley de ciberdefensa y la Ley de delitos informáticos – y la internacional – Convenio de Budapest – están actualizadas y son adecuadas para regular la gama de los delitos informáticos

Pregunta 2				
¿Considera que la normativa nacional – Ley de ciberdefensa y la Ley de delitos informáticos – y la internacional – Convenio de Budapest – están actualizadas y son adecuadas para regular la gama de los delitos informáticos? ¿Por qué?				
Entrevistado 1	Entrevistado 2	Entrevistado 3	Entrevistado 4	Entrevistado 5
Sí, pero particularmente considero que deberían actualizarlas puesto que la tecnología de hoy está muy avanzada.	En cierto modo, aunque debe existir mayor regulación específica para frenar la delincuencia, porque cada día que pasa la delincuencia avanza también.	Considero que no es suficiente porque en la realidad estos no son aplicados debidamente, por ende, debe existir una ley más estricta respecto a los delitos de ciberdelincuencia.	Deben reforzarse.	No están actualizadas, porque los paises desarrollados cuentan con mayor tecnología que los países como nosotros, lo que debería es estar actualizadas las normas, no solo nacional, sino internacional.

Fuente: Elaboración propia (2023).

Respecto a la segunda pregunta, los entrevistados 2, 3, 4 y 5 han considerado que la normativa nacional e internacional no están actualizadas y no son adecuadas para regular la gama de delitos informáticos, dado que han señalado que estas deben reforzarse, ser más estrictas y, además, debe existir mayor regulación específica que esté al corriente de la delincuencia.

Por otro lado, el entrevistado 1 ha respondido de manera afirmativa; sin embargo, precisó que la normativa nacional e internacional deben estar actualizadas sobre la base de los avances tecnológicos.

Al respecto, la Defensoría del Pueblo (2023) ha explicado que la extensión acelerada de la ciberdelincuencia ha ido forzando a los Estados a desarrollar sus propios diagnósticos para identificar y, evaluar sus causas y efectos en los derechos de la población y en las instituciones de gobierno. Además, señaló que en ciertos países, la atención y tratamiento de la ciberdelincuencia se ha efectuado con mayor énfasis y está incluido en sus políticas públicas; en consecuencia, ha conllevado a que disposiciones normativas de distinta índole sean promovidas y dictadas.

Carrera (2021) ha concluído que existe una mala aplicación normativa en nuestro país; además, la ley de delitos informáticos debe incluir tipos penales actuales y novedosos que regulen una mejor seguridad digital, dado que las medidas que son aplicadas tanto el Ministerio Público como la Policía Nacional, no se relacionan de manera eficaz a este tipo de delitos. Además, señaló que en muchos casos, los delitos informáticos actuales no se encuentran regulados; por lo que, los organismos de protección no cuentan con los conocimientos básicos de estos, como los elementos típicos. Sumado a ello, precisó que es necesario que la norma esté actualizada sobre la base de las nuevas modalidades de ciberdelitos.

El investigador comparte la opinión mayoritaria, tanto la normativa nacional como la internacional no están sujetas a los nuevos avances tecnológicos y los usos que se les están dado, especialmente la nacional. En los últimos años, el

mundo se ha modernizado de manera digital a gran escala, unos países más que otros, y el Perú no se ha quedado atrás. Y frente a estos cambios, los ciberdelincuentes se han adaptado y hacen uso de ellos para la comisión de sus crímenes; por lo que, la normativa nacional e internacional deben estar actualizadas y, ser adecuadas para regular los actuales y nuevos delitos informáticos.

Tabla 3 : Opinión respecto si las Fiscalías existentes del Ministerio Público están preparadas y son suficientes para identificar, investigar y sancionar los delitos informáticos

Pregunta 3				
¿Considera que las Fiscalías existentes del Ministerio Público están preparadas y son suficientes para identificar, investigar y sancionar los delitos informáticos? ¿Por qué?				
Entrevistado 1	Entrevistado 2	Entrevistado 3	Entrevistado 4	Entrevistado 5
Sí, considero que de acuerdo a las leyes que se formaron, están bien establecidas.	No, porque estadísticamente se demuestra que los procesos no son favorables para determinar.	No, porque si comprobamos no tienen carga procesal; es decir, no existen muchos procesos en investigación sobre los delitos informáticos, debido a que, no existen los medios idóneos para lograr una investigación idónea.	Necesitan especialización.	No, ya que no están actualizadas con los tipos de ataques cibernéticos y; por lo tanto, la mayoría de casos son archivados, también porque en Perú, no se cuenta con material logístico y científico para erradicar estos delitos.

Fuente: Elaboración propia (2023).

Respecto a la tercera pregunta, los entrevistados 2, 3, 4 y 5 han coincidido en que las Fiscalías existentes no están preparadas y no son suficientes para identificar, investigar y sancionar los delitos informáticos. El entrevistado 2 ha precisado que las Fiscalías existentes no cuentas con los medios para lograr una investigación idónea de los delitos informáticos. En esa misma línea, el entrevistado 5 ha precisado que no cuentan con material logístico y científico para erradicar esos delitos; por lo que, la mayoría de casos son archivados. El entrevistado 4 ha precisado que necesitan especialización.

Por otro lado, el entrevistado 1 ha respondido de manera positiva, explicando que las Fiscalías existentes están bien establecidas de acuerdo a las leyes sobre las que se formaron.

Al respecto, Bernal y Menacho (2021) han manifestado que no existen recursos logísticos y humanos suficientes para abastecer la gran comisión de delitos informáticos a nivel nacional; además, los fiscales no poseen conocimientos especializados que estén vinculando a la ciberdelincuencia.

Asimismo, Carrera (2021) ha explicado que es menester la aplicación de una nueva campaña en donde el gobierno brinde capacitación en materia legal a todos sus administradores de justicia en aras de buscar beneficios dentro del ciberespacio y plantear derechos que sean congruentes con la pena del delito y responsabilidad respecto a la víctima.

Por su parte, Cuadros (citado por Bernal y Menacho, 2021) ha señalado que en estos días, es vital que todo abogado – indepedientemente de sus labores – cuente con conocimientos en tecnología, y no con el fin de detectar o llevar casos de delitos informáticos, sino teniendo en cuenta que – en la actualidad – cualquier individuo puede tener acceso al ciberespecio, donde diferentes ilícitos pueden ser cometidos.

El investigador comparte la opinión mayoritaría, las Fiscalías existentes no están preparadas ni son suficientes para combatir la ciberdelincuencia. La falta de Fiscalías Especializadas en Ciberdelincuencia ocasiona que los casos de

delitos informáticos no sean identificados, investigados, ni sancionados; por lo que, es menéster que existan dichas Fiscalías. Además, se necesitan especializar a las actuales en temas de ciberdelincuencia para que estén preparadas frente a cualquier comisión de estos delitos.

Tabla 4 : Opinión respecto a la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú

Pregunta 4				
¿Qué opina de la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú?				
Entrevistado 1	Entrevistado 2	Entrevistado 3	Entrevistado 4	Entrevistado 5
Ya existe en Lima, pero considero que debería descentralizarse.	Que las autoridades deben preocuparse más en la prevención de este tipo de delitos, que, en implementar fiscalías especializadas que no investigan como deberían.	Me parece que está bien, ya que en el Perú se ha visto que últimamente hay muchos casos que se deberían castigar penalmente.	Un gran avance, necesita más presupuesto.	Que debería implementarse dicha Unidad especializada porque contribuiría a erradicar estos delitos.

Fuente: Elaboración propia (2023).

Respecto a la cuarta pregunta, los entrevistados 1, 3, 4 y 5 han considerado la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia en el Perú como algo positivo; no obstante, precisaron que esta debe descentralizarse y necesita más presupuesto. El entrevistado 2 ha indicado que el enfoque de las autoridades debe estár en la prevención de los delitos cibernéticos y no en la

implementación de Fiscalías especializadas que no realizan una adecuada investigación.

Al respecto, Bernal y Menacho (2021) han señalado que con la implementación de una Unidad Fiscal Especializada en Ciberdelincuencia, se logró el primer avance de una gran deuda pendiente con la nación; sin embargo, precisaron que una de las principales desventajas es su ámbito de competencia, dado que sería un órgano con función informativa y de consultoría.

Asimismo, Cuadros (citado por Bernal y Menacho, 2021) ha manifestado que la implementación de esta unidad es un acierto, dado que se recabará información relevante que facultará – a su vez – la elaboración de un muestreo de los lugares con una comisión alta de ciberdelitos.

El investigador comparte la opinión mayoritaria, la implementación de una Unidad Fiscal Especializada en Ciberdelincuencia en nuestro país es una gran avance en la lucha contra la ciberdelincuencia; además, se implementó de manera conjunta un laboratorio de ciberdelincuencia y una red de fiscales en ciberdelincuencia – labor adicional a sus funciones – en todo el país. Todo estos actos han posicionado al Perú en una mejor posición de defensa frente a los delitos informáticos, pero aún no es suficiente.

Tabla 5 : Opinión respecto si existe relación entre los delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia

Pregunta 5				
¿Considera que existe relación entre los delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia? ¿Por qué?				
Entrevistado 1	Entrevistado 2	Entrevistado 3	Entrevistado 4	Entrevistado 5
Porque el mismo nombre lo dice, hay coherencia entre el delito cibernético y la fiscalía especializada en ciberdelincuencia.	Sí, porque esta institución es la encargada de salvaguardar el bien jurídico tutelado respecto a los delitos informáticos.	Sí, porque ambos tienen que ver con la delincuencia informática.	Así es, se implementó para combatir este tipo de delincuencia.	Porque guardan relación, los delitos informáticos, en nuestro Código Penal son genéricos, y si existe una Unidad Fiscal especializada será más amplia en estos delitos.

Fuente: Elaboración propia (2023).

Respecto a la quinta pregunta, los entrevistados – de manera unánime – han considerado que sí existe relación entre los delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia. Al respecto, el entrevistado 1 ha precisado que existe coherencia en su relación. El entrevistado 2 ha sustentado que la relación radica en que la mencionada institución es la encargada de proteger el bien jurídico vulnerado por los

ciberdelitos. El entrevistado 4 ha indicado que la relación radica en que la unidad fue implementada para combatir la ciberdelincuencia.

El investigador comparte la opinión unánime, la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia guarda relación significativa con los delitos informáticos, dado que fue implementada para unificar criterios de aplicación normativos y orientar – de manera técnica – las investigaciones fiscales de los estos, además de los delitos tradicionales en donde la prueba digital sea imprescindible para su esclarecimiento. Sumado a ello, para su óptimo funcionamiento, se requiere actualizar la normativa jurídica sobre ciberdelincuencia.

Respecto al objetivo general, el investigador arriba al siguiente **resultado**: Frente al gran aumento de delitos informáticos en nuestro país, la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público ha sido implementada para acompañar de manera técnica – en la identificación, investigación y sanción de estos tipos penales – a los fiscales mediante el uso de recursos tecnológicos, ayudando a evitar que estos tipos penales queden impunes. Sumado a ello, nuestra normativa nacional no está actualizada a los últimos tipos penales informáticos; por lo que, los fiscales no poseen el sustento jurídico adecuado para hacer frente a estos delitos.

Objetivo Específico 1: Identificar si existen doctrinas y teorías modernas suficientes sobre los delitos informáticos.

Tabla 6 : Opinión respecto si la doctrina actual es vasta y suficiente para estudiar los delitos informáticos

Pregunta 6				
¿Considera que la doctrina actual es vasta y suficiente para estudiar los delitos informáticos? ¿Por qué?				
Entrevistado 1	Entrevistado 2	Entrevistado 3	Entrevistado 4	Entrevistado 5
No, porque no está muy desarrollada por los juristas, dado que este delito se ha venido desarrollando a raíz de la implementación de la virtualidad progresiva.	No, porque todavía existen vacíos legales, doctrinarios y jurisprudenciales.	Considero que se debería actualizar pues ya hay muchas doctrinas pasadas que no son de tiempos de hoy.	Es necesario profundizar, es un nuevo tipo de delito.	No, porque en nuestra doctrina no se cuenta con doctrina actualizada, y sobre todo en delitos informáticos, muy diferente que en otros países.

Fuente: Elaboración propia (2023).

Respecto a la sexta pregunta, los entrevistados 1, 2 y 5 han considerado que la doctrina actual no es vasta ni suficiente para estudiar los delitos informáticos. El entrevistado 1 ha indicado que estos delitos no están muy desarrollados debido a que son recientes, producto de la virtualidad progresiva. El entrevistado 2 ha precisado que el motivo es porque existen vacíos legales, doctrinarios y

jurisprudenciales, mientras que el entrevistado 5 precisó que es porque la doctrina no está actualizada, a comparación del extranjero.

Por otro lado, el entrevistado 3 ha explicado que la doctrina actual es antigua; por lo que, debería actualizarse. El entrevistado 4 ha mencionado la necesidad de profundizar en la doctrina actual, dado que es un nuevo tipo de delito.

Al respecto, Bernal y Menacho (2021) han señalado que los fiscales no poseen un bagaje cognitivo especializado en ciberdelincuencia. Además, indican que las capacitaciones brindadas por la Escuela del Ministerio Público y la Academia de la Magistratura son insuficientes, dado que el nivel de especialización requerido reviste una mayor complejidad para investigar y sancionar los delitos informáticos.

Aunado a ello, Cuadros (citado por Bernal y Menacho, 2021) ha precisado que la única manera de afrontar los delitos informáticos es con conocimiento; por lo que, si no se cuenta con la información adecuada sobre los riesgos del ciberespacio, es muy poco o nada lo que se puede hacer para prevenir la ciberdelincuencia.

El investigador comparte la opinión mayoritaria, la doctrina actual no es vasta ni suficiente para estudiar los delitos informáticos. Si bien en los últimos años, se tomó mayor importancia al mundo digital, aún le falta mucho al Perú para estar preparado y brindar protección frente a las amenazas que los avances tecnológicos traen consigo. La falta de doctrina referente a la ciberdelincuencia se ve reflejada en la práctica; en consecuencia, muchos casos de delitos informáticos son archivos porque los fiscales no están preparados y no tienen fuentes doctrinarias a las cuales recurrir, muchos menos a la norma que está desactualizada. Por lo tanto, es importante que se promueva la elaboración y desarrollo de artículos e investigaciones sobre el ciberespacio y la delincuencia de este, a efectos de brindar material informativo y de preparación para los prosecutores de justicia y que estos – conjuntamente con los magistrados – puedan usarlo en la identificación, investigación y sanción de los ciberdelitos.

Tabla 7 : Opinión respecto si la teoría clásica del delito debe ser tomada en cuenta para explicar la naturaleza de los delitos informáticos

Pregunta 7

¿Considera que la teoría clásica del delito debe ser tomada en cuenta para explicar la naturaleza de los delitos informáticos? ¿Por qué?

Entrevistado 1	Entrevistado 2	Entrevistado 3	Entrevistado 4	Entrevistado 5
Se puede tomar en cuenta para establecer un punto de partida, porque no existe mayor ahondamiento actualmente.	.	Considero que sí.	Se debe profundizar en cada tipo penal y su naturaleza jurídica.	Sí, sería como una base en estas clases de delitos, pero debe incrementarse y actualizarse la doctrina y jurisprudencia de otros países.

Fuente: Elaboración propia (2023).

Respecto a la séptima pregunta, los entrevistados 3 y 5 han considerado que la teoría clásica del delito debe ser tomada en cuenta para explicar la naturaleza de los delitos informáticos. El entrevistado 5 ha explicado que la teoría clásica del delito serviría como base; no obstante, debe actualizarse.

Por otro lado, el entrevistado 1 ha indicado que la teoría clásica del delito solo serviría como un punto de partida, dado que no existe mayor información al respecto. Por su parte, el entrevistado 4 ha señalado que lo que se debe hacer es profundizar en cada tipo penal y su naturaleza jurídica. El entrevistado 2 no respondió esta pregunta.

Chandra y Snowe (2020) han desarrollado una teoría de ciberdelincuencia basada en una taxonomía. Esta taxonomía sigue una estructura jerárquica que utiliza el concepto padre-hijo para representar cada categoría de delitos cibernético.

La información para describir un elemento típico de la taxonomía se divide en cuatro capas: de nivel, de nombre, de datos y de víctima. La capa de nivel utiliza el formato numérico de capa-subcapa para indicar la progresión de una categoría amplia a una específica y asigna una ubicación precisa en la taxonomía. La capa de nombre describe e identifica de forma descriptiva cada elemento. La capa de datos proporciona información sobre la definición, el vínculo del elemento con su raíz o padre, las características del elemento (como características heredadas, evolucionadas o únicas) y el proceso general para cometer el delito cibernético. La capa de víctima vincula cada delito cibernético con su impacto directo e inmediato. En este sentido, el elemento taxonómico representa los conceptos de herencia (jerárquica y padre-hijo), encapsulación y evolución (para denotar rasgos heredados y evolucionados o individuales). La función de herencia garantiza que el elemento secundario tenga las mismas propiedades, comportamiento y restricciones que el elemento principal. El elemento hijo también tiene propiedades, comportamiento o restricciones adicionales. Por ejemplo, un vehículo de dos ruedas es un tipo de vehículo; todos los vehículos de dos ruedas son vehículos, pero no todos los vehículos son vehículos de dos ruedas. Por lo tanto, el elemento hijo está característicamente más especializado en sus propiedades, comportamiento y restricciones que el elemento padre (Chandra y Snowe, 2020).

Chandra y Snow (2020) han concluído que la importancia de su teoría basada en una taxonomía radica en proporcionar una definición clara, una clasificación coherente y características de varios tipos de delitos cibernéticos. Los cuatro componentes básicos de su taxonomía proporcionan la base teórica (exclusividad mutua, exhaustividad colectiva, estructura y categorías bien definidas), al tiempo que garantizan su estabilidad, incluso a medida que la tecnología evoluciona en el futuro. Al validar su taxonomía usando ejemplos y

heurística, se proporciona una prueba de concepto. Las extensiones futuras pueden incluir la implementación de esta taxonomía en entornos organizacionales, el desarrollo de métricas para medir parámetros específicos de la taxonomía, la integración de su taxonomía de ciberdelincuencia con la de los delitos tradicionales (fuera de línea) y la automatización de elementos de la taxonomía para lograr eficiencias.

El investigador comparte la opinión de los entrevistados 1 y 5, la teoría clásica del delito debe ser tomada en cuenta para dar un enfoque general de los delitos informáticos, y dado que no existe información doctrinaria nacional propia de estos, debe recurrirse a fuentes extranjeras.

Respecto al objetivo específico 1, el investigador arriba al siguiente **resultado**: La doctrina nacional es escasa e insuficiente en cuanto a ciberdelincuencia; en consecuencia, los operadores de justicia no cuentan con materia bibliográfico que los faculten a identificar correctamente los delitos informáticos y; por consiguiente, investigarlos apropiadamente. Además, se tiene a la teoría clásica del delito como base para estudiar los ciberdelitos, cuando se requieren teorías especializadas en estos tipos penales. Por lo que, ante la falta de doctrina y teorías jurídicas, es viable recurrir al plano internacional para identificarlas e implementarlas en nuestra sistema jurídico. El investigador considera que la teoría de Chandra y Snow basada en una taxonomía es adecuada para englobar y estudiar a los delitos informáticos actuales y futuros.

Objetivo Específico 2: Comparar la Unidad Fiscal Especializada en Ciberdelincuencia con sus similares en otros países.

Tabla 8 : Opinión respecto si a nivel internacional, existen países que están mejor preparados en temas cibernéticos en cuanto a normativa e instituciones jurídicas

Pregunta 8				
¿Considera que a nivel internacional, existen países que están mejor preparados en temas cibernéticos en cuanto a normativa e instituciones jurídicas? ¿Por qué?				
Entrevistado 1	Entrevistado 2	Entrevistado 3	Entrevistado 4	Entrevistado 5
Sí.	Por el mismo desarrollo de otros Estados.	Claro, es porque se enfocan bastante en su realidad; es decir, analizan los hechos que se presentan y en base a ello formulan una legislación acorde, además de los sistemas electrónicos avanzados que poseen.	Porque la figura jurídica se ha regulado mucho tiempo antes.	Sí, por cuanto tienen mejor tecnología, científica, sobre todo en los países desarrollados, ellos están mejor implementados con tecnología avanzada.

Fuente: Elaboración propia (2023).

Respecto a la octava pregunta, los entrevistados – de manera unánime – han considerado que a nivel internacional, existen países que están mejor preparados en temas cibernéticos en cuanto a normativa e instituciones jurídicas. El entrevistado 2 ha precisado que el motivo radica en el mismo desarrollo de los Estados extranjeros. El entrevistado 3 ha explicado que el motivo radica en que los países extranjeros elaboran una legislación acorde a los hechos que se suscitan en su realidad, sumado a los sistemas electrónicos avanzados que poseen. El entrevistado 4 ha indicado que el motivo radica en que los delitos informáticos – en países extranjeros – llevan mucho tiempo de regulación. El entrevistado 5 ha explicado que el motivo radica en que los países extranjeros están mejor implementados y poseen tecnología avanzada.

Al respecto, Huamán (2020) ha señalado que la normativa sobre ciberdelincuencia en países sudamericanos que han suscrito el Convenio de Budaspest ha sufrido una uniformización respecto del contenido del mismo. Además, explicó que en este ámbito, nuestro país no posee una legislación conforme a dicho Convenio, en temas de cooperación universal.

Asimismo, Guerrero (citado por Bernal y Menacho, 2021) ha explicado que nuestro país no solo es uno de los últimos en suscribirse al Convenio de Budapest, sino que otros lo hicieron con varios años de antelación.

Por otro lado, Carrera (2021) ha referido que en el país de El Salvador se ha propuesto mejorar la habilidad de obtener información de los organismos administradores de justicia, en aras de publicitar los nuevos ciberdelitos y sus modalidades aplicables frente a los cambios normativos conforme al nuevo control tecnológico.

El investigador comparte la opinión unánime de los entrevistados, los países extranjeros cuentan con mejor preparación en ciberdelincuencia y tienen normativa e instituciones actualizadas referentes a este. Internacionalmente, existen países más desarrollados que cuentan con los últimos avances tecnológicos; y por ende, cuentan con un sistema de justicia adaptado a estos. Además, no solo están suscritos a convenios internacionales, sino que

interiorizan el contenido de los mismos a su normativa. A efectos de comparar, en Argentina, esta unidad fue implementada en 2015 y con el objetivo de trabajar en el área de la prevención general al ciudadano y de información al investigador en aras de conocer – con exactitud – los factores que una investigación debe tener en cuenta; y que, consecuentemente, pueda recabar las evidencias necesarias (Defensoría del Pueblo, 2021). Por nuestro lado, el Perú recién implementó dicha unidad a finales del 2020 con un rol informativo y de consultoría; por lo que, es evidente que el sistema de justicia peruano necesita reforzarse en cuanto a normativa e instituciones.

Tabla 9 : Opinión respecto si la Unidad Fiscal Especializada en Ciberdelincuencia – de nuestro país – debe tomar en cuenta lineamientos y medidas de instituciones especializadas en ciberdelincuencia extranjeras

Pregunta 9				
¿Considera que la Unidad Fiscal Especializada en Ciberdelincuencia – de nuestro país – debe tomar en cuenta lineamientos y medidas de instituciones especializadas en ciberdelincuencia extranjeras?				
Entrevistado 1	Entrevistado 2	Entrevistado 3	Entrevistado 4	Entrevistado 5
Sí, porque queramos o no, en otros países están mucho más avanzados de los cuales podemos tomarlo en cuenta.	Sí.	Sí, debe tomar en cuenta porque como ya dije antes, en otros países su legislación es mejor elaborada con el objeto de combatir los delitos informáticos.	Solo como referencia porque cada país tiene su propia sistematicidad.	Sí, debería tenerse algunos lineamientos, pero sobre todo, debe estar basado a nuestra realidad, y a los comportamientos de nuestro país, debería existir capacitaciones de otras instituciones extranjeras.

Fuente: Elaboración propia (2023).

Respecto a la novena pregunta, los entrevistados 1, 2, 3 y 5 han considerado que nuestra Unidad Fiscal Especializada en Ciberdelincuencia debe tomar en cuenta lineamientos y medidas de instituciones especializadas en ciberdelincuencia extranjeras. El entrevistado 1 ha basado su respuesta en que

otros países están mucho más avanzados. El entrevistado 3 ha sustentado su respuesta en que otros países cuentan con una legislación mejor elaborada con el fin de combatir la ciberdelincuencia. El entrevistado 5 ha explicado que debe tomarse algunos lineamientos basados en nuestra realidad, y que deberían existir capacitaciones de instituciones extranjeras.

Por otro lado, el entrevistado 4 ha considerado que los lineamientos y medidas de instituciones especializadas en ciberdelincuencia extranjeras solo deben tomarse en cuenta como referencia, dado que cada país cuenta con una sistematicidad propia.

Al respecto, la OFAEC (2021) ha explicado que el tipo de unidad que predomina entre los países de Iberoamérica es la Unidad de Coordinación Nacional con descentralización en la investigación, con labores de investigación en casos de alta compejidad y con potestad de coordinar con puntos de contacto en territorios específicos, del mismo modo que brinda capacitaciones, genera y promueve prácticas honestas a fiscalías que combatan ciberdelitos.

En esa misma línea, la Unidad Especializada de Delitos Informáticos de Paraguay tiene como función principal realizar las investigaciones en los delitos de su competencia; además, brinda apoyo técnico-jurídico y asesoramiento a los agentes fiscales (OFAEC, 2021).

Sumado a ello, Bernal y Menacho (2020) han señalado que es importante rescatar lo positivo de los demás estados vecinos y tratar de mejorarlo; por ejemplo, el país de Argentina incorporó Fiscalías Especializadas con participación como organismo completo, desde la etapa de investigación hasta la etapa de juzgamiento.

Asimismo, la Unidad Fiscal Especializada en Ciberdelincuencia de Argentina tiene como funciones principales intervenir en los casos de su competencia y asistir a los agentes fiscales; además, recibe denuncias y realiza investigaciones preliminares y genéricas (OFAEC, 2021).

En ese mismo sentido, Carrera (2021) ha referido que a efectos de las últimas regulaciones jurídicas, el Estado peruano puede usar como lineamientos convenios que tienen como objetivo otorgar una mejor seguridad jurídica respecto a la ciberdelincuencia.

El investigador comparte la opinión mayoritaria, el Estado peruano debe tomar en cuenta lineamientos y medidas de instituciones especializadas en ciberdelincuencia extranjeras. Existen países extranjeros que por el mismo desarrollo tecnológico avanzado en el que se encuentran, cuentan con normativa e instituciones mucho más antiguas y; por ende, actualizadas y con más experiencia que las nuestras. Por lo tanto, cuentan con mucha información y casuística que pueden servir como material de guía y estudio para el sistema de justicia peruano.

Respecto al objetivo específico 2, el investigador arriba al siguiente **resultado**: La implementación de una Unidad Fiscal Especializada en Ciberdelincuencia fue un gran acierto por parte del sistema de justicia peruano; no obstante, es un proyecto piloto por parte del Ministerio Público. Internacionalmente, existen instituciones especializadas en ciberdelincuencia – como en Paraguay y Argentina – que llevan muchos años en ejercicio; por lo que, cuentan con lineamientos actualizados a los delitos informáticos novedosos y experiencia en la investigación de estos. Por lo tanto, nuestra Unidad Fiscal Especializada en Ciberdelincuencia puede tomar como referencia la reglamentación y estudios de instituciones extranjeras, a efectos de adaptar lo que considere pertinente y adecuado para que le ayude en la identificación, investigación y sanción de la ciberdelincuencia.

Objetivo Específico 3: Analizar el avance en la identificación, investigación y sanción de los delitos informáticos tras la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia en el Perú.

Tabla 10 : Opinión respecto a la identificación, investigación y sanción de los delitos informáticos por parte del Ministerio Público

Pregunta 10				
En base a su experiencia, ¿qué opina de la identificación, investigación y sanción de los delitos informáticos por parte del Ministerio Público?				
Entrevistado 1	Entrevistado 2	Entrevistado 3	Entrevistado 4	Entrevistado 5
Es precario.	Que demoran demasiado en lograr el esclarecimiento de los hechos por la deficiencia electrónica que posee nuestro país.	Excelente, para así evitar que sigan obstruyendo las leyes.	Como no existe el suficiente presupuesto, la persecución de ese tipo de delitos es limitada.	Que, las penas y sanciones en nuestro país son muy blandas, debería incrementarse las penas y también con agravantes.

Fuente: Elaboración propia (2023).

Respecto a la décima pregunta, los entrevistados 1, 2, 4 y 5 han emitido una opinión negativa a la identificación, investigación y sanción de los delitos informáticos por parte del Ministerio Público. El entrevistado 1 ha considerado

que es precario. El entrevistado 2 ha explicado que existe deficiencia electrónica en nuestro país; en consecuencia, lograr el esclarecimiento de los hechos requiere de mucho tiempo. El entrevistado 4 ha precisado que la persecución de los delitos informáticos es limitada debido a la falta de presupuesto. El entrevistado 5 ha referido que las penas y sanciones son muy blandas; por lo que, deberían incrementarse y con agravantes.

Por otro lado, el entrevistado 3 ha emitido una opinión positiva a la identificación, investigación y sanción de los delitos informáticos por parte del Ministerio Público. Ha precisado que es excelente, dado que el Ministerio Público ayuda a evitar que los ciberdelincuentes sigan obstruyendo las leyes.

Al respecto, Carrera (2020) ha concluído que las deficiencias detectadas en la investigación fiscal son resultado de la falta de capacidad operativa de la DIVINDAT y, la carga procesal del Ministerio Público y la Policía Nacional; en consecuencia, se perjudica que se realice – de manera efectiva – las investigaciones por delitos informáticos. Además, ha explicado que producto del avance de la tecnología, nuvos tipos penales se han generado y estos no están regulados en la norma; por lo que, por desconocimiento, muchas veces no se identifica, investiga y sanciona la ciberdelincuencia.

El investigador comparte la opinión mayoritaria; la identificación, investigación y sanción de los delitos informáticos por parte del Ministerio Público es muy precaria, además de requerir demasiado tiempo y ser limitada. Existen muchas razones para esto. En primer lugar, el Ministerio Público no está bien implementando en cuanto a material tecnológico para combatir este tipo de delitos. En segundo lugar, no existe normativa que haya tomado en cuenta las nuevas modalidades y el avance tecnológico; por lo que, no existe sustento jurídico para sancionar la comisión de un ciberdelito. Por lo tanto, el Ministerio Público no está en una posición de realizar una adecuada identificación, investigación y sanción de la ciberdelincuencia.

Tabla 11 : Opinión respecto si ha llevado algún caso de delito informático reciente donde haya intervenido la Unidad Fiscal Especializada en Ciberdelincuencia y de ser afirmativo, sobre su participación

Pregunta 11				
¿Ha llevado algún caso de delito informático reciente donde haya intervenido la Unidad Fiscal Especializada en Ciberdelincuencia? De ser afirmativa su respuesta, ¿qué opina de su participación?				
Entrevistado 1	Entrevistado 2	Entrevistado 3	Entrevistado 4	Entrevistado 5
No.	Sí, y a la fecha no hay mayor razón sobre el avance del proceso que se lleva en Lima, respecto a un hurto usando medios tecnológicos.	No he llevado.	Aún no.	He participado en una investigación de delito informático, pero por falta de equipos tecnológicos, no se pudo recabar toda la información, esto conlleva que no haya un buen resultado.

Fuente: Elaboración propia (2023).

Respecto a la decimoprimera pregunta, el entrevistado 2 ha respondido que lleva un caso de delito informático donde ha intervenido la Unidad Fiscal Especializada en Ciberdelincuencia; sin embargo, no hay mayor razón sobre el avance de este caso. El entrevistado 5 ha respondido que ha participado en un

caso de delito informático; sin embargo, no se pudo obtener toda la información necesaria debido a la falta de equipos tecnológicos.

Por otro lado, los entrevistados 1, 3 y 4 han respondido de manera negativa, sin más detalle.

Respecto a avances, la Unidad Fiscal Especializada en Ciberdelincuencia ha instaurado una alianza estratégica de gran importancia con el Programa Global sobre Ciberdelincuencia de la Oficina de la Naciones Unidas contra la Droga y el Delitos – UNODC –, que le facultado organizar cursos especializados y básicos para todo su personal, así como para los miembros de la red de fiscales a nivel nacional. Esto ha permitido la elaboración de catorce módulos de capacitación respecto de los métodos de investigación de los delitos informáticos y otros temas relacionados, que fueron publicados en 2022 (Defensoría del Pueblo, 2023).

Según la DIVINDAT (citado por EYNG – Estrategias y Negocios –, 2023), se registran de manera mensual más de 300 denuncias de delitos informáticos; por ejemplo, en enero del presente año, se registraron 316 denuncias. Sin embargo, la cantidad de detenidos por estos delitos se ha incrementado, en el año 2021, hubieron 135 detenidos por ciberdelincuencia, mientras que en el año 2022, 229 detenidos. Además, se debe tener en cuenta que en 2021 hubieron 5620 denuncias; mientras que en 2022, 3946 denuncias.

En base a las respuestas, el investigador considera que al ser la Unidad Fiscal Especializada en Ciberdelincuencia un proyecto piloto y reciente, todavía le falta tiempo y logística para ser capaz de brindar asesoría a las diferentes fiscalías a nivel nacional; por lo que, los casos de delitos informáticos aún siguen siendo tediosos y con resultados desfavorables. Sin embargo, es un buen inicio contar con dicha unidad, ya que la cantidad de detenidos por delitos informáticos va en aumento.

Tabla 12 : Opinión respecto si se debe implementar una Fiscalía Especializada en Ciberdelincuencia en cada distrito fiscal

Pregunta 12

¿Considera que se debe implementar una Fiscalía Especializada en Ciberdelincuencia en cada distrito fiscal? ¿Por qué?

Entrevistado 1	Entrevistado 2	Entrevistado 3	Entrevistado 4	Entrevistado 5
Sí, para así evitar la carga procesal en diversas fiscalías.	Sí, porque de esta forma se logrará prosperar en los casos como se espera.	No, se debe implementar personal mejor capacitado.	Porque el delito no escatima competencia territorial, urge su implementación.	Sí, porque se está incrementando cada día esta clase de delitos y no sobre todo en clonación de tarjetas; sino en otros delitos como extorsiones, sicariato, que utilizan estos para poder cometer estos delitos.

Fuente: Elaboración propia (2023).

Respecto a la decimosegunda pregunta, los entrevistados 1, 2, 4 y 5 han respondido de manera positiva. El entrevistado 1 ha sustentado su respuesta en que la carga procesal de diversas fiscalías sería evitada. El entrevistado 2 ha basado su respuesta en que los casos podrán prosperar como se espera. El entrevistado 4 ha precisado que su implementación es requerida debido a que el delito no escatima competencia territorial. El entrevistado 5 ha sustentado su respuesta en que los delitos informáticos están en aumento y son muy variados.

Por otro lado, el entrevistado 3 ha respondido de manera negativa, precisando que lo que se debe implementar – en lugar de una una Fiscalía Especializada en Ciberdelincuencia en cada distrito fiscal – es personal mejor capacitado.

Al respecto, Elías (citado por Bernal y Menacho, 2020) ha manifestado que se deben implementar fiscalías especializadas en ciberdelincuencia en los distritos fiscales donde se presente mediana intensidad delictiva con el fin de que puedan comenzar a laborar y determinar la forma en que el Ministerio Público responde ante estas situaciones delictivas.

El investigador comparte la opinión mayoritaria, se debe implementar una Fiscalía Especializada en Ciberdelincuencia en cada distrito fiscal. Estando ya en el año 2023, no es factible que solo se haya implementado una Unidad Fiscal Especializada en Ciberdelincuencia y – a petición de esta – solo una Fiscalía Especializada en Ciberdelincuencia en el distrito fiscal de Lima Centro. Dada la gran gama de delitos informáticos que existen en la actualidad y las nuevas modalidades que surgirán, se debe descentralizar las instituciones especializadas en ciberdelincuencia e implementar una Fiscalía Especializa en cada distrito fiscal, empezando por aquellos donde exista una mayor carga procesal en cuanto a ciberdelitos.

Respecto al objetivo específico 3, el investigador arriba al siguiente **resultado**: Con la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia, se evidencia una mejora en la identificación, investigación y sanción de los delitos informáticos, dado que ha facultado herramientas modernas a los agentes fiscales y de capacitaciones especializadas; y esto se comprueba con el hecho de que la cantidad de detenidos – por estos tipos penales – ha sido mucho mayor en el año 2022 que en el 2021. No obstante, su avance se ve frenado, dado que requiere de la implementación de Fiscalías Especializadas en Ciberdelincuencia que tengan participación directa en la identificación, investigación y sanción de los delitos informáticos. Se debe tener en cuenta que ciberdelincuencia está en constante crecimiento y su comisión es

a nivel nacional; por lo que, se requieren instituciones especializadas en toda la República.

V. CONCLUSIONES

1. La Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público tiene implicancia significativa con los delitos informáticos, porque fue creada con el propósito de brindar apoyo técnico a los fiscales con herramientas digitales y asesoría especializada en la identificación, investigación y sanción de estos tipos penales.

2. En nuestro país, no existe doctrina suficiente ni teorías jurídicas referente a los delitos informáticos; por lo cual, existe la necesidad de desarrollar material académico y científico al respecto, con el fin de contar con soporte bibliográfico y de estudio.

3. La Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público del Perú, a diferencia de sus similares en países vecinos, ha sido implementada como un órgano informativo y consultor; por lo que, se requiere que sus funciones sean ampliadas, dado que no tiene mucha participación en los casos de delitos informáticos. Existen instituciones especializadas en ciberdelincuencia extranjeras que cuentan con varios años de experiencia y con funciones de órgano completo, como la de Argentina, que podrían ser tomadas como ejemplo a seguir.

4. Con la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia, se ha logrado un avance en la identificación, investigación y sanción de los delitos informáticos. No obstante, es menester contar con Fiscalías Especializadas en Ciberdelincuencia que tengan participación directa y que sean implementadas a nivel nacional.

VI. RECOMENDACIONES

1. La Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público debe asumir funciones de carácter resolutivo y competencias técnicas con el objetivo de investigar – de manera directa y propia – procesos complejos que poseen un modus operandi con alto grado de sofisticación en materia de ciberdelincuencia. Asimismo, se debe actualizar de manera constante la normativa referente a ciberdelincuencia.

2. El Ministerio Público debe promover la elaboración de artículos académicos y científicos en cuanto a ciberdelincuencia, así como desarrollar programas de capacitación de manera constante con las últimas modalidades de delitos informáticos. Por otro lado, se debe tomar en cuenta la implementación de teorías jurídicas extranjeras en ciberdelincuencia; por ejemplo , la teoría de Chandra y Snow.

3. El Ministerio Público debe rescatar lineamientos pertinentes y adecuados – que puedan ser implementados en nuestra Unidad Fiscal Especializada en Ciberdelincuencia – de instituciones especializadas en ciberdelincuencia extranjeras, con el fin de reforzar nuestra unidad para que – en un futuro – pueda asumir funciones de órgano completo.

4. Siendo la Unidad Fiscal Especializada en Ciberdelincuencia un órgano informativo y consultor, el Ministerio Público debe implementar fiscalías especializadas en ciberdelincuencia de manera progresiva a nivel nacional – según la carga procesal de cada distrito fiscal – en aras de ayudar en la identificación, investigación y sanción de los delitos informáticos.

REFERENCIAS

Autoridad Nacional del Servicio Civil (2021). *Estructura y Funcionamiento del Estado Peruano.* Escuela Nacional de Administración Pública. Recuperado de: https://cdn.www.gob.pe/uploads/document/file/2679306/Estructura%20y%20funcionamiento%20del%20Estado%20peruano.pdf

Alva, G. y Collave, Y. (s. f.). *Si ganaste un premio por actualizar tus datos desde el celular, te acaban de estafar*. https://especiales.elcomercio.pe/?q=especiales/estafas-electronicas-ecpm/index.html

Alvarez, A. (2020). *Clasificación de las Investigaciones*. Recuperado de: https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/10818/Nota%20Académica%202%20%2818.04.2021%29%20-%20Clasificación%20de%20Investigaciones.pdf?sequence=4

Applegate, S. y Stavrou, A. (2013). Towards a cyber conflict taxonomy. En K. Podings, J. Stinissen, M. Maybaum (Eds.), *5th internacional conference on cyber conflict* (pp. 1-18). NATO CCD COE Publications.

Barn, R. y Barn, B. (2016). An ontological representation of a taxonomy for cybercrime. *Research Papers, 45*, 12-15. http://aisel.aisnet.org/ecis2016_rp/45

Bernal, J. y Menacho, B. (2021). *Las fiscalías y los juzgados especializados en ciberdelincuencia y su implementación en el sistema de justicia del Perú, 2020.* [Tesis para optar el título profesional, Universidad Privada del Norte]. Repositorio Institucional UPN. https://hdl.handle.net/11537/26940

Carrera, I. (2021). *Deficiencias en las investigaciones por delitos de fraude informático en el destrito fiscal de Lima – 2021.* [Tesis de Maestría, Universidad César Vallejo]. Repositorio de la Universidad César Vallejo. https://hdl.handle.net/20.500.12692/71492

Chandra, A. y Snowe, M. (2020). A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems, 38*. https://doi.org/10.1016/j.accinf.2020.100467

CONSEJO NACIONAL DE POLÍTICA CRIMINAL (2020). *Diagnóstico situacional multisectorial sobre la ciberdelincuencia en el Perú*. Recuperado de: https://cdn.www.gob.pe/uploads/document/file/1616607/Diagnóstico%20Situacional%20Multisectorial%20sobre%20la%20Ciberdelincuencia%20%20en%20el%20Perú.pdf

De la Espriella, R. y Gómez, C. (2020). Grounded theory. *Revista Colombiana de Psiquiatría (English ed.), 49*(2), 126-132. https://doi.org/10.1016/j.rcp.2018.08.002

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

Donalds, C. y Osei-Bryson (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, 92, 403-418. https://doi.org/10.1016/j.chb.2018.11.039

EYNG (06 de junio de 2023). *Aumentan detenidos por delitos informáticos en Perú*. https://eyng.pe/web/2023/06/07/aumentan-detenidos-por-delitos-informaticos-en-peru/

Feria, H., Matilla, M. y Mantecón, S. (2020). La entrevista y la encuesta: ¿métodos o técnicas de indagación empírica?. *Didasc@lia: Didáctica y*

Educación, *11*(3), 62-79. https://dialnet.unirioja.es/descarga/articulo/7692391.pdf

Gallardo, E. (2017). *Metodología de la Investigación. Manual Autoformativo Interactivo.* Universidad Continental. https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_UC_EG_MAI_UC0584_2018.pdf

Goni, O., Ali, H., Showrov, I., Alam, M. y Shameem, A. (2022). The Basic Concept of Cyber Crime. *Journal of Technology Innovations and Energy, 1*(2), 29-39. https://doi.org/10.5281/zenodo.6499991

Graham, A. (2023). *Cybercrime: Traditional Problems and Modern Solutions*. [Master's thesis, Te Herenga Waka-Victoria University of Wellington]. Open Access Te Herenga Waka-Victoria University of Wellington. https://doi.org/10.26686/wgtn.22300909

Habirovs, A. (2018). *Factors that shape cybercrime victimization and use of prevention measures in England and Wales.* [Master's thesis, University of Huddersfield]. University of Huddersfield Repository. https://eprints.hud.ac.uk/id/eprint/35042/

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

Hofseth, L. (2018). Getting rigorous with scientific rigor. *Carcinogenesis, 39*(1), 21-25. https://doi.org/10.1093/carcin/bgx085

Huamán, M. (2020). *Los delitos informáticos en Perú y la suscripción del convenio Budapest*. [Tesis para optar el título profesional, Universidad Andina de Cusco]. Repositorio Digital Universidad Andina del Cusco. https://hdl.handle.net/20.500.12557/4116

INTERPOL (2021). *National Cybercrime Strategy Guidebook*. https://www.interpol.int/content/download/16455/file/Cyber%20Strategy%20Guidebook.pdf

Kasych, A. y Vochozka, M. (2019). Globalization processes in the modern world challenging the national economy development. *SHS Web of Conferences*, 65, 1-7. https://doi.org/10.1051/shsconf/20196509002

Leyva, C. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales*. Lucerna Iuris Et Investigatio,* (1), 29-47*.* http://dx.doi.org/10.15381/lucerna.v0i1.18373

Ley N.° 30096. Ley de Delitos Informáticos (22 de octubre de 2013). https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

Ley N.° 30171. Ley que modifica la Ley N.° 30096 (27 de marzo de 2014). https://www.leyes.congreso.gob.pe/Documentos/Leyes/30171.pdf

Ministerio Público Fiscalía de la Nación. (19 de octubre de 2021). *Ministerio Público registró más de 21 mil denuncias por delitos informáticos en los últimos años.* https://www.gob.pe/institucion/mpfn/noticias/546688-ministerio-publico-de-21-mil-denuncias-por-delitos-informaticos-en-los-ultimos-anos

Ministerio Público Fiscalía de la Nación. (22 de febrero de 2021). *Nueva Unidad Fiscal Especializada En Ciberdelincuencia inició sus funciones.* https://www.gob.pe/institucion/mpfn/noticias/343392-nueva-unidad-fiscal-especializada-en-ciberdelincuencia-inicio-sus-funciones

Moises, A. (2017). *Ciberdelitos Amenazas Criminales del Ciberespacio*. REUS.

Morón Lerma, E. (2016). *Nuevas tecnologías e instrumentos internacionales. Consecuencias penales. En F. Velásquez Velásquez, R. Vargas Lozano*

y J. D. Jaramillo Restrepo (Comps.), Derecho penal y nuevas tecnologías. A propósito del título VII bis del Código Penal. Universidad Sergio Arboleda.

Nicomedes, E. (2018). *Tipos de investigación*. Recuperado de: https://core.ac.uk/download/pdf/250080756.pdf

Nizama, M. y Nizama, L. (2020). EL ENFOQUE CUALITATIVO EN LA INVESTIGACIÓN JURÍDICA, PROYECTO DE INVESTIGACIÓN CUALITATIVA Y SEMINARIO DE TESIS. *VOX JURIS, 38*(2), 69-90. https://doi.org/10.24265/voxjuris.2020.v38n2.05

Observatorio Español de Delitos Informáticos (2021). *Estadísticas. Reporte de ciberdelitos en España.* Recuperado de: https://oedi.es/estadisticas/

Office of Civil and Criminal Justice Reform (2017). *Model Law on Computer and Computed Related Crime*. The Commonwealth. https://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf

OFICINA DE ANÁLISIS ESTRATÉGICO CONTRA LA CRIMINALIDAD (2021). *Informe de análisis N.° 04. Ciberdelincuencia en el Perú: pautas para una investigación fiscal especializada.* Recuperado de: https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERÚ%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIÓN%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf

Palmieri, M. y Shortland, N. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. *Computers in Human Behavior, 120*, 1-7. https://doi.org/10.1016/j.chb.2021.106745

Payne (2020). Defining Cybercrime. En Holt, T. & Bossler, A. (Eds.), *Handbook of International Cybercrime and Cyberdeviance* (pp. 3-25). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3_1

Pichihua, S. (25 de junio de 2023). *¡Cuidado con los fraudes informáticos! Estas son las modalidades más denunciadas en Perú*. https://andina.pe/agencia/noticia-cuidado-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-peru-928425.aspx

Puchkov, D. (2021). International Cyber Crime: Main Trends. *Revista San Gregorio*, (44), 9-13. https://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/1580/2-DENIS

Rodríguez, A. y Pérez, A. (2017). Métodos científicos de indagación y de construcción del conocimiento. *Revista Escuela de Administración de Negocios,* (82), 175-195. https://doi.org/10.21158/01208160.n82.2017.1647

Rojas, H. (2023). *Condena no pronunciada y el principio constitucional de igualdad ante la ley, Lima Noroeste 2021.* [Tesis de Maestría, Universidad César Vallejo]. Repositorio de la Universidad César Vallejo. https://hdl.handle.net/20.500.12692/114875

Rivera, M. (2020). *La tentativa en el delito de hurto mediante medios informáticos.* [Tesis de Maestría, Universidad Externado de Colombia]. Biblioteca digital Universidad Externado de Colombia. https://bdigital.uexternado.edu.co/handle/001/2935

Sánchez-Bayón, A. (2014). Fundamentos de derecho comparado y global: ¿cabe un orden común en la globalización? *Boletín Mexicano de Derecho Comparado*, (141), 1021-1051. https://eprints.ucm.es/id/eprint/44946/1/Fundamentos%20de%20Derecho.pdf

Serie de Tratados Europeos – N.° 185. Convenio sobre la Ciberdelincuencia (23 de noviembre de 2001). https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Siems, M. (2022). *Comparative Law* (3ª ed.). Cambridge University Press. https://doi.org/10.1017/9781108892766

Siregar, G. y Sinaga, S. (2021). The law globalization in cybercrime prevention. *International Journal of Law Reconstruction, 5*(2), 211-227. http://dx.doi.org/10.26532/ijlr.v5i2.17514

Somma, A. (2015). *Introducción al Derecho comparado*. Universidad Carlos II de Madrid. https://www.corteidh.or.cr/tablas/r34961.pdf

Villavicencio, F. (2019). *Derecho penal básico*. Fondo Editorial de la Pontificia Universidad Católica del Perú. https://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/170674/03%20Derecho%20penal%20básico%20con%20sello.pdf?sequence=1&isAllowed=y

Valarezo, E., Valarezo, R. y Durán, A. (2019). Algunas consideraciones sobre la tipicidad en la teoría del delito. *Revista Universidad y Sociedad*, *11*(1), 331-338. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000100331

Villanueva, V. (2023). Empirical Methods in Comparative Law: Data Talks. Comparative Law Review, 12(2), 55-84. https://www.researchgate.net/publication/370126935_Empirical_Methods_in_Comparative_Law_Data_Talks

Vinelli, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Ius Et Praxis,* (053), 95-110. https://doi.org/10.26439/iusetpraxis2021.n053.4995

ANEXO 1: MATRIZ DE CATEGORIZACIÓN

CATEGORÍA DE ESTUDIO	DEFINICIÓN CONCEPTUAL	CATEGORÍAS	SUBCATEGORÍAS	CÓDIGO
Delitos informáticos	"Son actividad delictivas que crean perturbaciones en la red; por ejemplo, robando datos privados de gran importancia, o pirateando información bancaria y transifiriendo dinero ajeno" (Goni, Ali, Showrov, Alam y Shameem, 2022, p. 29)	Delitos informáticos	Globalización Normativa Penal	Nominal

Unidad Fiscal Especializada en Ciberdelincuencia	Es un piloto de Fiscalía Especializada en ciberdelincuencia que fue implementada a finales de 2020 y cuenta con competencia a nivel nacional (OFAEC, 2021).	Unidad Fiscal Especializa en Ciberdelincuencia	Derecho Comparado Ministerio Público

Fuente: Elaboración propia (2023).

ANEXO 2: CONSENTIMIENTO INFORMADO

Título de la investigación: Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en Perú.

Investigador: Chavarría Velásquez Gustavo Rafael

Propósito del estudio: Le invitamos a participar en la investigación titulada "Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú", cuyo objetivo es: determinar la implicancia existente entre los delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú. Esta investigación es desarrollada por un estudiante de posgrado del programa académico de maestría en Dercho Penal y Procesal Penal, de la Universidad César Vallejo del campus Chimbote, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la institución.

Impacto del problema de investigación: Debido al fenómeno de la globalización y la pandemia de la COVID-19, grandes y modernos cambios tecnológicos han sido generados e implementados. Si bien es algo positivo, también han fomentado el riesgo de que se vulneren los bienes jurídicos expuestos en el mundo digital; por lo que, la ciberdelincuencia está muy latente. En diciembre de 2020, se creó la Unidad Fiscal Especializada en Ciberdelincuencia como respuesta a esta situación. Por lo tanto, existe una relación entre esta institución piloto y los delitos informáticos.

Procedimiento: Si usted decide participar en la investigación, se llevará a cabo lo siguiente:

1. Se realizará una entrevista donde se recogerán datos personales y algunas preguntas sobre la investigación titulada: "Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú".
2. La entrevista contará con un total de 12 preguntas y se realizarán en un lugar de preferencia de los entrevistados para mejor comodidad al

responder, concluyendo con el regreso de la guía de entrevista al investigador.

Participación voluntaria: Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si desea participar o no, y su decisión será respetada. Posterior a la aceptación, si no desea continuar, puede hacerlo sin ningún problema.

Riesgo: Indicar al participante la existencia de que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios: No recibirá ningún beneficio económico, ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona; sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad: Los datos recolectados deben ser anónimos y no tener ninguna forma de identificar al participante. Garantizamos que la información que usted nos brinde es totalmente Confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas: Si tiene preguntas sobre la investigación puede contactar con el Investigador Chavarría Velásquez Gustavo Rafael en su email: GustCV3@hotmail.com; y con la asesora Alva Diaz Lyda Palmira en su email: lyda923@hotmail.com.

Consentimiento: Después de haber leído los propósitos de la investigación, autorizo participar en la investigación antes mencionada.

Nombre y apellidos: Yoselina Benites Vidal.
Fecha y hora: 15/06/2023, 09:00 a.m.

Para garantizar la veracidad del origen de la información: en el caso que el consentimiento sea presencial, el encuestado y el investigador debe proporcionar: Nombre y firma. En el caso que sea cuestionario virtual, se debe solicitar el correo desde el cual se envía las respuestas a través de un formulario Google.

CONSENTIMIENTO INFORMADO

Título de la investigación: Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en Perú.

Investigador: Chavarría Velásquez Gustavo Rafael

Propósito del estudio: Le invitamos a participar en la investigación titulada "Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú", cuyo objetivo es: determinar la implicancia existente entre los delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú. Esta investigación es desarrollada por un estudiante de posgrado del programa académico de maestría en Dercho Penal y Procesal Penal, de la Universidad César Vallejo del campus Chimbote, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la institución.

Impacto del problema de investigación: Debido al fenómeno de la globalización y la pandemia de la COVID-19, grandes y modernos cambios tecnológicos han sido generados e implementados. Si bien es algo positivo, también han fomentado el riesgo de que se vulneren los bienes jurídicos expuestos en el mundo digital; por lo que, la ciberdelincuencia está muy latente. En diciembre de 2020, se creó la Unidad Fiscal Especializada en Ciberdelincuencia como respuesta a esta situación. Por lo tanto, existe una relación entre esta institución piloto y los delitos informáticos.

Procedimiento: Si usted decide participar en la investigación, se llevará a cabo lo siguiente:

1. Se realizará una entrevista donde se recogerán datos personales y algunas preguntas sobre la investigación titulada: "Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú".
2. La entrevista contará con un total de 12 preguntas y se realizarán en un lugar de preferencia de los entrevistados para mejor comodidad al

responder, concluyendo con el regreso de la guía de entrevista al investigador.

Participación voluntaria: Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si desea participar o no, y su decisión será respetada. Posterior a la aceptación, si no desea continuar, puede hacerlo sin ningún problema.

Riesgo: Indicar al participante la existencia de que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios: No recibirá ningún beneficio económico, ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona; sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad: Los datos recolectados deben ser anónimos y no tener ninguna forma de identificar al participante. Garantizamos que la información que usted nos brinde es totalmente Confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas: Si tiene preguntas sobre la investigación puede contactar con el Investigador Chavarría Velásquez Gustavo Rafael en su email: GustCV3@hotmail.com; y con la asesora Alva Diaz Lyda Palmira en su email: lyda923@hotmail.com.

Consentimiento: Después de haber leído los propósitos de la investigación, autorizo participar en la investigación antes mencionada.

Nombre y apellidos: Pamela Cerna Ruiz.
Fecha y hora: 15/06/2023, 10:00 a.m.

Para garantizar la veracidad del origen de la información: en el caso que el consentimiento sea presencial, el encuestado y el investigador debe proporcionar: Nombre y firma. En el caso que sea cuestionario virtual, se debe solicitar el correo desde el cual se envía las respuestas a través de un formulario Google.

CONSENTIMIENTO INFORMADO

Título de la investigación: Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en Perú.

Investigador: Chavarría Velásquez Gustavo Rafael

Propósito del estudio: Le invitamos a participar en la investigación titulada "Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú", cuyo objetivo es: determinar la implicancia existente entre los delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú. Esta investigación es desarrollada por un estudiante de posgrado del programa académico de maestría en Dercho Penal y Procesal Penal, de la Universidad César Vallejo del campus Chimbote, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la institución.

Impacto del problema de investigación: Debido al fenómeno de la globalización y la pandemia de la COVID-19, grandes y modernos cambios tecnológicos han sido generados e implementados. Si bien es algo positivo, también han fomentado el riesgo de que se vulneren los bienes jurídicos expuestos en el mundo digital; por lo que, la ciberdelincuencia está muy latente. En diciembre de 2020, se creó la Unidad Fiscal Especializada en Ciberdelincuencia como respuesta a esta situación. Por lo tanto, existe una relación entre esta institución piloto y los delitos informáticos.

Procedimiento: Si usted decide participar en la investigación, se llevará a cabo lo siguiente:

1. Se realizará una entrevista donde se recogerán datos personales y algunas preguntas sobre la investigación titulada: "Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú".
2. La entrevista contará con un total de 12 preguntas y se realizarán en un lugar de preferencia de los entrevistados para mejor comodidad al

responder, concluyendo con el regreso de la guía de entrevista al investigador.

Participación voluntaria: Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si desea participar o no, y su decisión será respetada. Posterior a la aceptación, si no desea continuar, puede hacerlo sin ningún problema.

Riesgo: Indicar al participante la existencia de que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios: No recibirá ningún beneficio económico, ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona; sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad: Los datos recolectados deben ser anónimos y no tener ninguna forma de identificar al participante. Garantizamos que la información que usted nos brinde es totalmente Confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas: Si tiene preguntas sobre la investigación puede contactar con el Investigador Chavarría Velásquez Gustavo Rafael en su email: GustCV3@hotmail.com; y con la asesora Alva Diaz Lyda Palmira en su email: lyda923@hotmail.com.

Consentimiento: Después de haber leído los propósitos de la investigación, autorizo participar en la investigación antes mencionada.

Nombre y apellidos: Sonia Carranza Tejón

Fecha y hora: 16/6/23 9:30 am.

CONSENTIMIENTO INFORMADO

Título de la investigación: Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en Perú.

Investigador: Chavarría Velásquez Gustavo Rafael

Propósito del estudio: Le invitamos a participar en la investigación titulada "Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú", cuyo objetivo es: determinar la implicancia existente entre los delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú. Esta investigación es desarrollada por un estudiante de posgrado del programa académico de maestría en Dercho Penal y Procesal Penal, de la Universidad César Vallejo del campus Chimbote, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la institución.

Impacto del problema de investigación: Debido al fenómeno de la globalización y la pandemia de la COVID-19, grandes y modernos cambios tecnológicos han sido generados e implementados. Si bien es algo positivo, también han fomentado el riesgo de que se vulneren los bienes jurídicos expuestos en el mundo digital; por lo que, la ciberdelincuencia está muy latente. En diciembre de 2020, se creó la Unidad Fiscal Especializada en Ciberdelincuencia como respuesta a esta situación. Por lo tanto, existe una relación entre esta institución piloto y los delitos informáticos.

Procedimiento: Si usted decide participar en la investigación, se llevará a cabo lo siguiente:

1. Se realizará una entrevista donde se recogerán datos personales y algunas preguntas sobre la investigación titulada: "Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú".
2. La entrevista contará con un total de 12 preguntas y se realizarán en un lugar de preferencia de los entrevistados para mejor comodidad al

responder, concluyendo con el regreso de la guía de entrevista al investigador.

Participación voluntaria: Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si desea participar o no, y su decisión será respetada. Posterior a la aceptación, si no desea continuar, puede hacerlo sin ningún problema.

Riesgo: Indicar al participante la existencia de que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios: No recibirá ningún beneficio económico, ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona; sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad: Los datos recolectados deben ser anónimos y no tener ninguna forma de identificar al participante. Garantizamos que la información que usted nos brinde es totalmente Confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas: Si tiene preguntas sobre la investigación puede contactar con el Investigador Chavarría Velásquez Gustavo Rafael en su email: GustCV3@hotmail.com; y con la asesora Alva Diaz Lyda Palmira en su email: lyda923@hotmail.com.

Consentimiento: Después de haber leído los propósitos de la investigación, autorizo participar en la investigación antes mencionada.

Nombre y apellidos: Eduardo Cano Lavado.
Fecha y hora: 19/06/2023, 09:00 a.m.

Para garantizar la veracidad del origen de la información: en el caso que el consentimiento sea presencial, el encuestado y el investigador debe proporcionar: Nombre y firma. En el caso que sea cuestionario virtual, se debe solicitar el correo desde el cual se envía las respuestas a través de un formulario Google.

CONSENTIMIENTO INFORMADO

Título de la investigación: Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en Perú.

Investigador: Chavarría Velásquez Gustavo Rafael

Propósito del estudio: Le invitamos a participar en la investigación titulada "Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú", cuyo objetivo es: determinar la implicancia existente entre los delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú. Esta investigación es desarrollada por un estudiante de posgrado del programa académico de maestría en Dercho Penal y Procesal Penal, de la Universidad César Vallejo del campus Chimbote, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la institución.

Impacto del problema de investigación: Debido al fenómeno de la globalización y la pandemia de la COVID-19, grandes y modernos cambios tecnológicos han sido generados e implementados. Si bien es algo positivo, también han fomentado el riesgo de que se vulneren los bienes jurídicos expuestos en el mundo digital; por lo que, la ciberdelincuencia está muy latente. En diciembre de 2020, se creó la Unidad Fiscal Especializada en Ciberdelincuencia como respuesta a esta situación. Por lo tanto, existe una relación entre esta institución piloto y los delitos informáticos.

Procedimiento: Si usted decide participar en la investigación, se llevará a cabo lo siguiente:

1. Se realizará una entrevista donde se recogerán datos personales y algunas preguntas sobre la investigación titulada: "Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú".
2. La entrevista contará con un total de 12 preguntas y se realizarán en un lugar de preferencia de los entrevistados para mejor comodidad al

responder, concluyendo con el regreso de la guía de entrevista al investigador.

Participación voluntaria: Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si desea participar o no, y su decisión será respetada. Posterior a la aceptación, si no desea continuar, puede hacerlo sin ningún problema.

Riesgo: Indicar al participante la existencia de que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios: No recibirá ningún beneficio económico, ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona; sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad: Los datos recolectados deben ser anónimos y no tener ninguna forma de identificar al participante. Garantizamos que la información que usted nos brinde es totalmente Confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas: Si tiene preguntas sobre la investigación puede contactar con el Investigador Chavarría Velásquez Gustavo Rafael en su email: GustCV3@hotmail.com; y con la asesora Alva Diaz Lyda Palmira en su email: lyda923@hotmail.com.

Consentimiento: Después de haber leído los propósitos de la investigación, autorizo participar en la investigación antes mencionada.

Nombre y apellidos: Johnny Quispe Cuba.
Fecha y hora: 19/06/2023, 10:00 a.m.

Para garantizar la veracidad del origen de la información: en el caso que el consentimiento sea presencial, el encuestado y el investigador debe proporcionar: Nombre y firma. En el caso que sea cuestionario virtual, se debe solicitar el correo desde el cual se envía las respuestas a través de un formulario Google.

ANEXO 3: INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUÍA DE ENTREVISTA

DIRIGIDA A ABOGADOS EN EJERCICIO EN EL ÁREA PENAL EN EL DISTRITO JUDICIAL DEL SANTA

La presente entrevista tiene el fin académico de recabar información especializada para la tesis de posgrado titulada: Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú.

I. INSTRUCCIÓN

La guía de entrevista consta de 12 preguntas. Lea con muchas atención cada una de ellas y, responda de manera clara.

II. PREGUNTAS

OBJETIVO GENERAL

Determinar la implicancia existente entre los delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público del Perú.

1. **¿Considera que la ciberdelincuencia es un problema jurídico actual? ¿Por qué?**

_____

_____

_____

_____

_____

2. **¿Considera que la normativa nacional – Ley de ciberdefensa y la Ley de delitos informáticos – y la internacional – Convenio de Budapest – están actualizadas y son adecuadas para regular la gama de los delitos informáticos? ¿Por qué?**

3. **¿Considera que las Fiscalías existentes del Ministerio Público están preparadas y son suficientes para identificar, investigar y sancionar los delitos informáticos? ¿Por qué?**

4. **¿Qué opina de la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú?**

5. **¿Considera que existe relación entre los delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia? ¿Por qué?**

_____
_____
_____
_____
_____

OBJETIVO ESPECÍFICO 1

Identificar si existen doctrinas y teorías modernas suficientes sobre los delitos informáticos.

6. **¿Considera que la doctrina actual es vasta y suficiente para estudiar los delitos informáticos? ¿Por qué?**

_____
_____
_____
_____
_____

7. **¿Considera que la teoría clásica del delito debe ser tomada en cuenta para explicar la naturaleza de los delitos informáticos? ¿Por qué?**

_____
_____
_____
_____
_____

OBJETIVO ESPECÍFICO 2

Comparar la Unidad Fiscal Especializada en Ciberdelincuencia con sus similares en otros países.

8. **¿Considera que a nivel internacional, existen países que están mejor preparados en temas cibernéticos en cuanto a normativa e instituciones jurídicas? ¿Por qué?**

_____
_____
_____
_____
_____

9. **¿Considera que la Unidad Fiscal Especializada en Ciberdelincuencia – de nuestro país – debe tomar en cuenta lineamientos y medidas de instituciones especializadas en ciberdelincuencias extranjeras?**

_____
_____
_____
_____
_____

OBJETIVO ESPECÍFICO 3

Analizar el avance en la identificación, investigación y sanción de los delitos informáticos tras la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia en el Perú.

10. **En base a su experiencia, ¿qué opina de la identificación, investigación y sanción de los delitos informáticos por parte del Ministerio Público?**

_____

_____

_____

_____

_____

11. **¿Ha llevado algún caso de delito informático reciente donde haya intervenido la Unidad Fiscal Especializada en Ciberdelincuencia? De ser afirmativa su respuesta, ¿qué opina de su participación?**

_____

_____

_____

_____

_____

12. **¿Considera que se debe implementar una Fiscalía Especializada en Ciberdelincuencia en cada distrito fiscal? ¿Por qué?**

_____

_____

_____

_____

_____