UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

La obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro 2021.

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
ABOGADO

AUTORES:

Hernández Ayala, Nancy (ORCID: 0000-0002-3850-3741)

Patricio Rojas, Alejandro Efraín (ORCID: 0000-0002-2399-6299)

ASESOR:

Dr. Vildoso Cabrera, Erick Daniel (ORCID: 0000-0002-0803-9415)

LÍNEA DE INVESTIGACIÓN:

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

CALLAO – PERÚ

2022

Dedicatoria

A Dios, por habernos guiado al camino de la sabiduría y orientarnos nuestros pasos al éxito, a la vez permitiéndonos a lograr nuestras metas y objetivos. A nuestros padres, quienes han sido, son y serán siempre nuestras guías en la vida, por la comprensión, la confianza y apoyo incondicional que nos brindaron en todo momento; y, a nuestra alma máter.

Agradecimiento

Agradecer en primer lugar a Dios por brindarnos salud y vida para poder concluir nuestra carrera profesional sacando provecho de las enseñanzas académicas de nuestra alma máter. Así mismo, agradecer a nuestros padres que con sus apoyos incondicionales nos enseñaron a luchar por lo que se desea alcanzar.

Índice de contenidos

Carátula i
Dedicatoria ii
Agradecimiento iii
Índice de contenidos iv
Índice de tablas v
Resumen vi
Abstract vii
I. INTRODUCCIÓN 1
II. MARCO TEÓRICO 6
III. METODOLOGÍA 17
3.1. Tipo y diseño 17
3.2. Categorías, Subcategorías y matriz de categorización 18
3.3. Escenario de estudio 18
3.4. Participantes 19
3.5. Técnicas e instrumentos de recolección de datos 20
3.6. Procedimientos 20
3.7. Rigor científico 21
3.8. Método de análisis de datos 22
3.9. Aspectos éticos 22
IV. RESULTADOS Y DISCUSIÓN 22
4.1. Resultados de investigación 22
4.2. Discusión 35
V. CONCLUSIONES 39
VI. RECOMENDACIONES 41
REFERENCIAS 42
ANEXOS 43

Índice de tablas

Tabla 1: Matriz de categorización..... 18
Tabla 2: Caracterización de los sujetos..... 19
Tabla 3: Respuestas de la primera pregunta del objetivo general..... 23
Tabla 4: Respuestas de la segunda pregunta del objetivo general..... 24
Tabla 5: Respuestas de la tercera pregunta del objetivo general..... 25
Tabla 6: Respuestas de la cuarta pregunta del objetivo general..... 26
Tabla 7: Respuestas de la quinta pregunta del objetivo general..... 27
Tabla 8: Respuestas de la sexta pregunta del objetivo general. 28
Tabla 9: Respuestas de la primera pregunta del objetivo específico 1. 29
Tabla 10: Respuestas de la segunda pregunta del objetivo específico 1. 30
Tabla 11: Respuestas de la tercera pregunta del objetivo específico 1. 31
Tabla 12: Respuestas de la primera pregunta del objetivo específico 2 32
Tabla 13: Respuestas de la segunda pregunta del objetivo específico 2. 33
Tabla 14: Respuestas de la tercera pregunta del objetivo específico 2. 34

Resumen

La presente investigación titulada “La obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro 2021” tuvo como objetivo analizar la afectación de la actuación fiscal en la obtención de pruebas digitales en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

La metodología de la investigación fue de tipo aplicada, de enfoque cualitativo y diseño no experimental. La población estuvo conformada por los fiscales y asistentes de la Fiscalía Especializada en Ciberdelincuencia de Lima Centro. La técnica utilizada fue la entrevista y el instrumento fue guía de entrevista.

Se concluyó que, debido a la falta de capacitación, herramientas óptimas y la legislación, la actuación fiscal es deficiente en la obtención y perennización de evidencia digital, información importante, para el planteamiento de la teoría del caso en las investigaciones seguidas contra los delitos de fraude informático y suplantación de identidad, lo que genera, una insuficiente protección de los bienes jurídicos tutelados.

Por otro lado, luego de una serie de encuestas por parte del personal fiscal especializado de las Fiscalías Especializadas en ciberdelincuencia de Lima Centro, se ha concluido que el acopio de evidencia digital se estaría realizando sin vulnerar ningún derecho fundamental.

Finalmente, se recomienda la implementación de más Fiscalías Especializadas en Ciberdelincuencia en todo el país, implementación de herramientas que ayuden con el acopio de la evidencia digital, una mayor especialización y capacitación a las Instituciones que se ven involucradas en la lucha contra los delitos cibernéticos, políticas de prevención por parte del Estado, así como la repotenciación de la DIVINDAT y la creación de un protocolo de perennización de evidencia digital.

Palabras clave: Actuación fiscal, pruebas digitales, suplantación de identidad, fraude informático.

Abstract

The present investigation entitled "The obtaining of evidence in cybercrimes in the Specialized Prosecutor's Offices in Cybercrime of Lima Centro 2021" aimed to analyze the impact of fiscal action in obtaining digital evidence in the Corporate Prosecutor's Office Specialized in Cybercrime of Lima – Centro.

The research methodology was of an applied type, of qualitative approach and non-experimental design. The population was made up of prosecutors and assistants of the Specialized Prosecutor's Office in Cybercrime of Lima Centro. The technique used was the interview and the instrument was an interview guide.

It was concluded that, due to the lack of training, optimal tools and legislation, fiscal action is deficient in obtaining and perennizing digital evidence, important information, for the approach of the theory of the case in the investigations followed against the crimes of computer fraud and identity theft, which generates, an insufficient protection of the legal assets protected.

On the other hand, after a series of surveys by the specialized fiscal personnel of the Specialized Prosecutor's Offices in cybercrime of Lima Centro, it has been concluded that the collection of digital evidence would be carried out without violating any fundamental right.

Finally, it is recommended the implementation of more Specialized Prosecutor's Offices in Cybercrime throughout the country, implementation of tools that help with the collection of digital evidence, greater specialization and training for institutions that are involved in the fight against cybercrimes, prevention policies by the State, as well as the repowering of divindat and the creation of a protocol for the perennialization of digital evidence.

Keywords: Tax action, digital evidence, identity theft, computer fraud.

I. INTRODUCCIÓN

En el mundo actual, la tecnología informática es la herramienta más utilizada por la humanidad, en lo cual interactúan por medio de plataformas conectados por internet. Sin embrago, esta herramienta viene funcionando de manera incorrecta debido a la expansión del liderazgo criminal a través de la informática, teniendo efecto en los derechos patrimoniales. Por otro lado, últimamente se han contabilizado muchos casos ilícitos siendo protagonista la ciberdelincuencia, teniendo actos ilícitos en las transferencias electrónicas y en el e-commerce.

Al nivel internacional, la ciberdelincuencia ha ido en aumento arruinando al sector empresarial y la vida de las personas, realizando comportamientos ilícitos, es por ello que las organizaciones luchan en detener este acto y contribuir con la seguridad. Fernández (2018) mencionó que la mayoría de ciberdelincuentes se encuentran ubicados en Europa, siendo EEUU el país más afectado por los hackers rusos que son personas con habilidades que buscan nuevos caminos para levantar contra los nuevos sistemas de seguridad con el uso de la tecnología.

En el contexto nacional, en tiempo de la pandemia Covid-19, se ha generado un escenario propicio de incremento de los delitos cibernéticos y el actuar desmedido de los agentes delictivos, que ante este escenario han incrementado sus modalidades de accionar y su mapa delictivo ha rebasado cualquier frontera nacional. Según La Asamblea General (2019), los avances tecnológicos abrieron puertas para los ciberdelincuentes y provocaron una expansión de la tasa y variedad de delitos. A pesar de que no existen figuras de autoridad que reflejen los resultados de esta irregularidad, además se evaluó que el ciberdelito genera gastos de aproximadamente 575.000 millones de dólares al año.

En base a este problema social, nuestro país en mérito al artículo 159° de la Constitución Política del Estado, el Ministerio Público como titular del ejercicio de la acción penal pública, la defensa de la legalidad y de los intereses públicos tutelados por el Derecho, ha instituido criterios competenciales para la distribución de las denuncias. Así, el artículo 80-B de la Ley Orgánica del Ministerio Público – D.L. N.° 052, establece la designación de fiscales especializados, para la investigación y juzgamiento de todos los hechos delictivos vinculados entre sí o que presenten características similares y que requieren de una intervención especializada del

Ministerio Público. Asimismo, en nuestro país, la CONACOP (2020) mencionó que los delitos se están expandiendo rápidamente paso a paso. De octubre de 2013 a julio de 2020, las fiscalías registraron 21.687 quejas, de las cuales el 40% provino de 2019. No obstante, el 58% de ellas fueron documentadas y solo se dictaron 108 sentencias.

En el desarrollo del precitado dispositivo y a través de las Resoluciones de Fiscalía de la Nación números 1025-2020-MP-FN y 1194-2020-MP-FN, del 18 de septiembre y 30 de octubre de 2020 respectivamente, se dispuso en base a la problemática social en la lucha contra los ciberdelitos y su alta incidencia, conformar una Comisión encargada de evaluar técnicamente la creación de un Piloto de la Fiscalía Especializada o Unidad Especializada en Ciberdelito, la cual estuvo conformada por diferentes fiscales y autoridades de la fundación mediante la Resolución del Ministerio Público No. 1503-2020-MP-FN, de 30 de diciembre de 2020, se creó la Unidad Fiscal Especializada en Ciberdelincuencia, considerando entre sus fundamentos, la modalidad delictiva utilizada (ciberdelitos).

En atención a ello, mediante Resolución de la Fiscalía de la Nación N.º 843-2021-MP-FN, del 08 de junio del 2021 y modificatoria (denominación) Resolución N.º 848-2021-MP-FN, del 11 de junio del 2021, con el propósito de ofrecer a la sociedad un servicio eficiente y eficaz que permita acceder a una pronta administración de justicia a favor de la ciudadanía y ante la alta incidencia delictiva respecto a la vulneración y/o utilización ilegal de las tecnologías de la información o de la comunicación, se creó la Fiscalía Especializada en Ciberdelincuencia de Lima Centro, cuya competencia se rige por la Ley N.º 30096 – Ley de Delitos Informáticos, del 22 de octubre de 2013 y modificatoria establecida en la Ley N.º 30171; así como, el artículo 196°-A, numeral 5, del Código Penal, debiendo dichas modalidades ser conocidas por este Subsistema Especializado en Ciberdelincuencia de Lima Centro (Competencia territorial y especial).

Asimismo, en el devenir de la investigación fiscal, en base a la facultad conferida por nuestra carta magna en el artículo 159, numeral 4, le ha asignado la atribución de “Conducir desde su inicio la investigación del delito (...)”, actuando con objetividad, a fin de aportar la carga de la prueba, indagando los hechos constitutivos de delito y demostrar la obligación u honestidad del denunciado.

No obstante, cuando hablamos de una investigación fiscal en materia de ciberdelitos, se ve en la obligación de utilizar las herramientas de cooperación internacional de manera directa con los proveedores de servicios, medio por el que debe recabar información que muchas veces a espalda de un posible “investigado” previamente identificado, pudiendo vulnerar el secreto a las comunicaciones, derecho constitucional indeleble y facultado a toda persona.

Lamentablemente, nuestro país en su iniciar a combatir la ciberdelincuencia que aqueja, estaría realizando una suerte de práctica que podría resultar perjudicial a futuro.

Por lo expuesto se planteó el problema general de la investigación: ¿De que manera la actuación fiscal en la obtención de pruebas digitales afecta la investigación de los delitos cibernéticos en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima - Centro?

Asimismo, se presentó los siguientes problemas específicos:

¿De qué manera la obtención de pruebas digitales influye en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro?

¿De qué manera la perennización de las pruebas digitales incide en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro?

Como justificación del presente estudio, Hernández y Sampieri (2018) definió que la justificación explica las razones y la pertinencia de la investigación. Por ende, la justificación del estudio fue conveniente porque permitió analizar la influencia de la actuación fiscal en la obtención de pruebas digitales, ya que gran parte de los delitos cibernéticos terminan archivándose. Además, mediante la recopilación de datos se obtendrá resultados sobre la el impacto de la actuación fiscal.

Por lo que, la justificación teórica de esta investigación se basó en buscar bases doctrinarias, jurisprudenciales y conocimiento existente, que luego de un análisis mediante herramientas adecuadas, contribuyen a identificar los factores de mejora

en la obtención de pruebas en la actuación fiscal de las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro.

En ese sentido, la justificación metodológica se realiza mediante un enfoque cualitativo, donde desarrollaremos un análisis exhaustivo del instrumento guía de entrevista, realizada a los expertos en la materia involucrados en nuestro problema de investigación. Nuestra investigación conllevará a una realización metodológica óptima académicamente y científica a la altura de una investigación para una tesis de grado, la misma que podrá ser aplicada en otras investigaciones.

Asimismo, la justificación práctica de la presente investigación parte de la preocupación por el incremento de los delitos cibernéticos, debido a que en la actualidad la población utiliza en su mayoría los medios digitales e informáticos para el devenir de sus quehaceres u obligaciones, lo que ha conllevado un escenario propicio para el incremento de este tipo de delitos; y, su volatilidad de datos ha generado una carencia en la obtención de pruebas conllevando al archivamiento de las investigaciones fiscales por parte de las fiscalías comunes del Ministerio Público, institución que creó las Fiscalías Especializadas en Ciberdelincuencia, a efectos de suplir dicha precariedad y falta de especialización en la investigación de esta clase de ilícitos penales. Por ello, nuestra investigación será un aporte práctico para el Estado en general (operadores de justicia, Fiscalía, abogados, policías y público en general) ya que, el resultado de nuestra investigación está basada en la actuación fiscal referente a la obtención de pruebas digitales en las investigaciones fiscales, por ende, permitirá elaborar estrategias concretas para mejorar la lucha contra cibercriminalidad.

Por consiguiente, se planteó el siguiente objetivo general:

Analizar de qué manera la actuación fiscal en la obtención de pruebas digitales afecta la investigación de los delitos cibernéticos en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima - Centro

Seguidamente, se propuso los objetivos específicos:

Determinar como la obtención de pruebas digitales influye en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro

Establecer como la perennización de las pruebas digitales incide en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

Finalmente, se tuvo el siguiente supuesto general:

La actuación fiscal en la obtención de pruebas digitales si afecta la investigación de los delitos cibernéticos en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima - Centro

Asimismo, se obtuvo los supuestos específicos:

La obtención de pruebas digitales influye negativamente en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

La perennización de las pruebas digitales incide negativamente en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

II. MARCO TEÓRICO

Conforme a la investigación, se abordó los antecedentes internacionales y nacionales.

Entre los antecedentes internacionales tenemos a Alarcón D. y Barrera J. (2017), en su tesis para la obtención del grado académico de maestro en informática educativa, “Uso de internet y delitos informáticos en los estudiantes de la Universidad Pedagógica y Tecnológica de Colombia”, presentó el objetivo de determinar a la relación que existe en el uso de internet y delitos informáticos. Por otro lado, la metodología fue de tipo básico, nivel correlacional y diseño no experimental. Así mismo, se usó la técnica de la encuesta e instrumento guía de entrevista sacando el alfa de Cronbach a una prueba piloto para la fiabilidad. Los resultados fueron que el uso del internet respecto a los delitos informáticos se encuentra en un nivel superior de 63%. Por último, se concluyó que los delitos informáticos quedan expuestos por las vulnerabilidades de los sistemas de intercomunicación y que la ciberdelincuencia seguirá aumentando por estudiantes de mano negra que poseen habilidades.

Abdulai (2016), en su tesis para la obtención del grado académico de Maestro en Artes en el Departamento de Sociología, aprobada por la Universidad de Saskatchewan titulada "Determinantes del miedo a la victimización del crimen de cibernética, un estudio del fraude a la tarjeta de crédito entre estudiantes de la Universidad de Saskatchewan", cuyo objetivo principal era investigar el temor al trato por los delitos cibernéticos (distorsión de Visas / cheques). Los hallazgos mostraron que la experiencia de victimización y las prácticas de uso de Internet están enfáticamente conectadas con el temor y el riesgo de los estudiantes de convertirse en víctimas de fraude con tarjetas de crédito / cheques. La técnica utilizada fue la encuesta y la población fueron los estudiantes del periodo de dos meses. Se concluyó que la experiencia de victimización y las prácticas de uso de Internet están enfáticamente conectadas con el temor y el riesgo de los estudiantes de convertirse en víctimas en la estafa de tarjetas de crédito / debito.

Rincón (2015), quien realizó la tesis para la obtención del grado académico de doctor en derecho, titulada “El delito en la cibersociedad y la justicia penal internacional”, tuvo como objetivo de investigación proponer la base de una elaboración teórica desde la dogmática penal internacional que permita discutir sobre la necesidad de incluir la investigación y juzgamiento de los delitos informáticos, electrónicos y de las telecomunicaciones en la competencia del Estatuto de Roma. Trabajo investigado desde el método deductivo partiendo de preceptos generales, hasta llegar a la particulariedad. Señaló el problema del fraude internacional ha sido planteado por diversos sectores de la sociedad internacional, desde organizaciones internacionales hasta empresas transnacionales, como por ejemplo la empresa McAfee, sustentado en información del FBI y la inteligencia europea en diciembre de 2006 publicitado en apartes por la Asociación de Internautas, se señala que una de las causas del auge del ciberdelito en Europa del Este, es el grave nivel de desempleo y los bajos salarios, un gran número de estos ciberdelincuentes consideran que es una oportunidad de negocio. En conclusión se señaló que el Organismo Internacional más adecuado debe tener competencia para sancionar los delitos informáticos es la Corte Penal Internacional, y la solución a largo plazo, como etapa inicial en el asentimiento global de las violaciones de delitos informáticos sería la adecuación del Estatuto de Roma, donde los delitos cibernéticos o fechorías generales no son conocidos por la Corte Penal Internacional de manera auxiliar o restante, en todo caso, en la actualidad, ya que son de violaciones universales, es este caso de Derecho Penal Internacional el que tiene los requisitos y calidades para adelantar su persecución, siendo este órgano quien realice su investigación, juzgamiento y sanción.

Piccirilli (2015), realizó la investigación titulada “Protocolos a aplicar en la Forensia Informática en el marco de las nuevas tecnologías”, se sustentó en la Facultad de Informática de la Universidad Nacional de La Plata para optar el grado de doctor en Ciencias Informáticas, cuyo objetivo fue desarrollar una propuesta metodológica para definir protocolos de base a utilizar en el uso de la forensia aplicada al tratamiento de la evidencia digital, en el marco de las nuevas tecnologías informáticas. En este sentido, se realizó un análisis de la prueba desde el secuestro hasta el análisis pericial correspondiente. El enfoque metodológico empleado en el

desarrollo del estudio fue analítico y señaló que es bastante alto el nivel de la ciberdelincuencia, y que la constante evolución del delito es la que provoca generar nuevas inquietudes. Se concluyó que la luz del nuevo Código Procesal Penal Argentino, tomando en cuenta el nuevo paradigma legal de las pericias en general y en particular las pericias de carácter informático, es necesario cubrir las falencias de los procedimientos vigentes, por lo que es necesario contar con un protocolo actual y formalizado para afrontar los desafíos técnicos relativos a las nuevas tecnologías informáticas.

Amaya, Avalos y Jule (2012), en la investigación sobre el "Derecho a la Intimidad en la estructura de la ley especial de intervención de telecomunicaciones" para optar el grado de Licenciado en Ciencias Jurídicas en la Universidad de El Salvador, mencionaron como objetivo determinar la relación que existe entre las Telecomunicaciones y el "Derecho a la Intimidad". Asimismo, concluyó que existen factores que limitan dichos derechos como son: la 34 seguridad del Estado, bienestar general, el desorden, el crimen y la protección a la Salud; asimismo, establece que la intervención entre ambas figuras jurídicas, está marcada por la posible vulneración al "Derecho a la Intimidad" cuando estas son realizadas en forma ilegítima; por otro lado señaló que la intercesión en las comunicaciones por radiodifusión restringe el aseguramiento del Derecho Fundamental a la Privacidad, el mismo que requiere la debida garantía del Estado para la concurrencia pacifica en la sociedad por ser este un derecho personalísimo y que además se encuentra protegido por instrumentos internacionales. Por otro lado, difundió que no en todos los países existe una ley especial que legisle sobre las telecomunicaciones y de ser el caso es en forma muy excepcional; respecto a la jurisprudencia como fuente del derecho indica que en dichos pronunciamientos se establece los criterios que se deben tener en cuenta al momento de analizar la intrusión en el campo de la intimidad de las personas, con la finalidad de no colisionar con otros derechos.

Asimismo, en los antecedentes nacionales, podemos vislumbrar a los siguientes autores:

Ávalos Rivera (2020) en su informe "La Ciberdelincuencia: pautas para una investigación fiscal especializada", presentó como objetivo analizar la actuación fiscal en la ciberdelincuencia. La metodología fue de nivel descriptiva, análisis

informativo de diseño no experimental. Se usó la técnica de la entrevista a una muestra de representantes de fiscalías con incidencia de delitos informáticos. Los resultados fueron que el 48% de las denuncias fueron en el Distrito Fiscal de Lima: Lima Norte (7%), Arequipa (6%), Lima Este (6%), La Libertad (5%) y Lambayeque (4%), Callao (3%) y Lima Sur (3%). El 83% de los delitos informáticos se concentró en ocho Distritos Fiscales. Se concluyó que la incidencia de denuncias de delitos sigue han aumentado en los años 2013 a 2020.

Condori y Rufino (2020) para optar el grado de maestro en Derecho Penal y Procesal Penal en la Universidad de Cesar Vallejo, “Implicancias Jurídicas del Fraude Informático y la Protección Penal del Delito Contra el Patrimonio”, tuvo como objetivo analizar la relación de Implicancias Jurídicas del Fraude Informático y la Protección Penal del Delito. La metodología fue cualitativa, de nivel descriptiva, no experimental, y el diseño de la presente tesis es socio crítico de la fenomenología. Asimismo, concluyó que el fraude informático en la protección penal de los delitos contra el patrimonio repercute de manera negativa frente a los derechos patrimoniales de los privados y del propio Estado debido a que en la mayoría de los casos de investigación a nivel fiscalía no se logra identificar al autor material del hecho ilícito fraudulento teniendo como consecuencia el archivo definitivo de la investigación quedando impune el delito siendo afectado la esfera patrimonial de la parte agraviada. Se recomendó al Ministerio Público al Poder Judicial, la Policía Nacional del Perú que sumen esfuerzos de forma conjunta con la solidaridad y cooperación interinstitucional a fin que con prontitud planifiquen y establezcan los lineamientos y protocolos a seguir ceñido a los avances vertiginosos de la vanguardia tecnológica para tener mayores alcances y posibilidades de enfrentar con mayor efectividad la ciberdelincuencia. Para que la nueva creación de las fiscalías especializadas en la lucha contra los delitos informático específicamente en la modalidad de fraude informático recientemente creadas que invierta más en contar con personal capacitada en informática y logística necesaria para combatir este tipo de delitos, así como que tenga alcance para todos los recursos indispensables para la prevención del delito y afrontar la ciberdelincuencia.

Gómez Vásquez (2020), realizó la investigación titulada “El tratamiento jurídico penal por parte del fiscal en los delitos informáticos contra el patrimonio, distrito

judicial de Lima Norte 2019”, para optar el grado académico de Título profesional de abogado. Tuvo como objetivo general determinar de qué manera se da el Tratamiento Jurídico Penal por parte del Fiscal en los Delitos Informáticos contra el Patrimonio, en el Distrito Judicial de Lima Norte 2019. La investigación fue cualitativa, de nivel descriptivo, empleándose la guía de entrevista, y guía de análisis de fuente documental en la que se analizaron diferentes artículos científicos. Cuya primera conclusión fue que el tratamiento jurídico penal por parte del fiscal se da de una manera deficiente ya que la estructura legítima de las violaciones informáticos personales contra la propiedad se describe en el marco de las irregularidades del fraude informático. En su conclusión señaló que se apreció un crecimiento de la criminalidad informática debido a la coyuntura social de la pandemia. En sus recomendaciones refirió que se deberían crear fiscalías especializadas en delitos informáticos para que así se pueda dar un adecuado tratamiento jurídico penal por parte del Fiscal, asimismo, podría tener los dispositivos adecuados para realizar exámenes iniciales y no necesitar aludirlos al comando central de la policía.

Tenorio y Tuesta (2012), presentaron el estudio denominado "Legislación del secreto bancario y su relación con el delito de hurto informático de dinero mediante la violación de claves secretas" Escuela de Postgrado de la Universidad Nacional de la Amazonía Peruana, para opta el agrado académico de Magister en Derecho y Ciencias penales, cuyo objetivo de investigación fue determinar cómo influyó la regulación de la legislación del secreto bancario en el incremento del delito de hurto informático de dinero, mediante la violación de llaves misteriosas, en Iquitos durante 2010, en el cual la población de revisión fueron los clientes que fueron bajas, policías, abogados, autoridades de sustancias monetarias e INDECOPI que ven la infracción en estudio, el grado de fiscalización fue correlacional, plan no procesal. Como método la obtención de información utilizó la encuesta. Entre las principales conclusiones señaló que la legislación del secreto bancario en el Perú, no es acorde con el avance tecnológico y el incremento de la criminalidad cibernética, asimismo señaló que el misterio bancario establece un obstáculo en el estudio de la infracción del robo de efectivo informático, ya que el secreto bancario se resuelve únicamente por solicitud judicial orden 26 en procesos concretos, el cual influyó en la impunidad

de los autores del delito de hurto informático de dinero, es más, ninguna de las instituciones cuenta con estadísticas del registro de instancias de robo de efectivo a los registros de los clientes de los elementos monetarios.

Seguidamente, se procedió a definir las bases teóricas:

Como Fiscalía, siendo esta institución protectores legales y sus capacidades principales son el resguardo de la legitimidad, los derechos de los ciudadanos y los intereses públicos; la representación de la sociedad en los tribunales, por las razones de defender a la familia, los menores y el interés social, así como para garantizar la ética pública; la acusación de irregularidades y la indemnización común. Así mismo, vela por la contrarestación de la infracción dentro de las limitaciones que emanan de la ley y por la libertad de los cuerpos legales y la justa organización de la equidad y las demás que señala la Constitución Política del Perú y el ordenamiento jurídico general de la Nación. (Pavajeau y Barranco, 2017)

Como actuación fiscal, determinando según el Código Procesal Penal, en el artículo 61, la Fiscalía actúa con independencia de criterio, actuará bajo las premisas de la Constitución y la Ley, sin perjuicio a las órdenes generales o lineamientos dictados por el Ministerio Público. - Fiscalía de la Nación. Así como, dirigirá la investigación. Además, practicará o solicitará las diligencias de investigación necesarias, observando no solo las condiciones que permiten ilustrar la acusación, sino que además sirven para absolver o reducir la responsabilidad del sujeto activo (prueba de acusación y liberación). Requerirá al juez de instrucción, las acciones que considere significativas. (Coronado y Segura, 2018)

Como licitud, siente este el componente principal que es legal en el objeto, fundamento o estado de la manifestación, es decir, las manifestaciones deben ser legales en la totalidad de sus apariencias para que la ley las ampare y les dé resultados legítimos. El acto ilícito se caracteriza dentro de una progresión de estatutos: Que se cambie de acuerdo con el estándar ético de un público en general y de una época. Eso no está restringido por la ley. Que el derecho positivo lo dirija o asigne. Para algunos propósitos que sea equitativo. (Rodríguez, 2021)

Sobre pruebas digitales, siendo estos los resultados de los avances tecnológicos, está resultando cada vez más incesante que en un proceso judicial se utilicen en juicio pruebas de origen digital. No obstante, el compromiso básico de este tipo de prueba no se concede constantemente y es importante decidir el método correcto para hacerlo. (Santos, 2020)

La prueba digital, es todo aquel dato avanzado que demuestra la verdad de una realidad insistida por las tertulias y que es importante con el objeto del ciclo legal. Además, alude a cualquier tipo de datos informáticos. Es más probable que los datos se entreguen, guarden o envíen por medios avanzados digitalizados. (Vilca, 2018)

Según el artículo 299 de la Ley 1/2000, de 7 de enero, de Procedimiento Civil, establece el método de confirmación que podrá ser utilizado en los tribunales. De ella, la idea de informe digital puede ser removida por implicación, explícitamente del artículo 299.2 cuando dice "los instrumentos que permiten el registro y conocer o recrear palabras, información, cifras y operaciones". (Vilca, 2018)

La ciberdelincuencia, o ciberdelito es una manifestación que viola la ley y es utilizado por avances de tecnología (TIC) para asaltar sistemas, redes, información, sitios o para trabajar con una infracción. El ciberdelito difiere de los delitos convencionales en que no tiene fronteras físicas o geográficas y puede llevarse a cabo no tanto con esfuerzo sino con más sencillez y rapidez que los delitos estándares (aunque esto depende del tipo de delito cibernético) (Vílchez, 2020)

Los ciberdelincuentes atacan a personas, organizaciones y gobiernos con diversos objetivos: Dañar sus sistemas informáticos, normalmente, para utilizar estos métodos innovadores y acceder a carteras de información individual, incluso generar una estafa económica por los medios de plataformas de transferencias. También, llevar delitos normales mediante medios cibernéticos para agredir a las personas directamente y perpetrar una gran cantidad de delitos a través del espacio virtual. (Rojas, 2016)

Cuando hablamos de delitos informáticos, menciona Lamperti (2017) que es una infracción que debe ser gestionada penalmente; entonces, en ese punto se podría decir que la manifestación cae dentro de la tipología delictiva, esto es lo que se

conoce como principio de legalidad, y el juez está prohibido de sancionar diferentes conductas que no están rigurosamente ordenadas en el derecho penal. A través de los avances tecnológicos suplanta la identidad de un individuo, dado que tales resultados directos en cualquier daño material o moral, será rechazado con una pena privativa de libertad de menor de tres ni mayor de cinco años.

El delito informático es la corriente ilícita y culpable que influye en la seguridad de la información y el derecho básica de protección de las personas, a través del tratamiento engañoso de la información, que son reconocidos en diferentes instancias de supuestos delitos electrónicas. Posteriormente, se puede decir que la infracción del delito informático es lo que implica el uso regular, ilícito y culpable directo que se lleva a cabo utilizando medios de información, para beneficio o no. (Santacruz y Hermosa, 2019)

El fraude informático alude al fraude realizado mediante una computadora o Internet. La piratería informática es el hacker que es representando como un fraude: el delincuente utiliza aparatos modernos e innovadores para acceder de forma distante a datos confidenciales. Otro tipo de fraude incluye la interferencia de una transmisión electrónica. Esto puede provocar el robo de una contraseña, un número de cuenta de tarjetas u otros datos confidenciales de una identidad. (Oxman, 2013)

Por otra parte, el delito de fraude informático, influye adicionalmente en la gran legitimidad que imparte a los diferentes ciberdelitos, denominados "Funcionalidad informática". Dicho recurso adquiere una importancia excepcional, ya que la mayoría de los casos de estos tipos de delitos que se completan utilizan Internet como escenario para la ejecución de una conducta delictiva. (Mayer y Oliver, 2020)

La ley gubernamental caracteriza al fraude informático como la utilización de una computadora con la finalidad de distorsionar información para instigar a otra persona a una pérdida económica. Los delincuentes pueden robar la información de varias maneras En primer lugar, pueden cambiar la información ingresada en la computadora sin aprobación. Sin duda, los trabajadores pueden utilizar esta técnica para modificar estos datos y abusar de las reservas de fondos. En segundo lugar, los infractores de la ley pueden cambiar o eliminar los datos guardados. En tercer lugar, los delincuentes modernos pueden reelaborar códigos de programación y

transferirlos al sistema central de un banco para que el banco proporcione los caracteres del cliente. Los estafadores cibernéticos podrían utilizar estos datos para realizar compras con tarjetas no aprobadas. (Ramírez y Castro, 2016)

La suplantación de identidad es una articulación informática que se utiliza para aludir a las manipulaciones informáticas llevadas a cabo por infractores de la ley para engañar, obtener datos individuales, contraseñas, etc., de manera ilegal. Asimismo, el Pisher o delincuente digital que utiliza el diseño social (Seguridad informática), imita o suplanta la identidad de un individuo u organización de confianza en una correspondencia electrónica, como correo electrónico, WhatsApp, redes sociales, llamadas o SMS. (Aguilar, 2019).

La perennización, mediante esta operación se preserva utilizando credenciales de acceso a plataformas del internet que pueden ser obtenidas desde los mismos dispositivos o información digital aportada por el mismo titular de la fuente de datos. (Semprini, G., Nilles, G., & Silva, G., 2021)

Finalmente, sobre Obtención de evidencia digital tenemos que entender que es el Procedimiento mediante el que se requiere a un proveedor o fuente de información el resguardo y respaldo cierta información que servirá como evidencia digital, para su posterior solicitud de obtención.

Por otro lado, se ha obtenido legislación comparada del delito de fraude informático de la siguiente manera:

En Perú, el tipo determina a la persona deliberada e ilegítimamente busca por sí mismo o por uno más un beneficio ilícito en perjuicio de un tercero a través del diseño, presentación, modificación, erradicación, cancelación, clonación de datos informáticos o cualquier manipulación en la actividad de un sistema informático. (Ley 30096, 2013, Articulo 8)

En Colombia, según la Ley N° 1273, en su artículo 69K del año 2009, refiere sindica al individuo que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a otra persona ante los sistemas de autenticación y de autorización establecidos. (Código Penal de Colombia, 2000, Articulo 2691)

En Alemania, se describe a quien, decidido, a procurarse para sí o para un tercero un beneficio patrimonial ilícito, en la medida en que perjudique el patrimonio de otro, por una mala organización del programa, por la utilización de información incorrecta o inadecuada, por información no aprobada, o en todo caso por impacto no autorizado en el desarrollo de la interacción (...). (Código Penal Alemán, 1871, Artículo 263a)

En España, se sindica a quienes, impulsados por los ingresos, utilizan la astucia suficiente para provocar un error en otro, mostrándolo para completar una demostración de actitud en perjuicio propio o ajeno. (2) los siguientes también son vistos como litigantes: a) los individuos que, en beneficio y utilizando algún control informático o dispositivo comparativo, obtienen una transferencia no consentida de cualquier recurso patrimonial por el obstáculo de otro; b) las personas que hacen, presentan, tienen o trabajan con programas informáticos, explícitamente planeados para someter extorsión en este artículo (…). (Código Penal de España, 1995, Articulo 248)

Asimismo, se obtuvo legislación comparada del delito de suplantación de identidad de la siguiente manera:

En Perú, según la Ley de Delitos Informáticos, refiere a este tipo penal como: el que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. (Ley 30096, 2013, Articulo 9)

En Chile, en cambio describe como el actor de este delito a la persona que usurpa el nombre de otro será castigado con presidio menor en su grado mínimo, sin perjuicio de la pena que pudiere corresponderle a consecuencia del daño que en su fama o intereses ocasionare a la persona cuyo nombre ha usurpado. (Código Penal de Chile, 1874, Articulo 214)

En España, se imputa a quien usurpe el estado civil de otro será castigado con la pena de prisión de seis meses a tres años. (Código Penal de España, 1995, Articulo 401)

En Ecuador, se describe a la persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años. (Código Orgánico Integral Penal, 2014, Articulo 212)

Según el Convenio de Budapest, en el artículo 7, describe a la Falsificación Informática como una suerte de guía que: Cada parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las partes podrán exigir que exista una intención dolosa o delictiva similar para que se considera que existe responsabilidad penal.

Congruentemente, la presente investigación al cumplir con los estándares respectivos, describe Jurisprudencia Extranjera recabada, como fuente importante de la siguiente manera:

En este ítem podemos citar el expediente N.º: 2387/2014 del Tribunal Supremo, Sala de lo Penal, Sentencia Nº 300/2015, de España, que señala:

“Y es que la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido” (Sentencia Nº:300/2015, Tribunal Supremo, Sala de lo Penal, 2015)

Analizando lo establecido en la jurisprudencia española, denota la importancia sobre la manipulación de los documentos digitales.

Aunado a ello, es importante y enriquecedor citar Jurisprudencia Nacional:

Por lo que, se tiene el expediente N ° 99-09 (527-09), 2012, de la Corte Superior de Justicia de Lima, Segunda Sala Especializada en lo Penal para Procesos con Reos en Cárcel, en el acápite 12 de la Evaluación de la Prueba Actuada y Determinación de Responsabilidad Penal, menciona que, para efectos de garantizar la validez de las evidencias digitales estas necesariamente deben de describir las características y propiedades de dicha evidencia para que luego no exista cuestionamiento, en ese sentido declara:

“Tal requerimiento cobra mayor exigencia tratándose de dispositivos de almacenamiento de la información (evidencia digital) cuyas características en cuanto a la posibilidad de ser modificados difieren según el tipo de dispositivo del que se trate, así por ejemplo mientras los discos compactos CD-R no puede ser modificados, los discos compactos CD-RW si pueden ser regrabables, de ahí que para efectos de garantizar su plena identidad es necesario que mínimamente se describa, la clase, cantidad, estado, capacidad, número de registro, color, propiedades, etc., para finalmente sellarse, de tal manera que no se ponga en cuestionamiento su autenticidad”(23 de marzo del 2012)

De lo indicado, podemos señalar que, la evidencia digital obtenida de una fuente informática o medio digital, para poder ser utilizada como medio probatorio necesita cumplir con ciertos requisitos.

III. METODOLOGÍA

3.1. Tipo y diseño

La investigación es de tipo aplicada, tiene la finalidad de centrarse en un tema y ampliar el conocimiento para la evolución de la ciencia y mejorar la comprensión del fenómeno tratado. (Baena, 2017). El estudio será de tipo aplicada ya que se ampliará los conocimientos de las categorías mediante ideas, principios y teorías mejorando la determinación del problema de la investigación.

La metodología cualitativa es el método que recopila los datos no numéricos y evalúa los datos no estandarizados. (Azcorra y López, 2016). Para la investigación fue de enfoque cualitativa porque se recogió los datos no numéricos ni estadísticos para la obtención de la visión del comportamiento del tema de la investigación

La investigación explicativa describe los hechos para encontrar el problema, se encarga de encontrar las causas de los hechos. (Hernández, et al., 2014). La investigación fue de nivel explicativo ya que se examinó el problema y la relación causal de las categorías, de tal manera explicando los aspectos de la investigación.

El diseño de la teoría fundamentada analiza la complejidad del fenómeno con los intereses del investigador y con la colaboración activa de los involucrados en el estudio. (Páramo, 2015). El estudio fue de diseño teoría fundamentada ya que con la recolección de datos del campo (los participantes) sirvió como sustento para la investigación.

3.2. Categorías, Subcategorías y matriz de categorización

Tabla 1: Matriz de categorización

N^0	Categoría	Subcategoría 1	Subcategoría 2
1	Actuación Fiscal	Delito de Suplantación de identidad	Delito de fraude informático
2	Pruebas digitales	Obtención de pruebas digitales	Perennización de pruebas digitales

Fuente: Elaboración propia

3.3. Escenario de estudio

Es el universo o escenario geográfico el estudio que se investiga para dar a conocer las características. (Hernández y Mendoza, 2018)

La investigación se realizó en Lima centro, siendo la población del estudio los fiscales y asistentes de la Fiscalía Especializada en Ciberdelincuencia.

3.4. Participantes

Los participantes es la población que se investiga para la recolección de datos (Hernández y Mendoza, 2018). Los participantes fueron los fiscales y asistentes de la Fiscalía Especializada en Ciberdelincuencia de Lima Centro.

El muestreo no probabilístico es la selección de acuerdo al investigador de las muestras basadas. (Otzen y Manterola, 2017). En el estudio se realizó el muestreo no probabilístico por conveniencia ya que se eligió en base del criterio del investigador los entrevistados.

Tabla 2: Caracterización de los sujetos.

N^0	Nombres y Apellidos	Ocupación	Lugar de trabajo
1	Marilyn Rocío Narváez Morán	Fiscal Adjunto provincial	Ministerio Público- Fiscalía Especializada en Ciberdelincuencia
2	Kimberly Madueño Oscorima	Asistente Administrativo (Asist. Fiscal)	Ministerio Público- Fiscalía Especializada en Ciberdelincuencia
3	Jhonatan Cachique Abundo	Asistente en Función Fiscal	Ministerio Público- Fiscalía Especializada en Ciberdelincuencia
4	Jesús Pedro Ojeda Valdiviezo	Fiscal Adjunto Provincial	Ministerio Público- Fiscalía Especializada en Ciberdelincuencia
5	Jessica Pamela Cajo Rodas	Asistente en Función Fiscal	Ministerio Público- Fiscalía Especializada en Ciberdelincuencia
6	Angelica Lorena Pérez Asencio	Fiscal Adjunto Provincial	Ministerio Público- Fiscalía Especializada en Ciberdelincuencia
7	Mónica Rocío Vargas Carpio	Fiscal Adjunto Provincial	Ministerio Público- Fiscalía Especializada en Ciberdelincuencia
8	Jonathan Cirilo Portillo Vela	Fiscal Provincial	Ministerio Público- Fiscalía Especializada en Ciberdelincuencia

Fuente: Elaboración propia.

Los participantes que intervinieron en la investigación son fiscales y asistentes de la Fiscalía Especializada en Ciberdelincuencia de Lima Centro.

3.5. Técnicas e instrumentos de recolección de datos

Técnica

La técnica es el procedimientos e instrumentos que tiene la finalidad de recopilar información del desarrollo de la investigación. (Baena, 2017)

La técnica para la investigación fue la entrevista, ya que se recogió información mediante las repuestas de los fiscales y asistentes de la Fiscalía Especializada en Ciberdelincuencia de Lima Centro.

Instrumento

El instrumento son recursos de medición que el investigador aplica para extraer datos e información sobre un tema determinado. (Hernández y Mendoza, 2018)

Para el estudio se usó el instrumento fue una guía de entrevista para la recolección de información de las categorías y luego ser procesados para analizar los resultados. (ver anexo 3)

3.6. Procedimientos

Primera etapa, se planteó el título de investigación y la realidad problemática internacional y nacional a través de libros, artículos y tesis. Por lo mencionado, se procedió a realizar la justificación del estudio para detallar el motivo de la investigación; seguidamente, se planteó los problemas, objetivos y los supuestos. Por último, se definió los antecedentes internacionales y nacionales para el respaldo de la investigación. También, se definió las bases teóricas de las variables.

Segunda etapa, se realizó la metodología describiendo el tipo de investigación que fue aplicada, enfoque cualitativo y diseño de teoría fundamentada. Los participantes fueron los fiscales y asistentes de la Fiscalía Especializada en Ciberdelincuencia de Lima Centro. Por otro lado, el muestreo fue no probabilístico por conveniencia. Seguidamente, la técnica utilizada fue la entrevista y el instrumento guía de entrevista permitiendo la recolección de datos.

Tercera etapa, los datos seleccionados por medio del instrumento fueron recopilados para la interpretación, contrastando las hipótesis de la investigación. Finalmente, se realizó las discusiones con el respaldo de los antecedentes y se presentaron las conclusiones y recomendaciones.

3.7. Rigor científico

El rigor científico es aquel juicio crítico que se tiene mediante la investigación, estableciendo viabilidad, valor y respaldo de los métodos y análisis de datos procesados que se realizan. (Trochim, 2020)

Para la investigación fue en base a la recolección de datos de los entrevistados y análisis de información de diferentes autores que contribuyeron para el desarrollo de la investigación

Dependencia

Según Hernández y Mendoza (2018). La dependencia, es el grado en que los investigadores que recolectan datos similares al mismo contexto en el que se desarrolló en una investigación inicial, con una coherente interpretación. Por ello, para la presente investigación se recogió y ordenó los datos con interpretación y coherencia para la importancia del estudio.

Credibilidad

Para Moscoso y Díaz (2018) la credibilidad es demostrar que los resultados de una investigación sean verídicos para los participantes que formaron parte del estudio. Por ende, se generó dicho criterio ya que de acuerdo a las experiencias de los participantes se demostraron resultados verídicos.

Transferencia

Según Hernández y Mendoza (2018) tiene relación a que un trabajado realizado pueda ser aplicado a contextos similares para la comprensión del problema estudiado. Con los resultados cualitativos de la investigación se pudo analizar el problema y dar sugerencias de soluciones.

Conformabilidad

Para Moscoso y Díaz (2018) menciona que tiene relación con la credibilidad ejerciendo un rastreo de datos. La investigación rastreó datos para dar explicaciones con claridad para ser interpretadas.

3.8. Método de análisis de datos

Describe, organiza los datos existentes que fueron recopilados en base a las preguntas de la investigación para luego ser interpretadas**.** (Narkhede, 2020).

En la investigación se recopiló datos en base a las preguntas estructuradas de la entrevista, además, se interpretó y analizó los datos obtenidos para la determinación de conclusiones.

3.9. Aspectos éticos

La investigación tuvo referencias bibliográficas de fuentes confiables para respaldar el estudio, también tuvo información original sin plagio. Asimismo, se usó la guía de productos de información de la UCV, además los datos recopilados no fueron alterados y fueron validado por juicios de expertos y se contó con el consentimiento de los fiscales y asistentes de la Fiscalía Especializada en Ciberdelincuencia de Lima Centro.

IV. RESULTADOS Y DISCUSIÓN

En el presente trabajo se obtuvo información mediante el instrumento guía de entrevista, del cual se obtuvieron datos que, luego fueron analizados para continuar con la discusión correspondiente, en mérito de poder efectuar la conclusión de nuestro trabajo y las recomendaciones debidas más adelante, todo ello, bajo el cumplimiento estricto de los objetivos éticos y académicos planteados.

4.1. Resultados de investigación

Se muestran los resultados de los entrevistados, asimismo el análisis e interpretación.

Entrevistados.

E1- Marilyn Rocío Narváez Morán.

E2- Kimberly Madueño Oscorima.

E3- Jhonatan Cachique Abundo.

E4- Jesús Pedro Ojeda Valdiviezo.

E5- Jessica Pamela Cajo Rodas.

E6- Angelica Lorena Pérez Asencio.

E7- Mónica Rocío Vargas Carpio.

E8- Jonathan Cirilo Portillo Vela.

Objetivo General: Analizar la afectación de la actuación fiscal en la obtención de pruebas digitales en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

Tabla 3: Respuestas de la primera pregunta del objetivo general.

1- ¿En su país ofrecen programas de capacitación en Ciberdelincuencia a la Policía Nacional, Ministerio Público y Órganos de Justicia en general?	
E1	Con la creación de fiscales especializados en ciberdelincuencia en el distrito fiscal de lima, se han iniciado con las capacitaciones a los integrantes de los despachos, pero no tengo conocimiento que se haga los mismo con la Policía Nacional.
E2	Si, periódicamente, y por iniciativa de ellos, los organismos internacionales a los que nos encontramos adscritos.
E3	En el Perú si ofrecen programas de capacitación a las instituciones antes referidas, pero más que capacitación se debería enseñar estrategias para resolver la problemática de manera certera.
E4	Pese que a la ley de delitos informáticos N^0 30094 fue publicada en el año 2013, aun es insípida el conocimiento que pueda tener la policía, el ministerio público o el poder judicial respecto a los ciberdelitos, no obstante, se están apreciando cambios como la creación de una fiscalía especializada en la investigación de estos delitos.
E5	Con el paso del tiempo se están ofreciendo dichas capacitaciones y eso es una base de incremento de los delitos informáticos que sufren los ciudadanos.

E6	Sí, la unidad Nacional de ciberdelincuencia del Ministerio Publico, se capacita progresivamente.
E7	Actualmente, las Fiscalías especializadas en ciberdelincuencia vienen recibiendo capacitación de la oficina de Naciones Unidas contra la droga y delito.
E8	En líneas generales, la capacitación no es generalizado, se da solo o en su mayoría para las áreas especializadas.
Interpretación: Se interpreta que en el Perú si se están realizando programas de capacitación a las fiscalías especializadas en ciberdelincuencia; no obstante, no se tiene conocimiento de los otros órganos de justicia, por lo que se advierte una falta de comunicación interinstitucional.	

Fuente: Elaboración propia.

Tabla 4: Respuestas de la segunda pregunta del objetivo general

2- ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos?	
E1	Nuestra legislación no ha establecido una política estratégica para prevenir la comisión de un delito informático, únicamente se tiene las recomendaciones realizadas por las entidades financieras y respecto a la sanción por estos delitos que se tiene en la ley N^0 30096.
E2	No, al ser delitos relativamente nuevos y complejos por el detalle de su ejecución, siguen teniendo grandes barreras en su prevención.
E3	No, porque muchas de las instituciones encargadas de prevenir y sancionar el delito informático no unifican criterios ya que muchas veces ante un mismo caso utilizan criterios distintos
E4	En mi opinión la mayoría de delitos que atentan contra el patrimonio, debería optarse por mecanismos alternativas de resolución de conflictos respecto a las políticas de prevención, son casi nulas, nuestro estado es ineficiente, por lo que siempre tiende a endurecer la incidencia delictivo, sin dar ninguna solución.
E5	Para la prevención opino que no las hay, porque inclusivo en las entidades bancarias no cuentan con suficientes medidas de seguridad, en cuanto a la sanción aún se trabaja en ello.
E6	No, sigue habiendo ineficiencia en las instituciones encargados en dicho rol, ya que aún se presentan barreras para la prevención.

E7	La implementación de la ley N^0 30096 y su modificatoria por ley N^0 30171 es una forma de prevención. Sin embargo, requiere adaptarse a los cambios sociales y el desarrollo tecnológico.
E8	Considero que no existen adecuados programas de difusión por parte del Estado para prevenir delitos informáticos.
Interpretación: Se deduce que el Estado no ha propuesto estrategias adecuadas para la prevención de delitos informáticos; siendo que, la legislación nacional de delitos informáticos, no es suficiente tanto para su prevención o para la búsqueda de una sanción.	

Fuente: Elaboración propia.

Tabla 5: Respuestas de la tercera pregunta del objetivo general.

3- ¿Qué opina sobre la creación de las Fiscalías Especializadas en Ciberdelincuencia en el Perú, considera que se han visto cambios significativos en la actuación fiscal en la lucha contra los delitos informáticos?	
E1	Teniendo en cuenta el incremento de denuncias por delitos informáticos se crearon estos despachos fiscales especializados, que teniendo un criterio por competencia inmaterial y proyectando una estrategia de investigación adecuada, se lleve a cabo la investigación de manera eficiente para la lucha contra delitos.
E2	Considero un gran avance en el sistema de justicia al crear la FCEC, pues resulta de mucha importancia los delitos, más aún los complejos.
E3	Opino que la fiscalía especializada en la ciberdelincuencia tiene un rol muy importante, ya que ayuda significativamente a que no siga creciendo de manera acelerada el tipo de delito.
E4	La creación de una fiscalía especializada es un gran avance, pero para dar cambios y resultados aún es muy pronto.
E5	Me parece muy importante su creación, ya que al ser especializado solo se enfocan en los delitos cibernéticos, asimismo, los cambios han mejorado, aunque es un poco lento por el apoyo insuficiente de determinados establecimientos o entidades, ya que a ellos se le solicitan información, pero demoran en contestar.
E6	Sí, los delitos informáticos tienen una estrategia de investigación diferente a los delitos comunes.

E7	Sin duda simboliza un avance significativo en la lucha contra los ataques informáticos, la fiscalía especializada ha iniciado recientemente sus funciones, los cambios surgirán en un mediano plazo.
E8	Considero que es un avance importante para reconocer la importancia del delito y la necesidad de establecer la especialización para la lucha del delito.
Interpretación: Tras lo mencionado, concuerdan que la creación de una fiscalía especializada en la ciberdelincuencia es primordial para la reducción de estos tipos de delitos, de tal forma haya investigación eficiente y resultados satisfactorios, además de contar con profesionales especializados en la materia. Sin embargo, aun los cambios no son observables, ya que la creación de estas fiscalías es reciente.	

Fuente: Elaboración propia.

Tabla 6: Respuestas de la cuarta pregunta del objetivo general

4- ¿Considera usted que la legislación sobre delitos informáticos en el Perú es eficiente para la obtención y perennización de material probatorio? ¿Por qué?	
E1	No, porque la ley N^0 30096 únicamente en su primera disposición complementaria final establece sobre la conservación de material probatorio, después no se tiene una legislación específica.
E2	Considero que no se encuentran brindada con la realidad y las leyes internas del país, puesto que se debe tener cuidado con los datos a los cuales se quiere y necesita acceder, sin vulnerar otra.
E3	No, ya que no se cuentan con especialistas en esta materia, por la misma razón de que es una nueva materia para muchos aquellos que imparten justicia.
E4	Si, es eficiente ya que se cuenta con las medidas de derechos para la conservación del material probatorio.
E5	No es suficiente, ya que para ellos se necesita una especialización constante, puesto que la tecnología no va en progreso.
E6	No es eficiente, ya que hace falta de especialización para esta materia, además no se tiene una legislación específica.
E7	No, en la medida que no regulan los supuestos típicos del delito, más no el procedimiento para obtener la prueba.

E8	Considero que existe ausencia de protocolos, de guías de actuación conjunta para el manejo de este material probatorio.
Interpretación: Se contrasta que la legislación de delitos informáticos no es eficiente, por lo tanto, no aporta un procedimiento claro para la perennización y obtención del material probatorio.	

Fuente: Elaboración propia.

Tabla 7: Respuestas de la quinta pregunta del objetivo general

5- ¿Considera usted que la obtención y perennización de evidencias digitales requieren de una adecuada especialización? ¿Por qué?	
E1	Si, porque a fin de la evidencia digital posea valor necesario para el juicio penal, esto debe ser recibido por el perito informático forense de la oficina de Pericia.
E2	Considero que sí, puesto que los datos a los cuales se necesitan acceder son de calidad personal y se podría vulnerar otros derechos fundamentales.
E3	Si, ya que para poder obtener resultados satisfechos es necesario tener especialistas en delitos de ciberdelincuencia, ya que su labor será más capaz y minucioso.
E4	Es de suma importancia que las evidencias digitales encontradas sean conservadas y perennizadas por un perito especialista, dado que estas evidencias se encuentren en entornos digitales, por lo que su volatilidad requiere de un conocimiento especial, además que estas evidencias deberán constituirse en material probatorio.
E5	Si, puesto que el uso de las TICS y con la globalización va en aumento. La tecnología va en un paso más allá y para eso la especialización cubre un papel muy importante.
E6	Definitivamente, es necesario que tanto el personal Fiscal, como administrativo se encuentren capacitados en la obtención y perennización de las evidencias, los mismos que deben ser ejecutaos con rapidez.
E7	Sí, pues la evidencia digital presenta determinadas características como la velocidad, volatilidad y fragilidad.

E8	Sí, porque para la obtención de pruebas digitales se requiere un mayor conocimiento, manejo de concepto y procedimiento en cada caso.
Interpretación: Mediante la contrastación de respuestas, se analiza que, si se requiere de una buena especialización ya que las evidencias digitales son la fuente del material probatorio, que será contrastada, de ser el caso, por un perito.	

Fuente: Elaboración propia.

Tabla 8: Respuestas de la sexta pregunta del objetivo general.

6- ¿Considera usted que el valor probatorio de las evidencias digitales es determinante para acreditar la responsabilidad por delitos informáticos de fraude informático y suplantación de identidad? ¿Por qué?	
E1	En el caso específico de la evidencia digital sea el único medio probatorio para determinar que el imputado es el responsable de la comisión del ilícito penal, esta si es determinante.
E2	Si, puesto que, al ser incorporados de manera correcta, se podría tener claridad del responsable conllevando a un adecuado proceso con carácter garantista.
E3	No, ya que para acreditar tal responsabilidad se requiere conocer y valorar a otros medios de prueba.
E4	En relación a que estas evidencias digitales se constituirán en material probatorio se puede elaborar la teoría del caso.
E5	Claro que sí, porque las evidencias digitales también pueden ser materia de falsificación y para ello se necesita acreditar su valor probatorio y su importancia en las investigaciones.
E6	Sí, sobre todo en los delitos de suplantación de identidad donde su medio son las redes sociales, correos electrónicos y otros elementos de comunicación.
E7	Sí, en la medida que solo a través de la prueba, en cualquier tipo de proceso o procedimiento, se puede acreditar la responsabilidad del sujeto activo.
E8	Se estima que su corrido manejo es importante porque es necesario obtener pronunciamientos adecuados.

Interpretación: Se deduce que sí, las evidencias digitales es el medio de valor probatorio de la comisión del ilícito penal para tener la claridad de los hechos y por lo tanto un adecuado proceso y solución del caso.

Fuente: Elaboración propia.

Objetivo Específico 1: Determinar como la obtención de pruebas digitales influye en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro

Tabla 9: Respuestas de la primera pregunta del objetivo específico 1.

1- ¿La legislación de su país influye que los órganos de justicia permitan a las autoridades investigadoras (Fiscal) la obtención de medios de prueba mediante el uso de medidas limitativas de derecho en los delitos: contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?	
E1	Los datos personales en Perú están protegidos institucionalmente y mediante la ley especial N.° 29733. Sin embargo, el persecutor del delito requiere la medida de estos derechos, cuando se presenten los presupuestos establecidos en la norma procesal.
E2	Si, una vez iniciada la investigación y esta se considere necesario, se formula las medidas restrictivas del derecho.
E3	Si, ya que muchas veces hay derechos que favorecen a la persona que ha cometido un delito como lo señalado, impidiendo así el actuar inmediato de los fiscales.
E4	El código penal contempla las medidas tentativas correspondientes, los cuales deben estar debidamente fundamentadas para que el juez de investigación prepare el requerimiento fiscal.
E5	Si, ya que dichas medidas limitativas son requeridas en su oportunidad bajo ciertos fundamentos y con el resultado se logra contra con mayor información.
E6	Sí, debido a que hay derechos de propicio a los que establecen un constitutivo delito, lo que genera al fiscal retraso en su actuación.

E7	Sí, conforme ello lo precisa el artículo 202 del código proceso penal.
E8	Estimo que sí, ya que existen herramientas que deben ser utilizados e interpretadas a la luz de los avances para que el fiscal proceda con el requerimiento.
Interpretación: se interpreta que la legislación si influye en los órganos de justicia para la obtención de medios de prueba con las medidas restrictivas de derechos para que el juez determine el requerimiento de la fiscalía.	

Fuente: Elaboración propia.

Tabla 10: Respuestas de la segunda pregunta del objetivo específico 1.

2- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta obtención de material probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático y contra la fe pública, en la modalidad de suplantación de identidad?	
E1	Que el Ministerio Público por el poco presupuesto no tiene el suficiente material, logística necesaria y la Fiscalía Especializada en Ciberdelincuencia al estar recientemente creada carece de estas, además, es necesario contar con suficiente personal técnico para la ejecución de la parte técnica de estos delitos.
E2	Lo considero escasa, aun no se tiene un amplio manejo de la adecuada recolección de evidencias.
E3	Si bien se puede tener el apoyo policial, pero aún falta las herramientas necesarias para obtener resultados inmediatos y satisfactorios.
E4	No, ya que no se cuenta con peritos informáticos necesarios ni la adecuada participación judicial.
E5	No, ya que hay deficiencias y ciertos vacíos legales, aparte la policía no colabora inmediatamente con las diligencias que se le solicita, existe la falta de interés por estos tipos de delitos informáticos.
E6	Sí, además el Ministerio Público cuenta con la asistencia técnica del personal de la Unidad de Ciberdelincuencia de Lima.
E7	Sí, contamos con una Policía Especializada la División de investigación de Delitos de Alta Tecnologías.

E8	Considero que no, el acceso a la información es limitado y existen barreras para el tratamiento de información.
Interpretación: Se corroboro que las herramientas para la obtención de un material probatorio es escaza, es decir no es eficiente debido a que no hay presupuesto suficiente para la implementación de las medidas, además no se obtiene el material probatorio adecuado porque no hay participación seria de parte del personal policial.	

Fuente: Elaboración propia.

Tabla 11: Respuestas de la tercera pregunta del objetivo específico 1.

3- ¿La legislación de su país obliga a una empresa y/o proveedor de servicios, revelar información personal – privada (por ejemplo, datos de una cuenta, titular de una línea telefónica, información de movimiento de una cuenta bancaria, celda de ubicación de línea telefónica, la identidad de sus suscriptores, etc.)?	
E1	No la obliga, pero el órgano jurisdiccional ordena el otorgamiento de esta información, cuando se ha efectuado un requerimiento fundamentado por parte del Ministerio Público.
E2	Solo si en el caso concreto existe la autorización expresa del titular de la cuenta, de lo contrario es denegada por ser confidencial.
E3	No, ya que, para obtener información personal-privada, se requiere previa autorización del titular, salvo en casos excepcionales.
E4	Si, mediante el requerimiento del secreto de las comunicaciones, el cual debe estar debidamente concretado.
E5	No exactamente, siempre hay limitaciones con los datos privados, ya que se busca proteger datos personales del usuario, pero para que ello sea requerido hay previa coordinación con el titular o con el poder judicial (depende de lo que se solicite).
E6	Sí, siempre que dicha solicitud sea seguida y acompañada a la Resolución Judicial. También, puede ser solicitada acompañada de la carta de autorización de la parte agraviada.
E7	Sí, previa autorización judicial.
E8	Sí existen cumplimientos de revelación de información, pero estimo que tiene que ser un proceso de demora para su obtención automática y rápida.

Interpretación: Se deduce que, en el Perú, tras la autorización del titular, una empresa y/o proveedor de servicios, puede remitir información personal, pero con ciertas limitaciones para respetar el espacio y seguridad del dato privado. Sin embargo, la legislación obliga a remitir la información, cuando existe una orden de medida limitativa de derecho, dictada por un órgano jurisdiccional.

Fuente: Elaboración propia.

Objetivo Específico 2: Establecer como la perennización de las pruebas digitales incide en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

Tabla 12: Respuestas de la primera pregunta del objetivo específico 2

1- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta perennización de material probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?	
E1	En cuanto a la perennización, únicamente se cuenta con los peritos de la oficina de peritajes del Ministerio Publico.
E2	De igual forma, lo considero escaso, no se tiene un buen manejo de ello, y se llega a alterar la evidencia.
E3	No, ya que muchas de los escases de estas herramientas hacen que los propios policías y personas encargadas de la investigación filtren el material obtenido,
E4	No, el especialista informático requiere de un equipo más amplio y herramientas potenciales y actualizadas.
E5	No, aún falta mucho por aprender y actualizarnos, así como por parte de la PNP tener mayor compromiso con su colaboración con el fiscal.
E6	No, existen programas que por su costo no son de acceso libre, de igual manera, el personal fiscal y policial necesita más formación en el delito informático, pero la elevada carga no lo hace posible.
E7	No, ya que aún no se obtiene las herramientas adecuadas tanto la División Policial y la Fiscalía Especializada de Ciberdelincuencia.

E8	No, considero que existen deficiencias en la capacitación y en el material logístico.
Interpretación: Según las respuestas de los encuestados, se menciona que aún no se obtienen las adecuadas herramientas para la perennización y la PNP no participa de manera comprometida, lo que genera una investigación deficiente en los delitos informáticos, perjudicando la perennización del material probatorio.	

Fuente: Elaboración propia.

Tabla 13: Respuestas de la segunda pregunta del objetivo específico 2.

2- ¿Considera necesaria la perennización de datos digitales, al existir la posibilidad que se alteren, clonen, modifiquen o borren los datos almacenados en fuentes digitales, si fuera así determine si estos actos lo pueden realizar cualquier persona? Explique	
E1	Justamente esa es la finalidad de la perennización de los digitales, utilizando para ello, las herramientas como el código Hash, entre otros.
E2	Lo considero necesaria, sin embargo, se debe conocer de manera adecuada a que TIC esta más accediendo, debiendo ser un profesional capacitado para ello.
E3	Si, es necesario la perennización de datos digitales, las mismas que deberían ser realizados por profesionales especialistas capacitados para tal situación.
E4	Dada las características de las evidencias, estas deben efectuarse por un perito informático.
E5	Se considera que sea necesario, para estos actos solo se podrían realizar personas que sean especialistas, peritos a que tenga conocimientos solo en ello.
E6	SI es necesario, deben ser ejecutadas por profesionales especialistas utilizando las herramientas correspondientes para el caso.
E7	Es necesario conservar y perennizar los datos digitales o prueba digital ya que dada a su naturaleza puede ser manipulado, borrado o suprimido dentro de un proceso penal la perennización tiene que ser realizada por un agente de la ley para que tenga validez legal.
E8	Sí, por la propia naturaleza de la prueba digital, ello debe ser procesada de forma oportuna.

Interpretación: Se concuerda que, si es necesario, ya que la evidencia digital es todo registro informático almacenado en un dispositivo informático con la finalidad de tener material probatorio para una investigación. Asimismo, concuerdan que los actos de perennización deben ser realizados por un especialista en la materia.

Fuente: Elaboración propia.

Tabla 14: Respuestas de la tercera pregunta del objetivo específico 2.

3- ¿En la perennización de las evidencias digitales en los delitos informáticos de fraude informático y suplantación de identidad se garantiza el derecho a la privacidad e intimidad? ¿Por qué?	
E1	Si, porque lo que se efectúa en la conservación, lo cual será emitida previa resolución judicial que los autorice, de igual modo el juez evalúa porque se ven afectados los derechos fundamentales.
E2	Se considera correcto garantizar la privacidad de las partes, por lo que se debe manejar los procesos adecuados para la obtención de información, salvaguardando la vida privada no competente al caso concreto.
E3	Sí, toda vez que las evidencias obtenidas de manera digital son reservadas y de conocimientos únicamente de las partes del proceso.
E4	SI, toda la información obtenida en el desarrollo de una investigación tiene el carácter de reservarlo.
E5	No exactamente, ya que no se mide en si el contenido de las evidencias digitales, ya que normalmente se busca identificar a los responsables de dichos delitos, pero no se enfocan en los derechos que se evidencian.
E6	Sí, se garantiza el derecho a la privacidad, pero debe ser ejecutado de manera correspondiente para la obtención de datos, sin perjudicar los derechos reservados.
E7	Sí, conforme lo estipula la ley de Protección de datos es una exigencia legal. Además, la intimidad es un derecho fundamental.
E8	Considero que sí, porque es una sola preservación para obtención judicial a futuro, la intimidad no se ve afectada el solo preservar información, su gestión es mínima al fin del proceso.

Interpretación: Se interpreta que, si se garantiza el derecho a la privacidad e intimidad porque la evidencia digital es un registro de información guardada para que sea utilizada como una prueba en el proceso judicial, donde el juez evalúa la originalidad de la evidencia digital

Fuente: Elaboración propia.

4.2. Discusión

A través de los resultados recolectados de los entrevistados y los trabajos previos de la investigación se procedió a realizar la discusión.

Discusión del objetivo general

Analizar de qué manera la actuación fiscal en la obtención de pruebas digitales afecta la investigación de los delitos cibernéticos en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima - Centro

Supuesto general: La actuación fiscal en la obtención de pruebas digitales si afecta la investigación de los delitos cibernéticos en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima - Centro

De acuerdo a la entrevistada Narváez, M. (2021) sostiene que teniendo en cuenta el incremento de denuncias por delitos informáticos se da la necesidad de la actuación del fiscal especializado, que teniendo un criterio por competencia material y proyectando una estrategia de investigación adecuada, se tiene que llevar la investigación de manera eficiente para la lucha contra delitos informáticos. Sin embargo, nuestra legislación no ha establecido una política estratégica para prevenir la comisión de un delito informático, lo que hace que la actuación fiscal no sea de manera satisfactoria. Por otro lado, esto tiene concordancia con el trabajo previo de Ávalos Rivera (2020) que en su estudio mencionó que la incidencia de denuncias de delitos sigue en aumento en los años 2013 a 2020, ya que para el procedimiento de la actuación fiscal existe una demora debido a la falta de estrategias adecuadas para la prevención y sanción de los delitos informáticos.

Asimismo, el entrevistado Ojeda, J. (2021) respecto al valor probatorio de las evidencias digitales, menciona que en el caso específico de la evidencia digital sea el único medio probatorio para determinar que el imputado es el responsable de la comisión del ilícito penal, esta es determinante para la elaboración de la teoría del caso. Por otro lado, Cajo, J (2021) infiere que las evidencias digitales también pueden ser materia de falsificación y para ello se necesita acreditar su valor probatorio y su importancia en las investigaciones. Esto guarda relación con Condori y Rufino (2020) que en su estudio difundió que el fraude informático en la protección penal de los delitos para la obtención de pruebas digitales contra el patrimonio repercute de manera negativa frente a los derechos patrimoniales de los privados debido a que en la mayoría de los casos de investigación a nivel fiscalía no se logra identificar al autor material del hecho ilícito fraudulento teniendo como consecuencia el archivo definitivo de la investigación quedando impune el delito, siendo afectado la esfera patrimonial de la parte agraviada.

Tras lo mencionado, se concuerda que la fiscalía especializada en ciberdelincuencia es primordial para la reducción de estos tipos de delitos, de tal forma que haya una investigación eficiente y con resultados satisfactorios. Sin embargo, la legislación de los delitos informáticos no es eficiente, por lo tanto, no aporta un procedimiento claro para la perennización y obtención del material probatorio. Por ello, se analizó que se requiere de una buena especialización ya que las evidencias digitales son la fuente del material probatorio, que será contrastada, de ser el caso, por un perito; además, de ser el medio de valor probatorio de la comisión del ilícito penal para tener la claridad de los hechos y por lo tanto un adecuado proceso y solución del caso.

Discusión del objetivo específico 1:

Determinar como la obtención de pruebas digitales influye en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro

Supuesto especifico 1: La obtención de pruebas digitales influye negativamente en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

Según los encuestados Madueño, K y Cachique, J. (2021) hacen mención que existe escasa e inadecuada colaboración policial para una correcta obtención de material probatorio por parte del fiscal contra el delito informático, si bien es cierto, se puede tener el apoyo policial, pero aún faltan las herramientas necesarias para obtener resultados inmediatos y satisfactorios, en los delitos de fraude informático y suplantación de identidad. Lo mencionado tiene relación con la investigación de Piccirilli (2015) mencionó que el paradigma legal de las pericias en general y en particular las pericias de carácter informático, es necesario cubrir las falencias de los procedimientos vigentes, por lo que es necesario contar con un protocolo actual y formalizado para afrontar los desafíos técnicos relativos a las nuevas tecnologías informáticas.

Del mismo modo, Pérez, A. y Vargas, M. (2021) detallaron respecto a la legislación en el delito de suplantación de identidad y fraude informático en las pruebas digitales, siempre hay limitaciones con los datos privados, ya que se busca proteger datos personales del usuario, pero para que ello sea requerido hay previa coordinación con el titular o con el poder judicial (depende de lo que se solicite). De igual manera en el estudio de Gómez Vásquez (2020), refirió que se da el crecimiento de la criminalidad informática debido a que se tiene dispositivos inadecuados para realizar exámenes iniciales de material probatorio.

Por lo antes mencionado, se analizó que las herramientas para la obtención de material probatorio son ineficientes, debido a que no se tiene la implementación de las medidas necesarias; además, no se obtiene el material probatorio adecuado porque no hay participación seria por parte de la Policía Nacional del Perú. Asimismo, tras la autorización del titular, una empresa y/o proveedor de servicios, puede remitir información personal, pero con ciertas limitaciones para respetar el espacio y seguridad del dato privado. Sin embargo, la legislación obliga a remitir la información, cuando existe una orden de medida limitativa de derecho, dictada por un órgano jurisdiccional.

Discusión del objetivo específico 2:

Establecer como la perennización de las pruebas digitales incide en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

Supuesto especifico 2**:** La perennización de las pruebas digitales incide negativamente en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

De acuerdo al encuestado Portillo, J. (2021) fomenta que es necesario conservar y perennizar los datos digitales o prueba digital, ya que dada a su naturaleza puede ser manipulado, borrado o suprimido dentro de un proceso penal, la perennización tiene que ser realizada por un agente de la ley para que tenga validez legal. Asimismo, el encuestado Vargas, R. (2021) sostiene que, en la perennización de las evidencias digitales en los delitos informáticos, se garantiza el derecho a la privacidad e intimidad ya que es una sola preservación para una obtención judicial a futuro, la intimidad no se ve afectada con el solo hecho de preservar información, su gestión es mínima al fin del proceso. Sin embargo, en el estudio de Alarcón D. y Barrera J. (2017), detalla que no se cuenta con programas adecuados en las Organizaciones Públicas, y que los delitos informáticos quedan expuestos por las vulnerabilidades de los sistemas de intercomunicación y que la ciberdelincuencia seguirá aumentando por manipulación de mano negra que poseen habilidades.

Se advierte con esta posición que aún no se obtienen las adecuadas herramientas para la perennización de evidencia digital; aunado a ello, la Policía Nacional del Perú no participa de manera comprometida, lo que genera una investigación deficiente en los delitos informáticos, perjudicando la perennización del material probatorio, ya que la finalidad es obtener la evidencia digital para una investigación, y de cierta forma garantizando el derecho a la privacidad e intimidad.

Finalmente, bajo el principio de la libertad probatoria y la falta de regulación se puede ver el peligro de avasallar garantías individuales, sobre todo vinculadas a la intimidad y privacidad. Por todo ello se vuelve necesaria una regulación procesal específica para la obtención de evidencia digital, en función de las nuevas prácticas en ese ámbito y sobre todo teniendo en consideración los respectivos estándares de sospecha requeridos para cada medida. (Solari M., 2018)

V. CONCLUSIONES

Concluimos lo siguiente:

1. Supuesto general: La actuación fiscal en la obtención de pruebas digitales si afecta la investigación de los delitos cibernéticos en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

   Este supuesto general, es aceptado debido a que, las Fiscalías Especializadas en Ciberdelincuencia son primordiales para la reducción de estos tipos de delitos, sin embargo, tienen una reciente creación, por lo tanto, aun no existen pautas claras, y los resultados no son evidentes. Es decir, lo que se ha detectado que afectaría negativamente a la obtención de pruebas digitales, es que el personal fiscal carece de herramientas o procedimientos claros para la perennización y obtención del material probatorio, además, aún están en proceso de especialización para el tratamiento de la evidencia digital por ser de naturaleza volátil; aunado a ello, el Estado y la legislación de los delitos informáticos, no son suficientes, debido a que no indican políticas de prevención, y por lo tanto, no ayudan a su correcta aplicación punitiva. Por ende, estas carencias afectan a la actuación fiscal en la actualidad. No obstante, cuando se habla de licitud de la obtención de la prueba, verificamos mediante las entrevistas realizadas, que el personal fiscal, en su actuación de obtención de evidencia digital, respeta las formas establecidas por ley, solicitando el permiso al titular de los datos o de lo contrario mediante un mandato judicial.

2. Supuesto especifico 1: La obtención de pruebas digitales influye negativamente en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

   Este supuesto es aceptado, debido a que la obtención de pruebas digitales, está influyendo negativamente en la investigación de estos delitos en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro, debido a que, la legislación establece herramientas para solicitar información

mediante una orden judicial, así como también faculta al titular de la información personal a otorgar a la Fiscalía la autorización correspondiente para la obtención de información; sin embargo, las herramientas para la obtención de material probatorio es escaza. Aunado a ello, no hay participación seria de parte del personal policial en apoyo para la recolección de material probatorio.

3. Supuesto especifico 2: La perennización de las pruebas digitales incide negativamente en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

   Este supuesto es aceptado debido a que aún no se obtienen las adecuadas herramientas y logística para la perennización de evidencia digital y como consecuencia deviene la pérdida de este tipo de información; aunado a ello, la Policía Nacional del Perú no participa de manera comprometida con la conservación del material probatorio, lo que genera una investigación deficiente en los delitos de suplantación y fraude informático, perjudicando la perennización del material probatorio, ya que la finalidad es obtener la evidencia digital para una investigación, y de cierta forma garantizando el derecho a la privacidad e intimidad.

VII. RECOMENDACIONES

Recomendamos lo siguiente:

1. Se recomienda la creación de un protocolo o guía estandarizada de perennización y obtención de evidencia digital Estatal, dirigido a las instituciones del gobierno inmersas en las investigaciones de estos delitos, a modo de herramienta de capacitación en evidencia digital, ello, conllevaría a una actuación fiscal más rápida en la solicitud de preservación y obtención de información a las distintas empresas prestadoras de servicios nacionales e internacionales, y así evitar la pérdida de material probatorio.

2. Se deberían crear más Fiscalías Especializadas en Ciberdelincuencia a nivel nacional para que el Fiscal pueda dar un tratamiento legal criminal satisfactorio en esta clase de delitos, además, de llevar cursos de especialización con talleres prácticos, a todas la Instituciones involucradas en la lucha contra la ciberdelincuencia, como la Policía Nacional, Ministerio Público, Poder Judicial, entre otros; aunado a ello, se debe desarrollar a cabo una mesa de trabajo multisectorial, a efectos de poder crear un manual multifuncional integrado con una debida base legal, que sea una suerte de guía para cualquier funcionario público. Asimismo, generar políticas públicas de prevención a la ciudadanía para evitar y erradicar la ciberdelincuencia en el país.

3. Se recomienda repotenciar a la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), a efectos de poder implementar mayores herramientas necesarias para la obtención de pruebas digitales, y con ello poder cumplir con una participación y apoyo más activo a la Fiscalía Especializada en Ciberdelincuencia.

REFERENCIAS

Ávalos Rivera, Z. (2020). *Ciberdelincuencia: pautas para una investigación fiscal especializada. Informe de análisis del ministerio público*. Disponible en: https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf

Abdulai Mohammed, A. (2016). *Determinantes del miedo a la victimización del crimen de cibernética: un estudio del fraude a la tarjeta de crédito / débito entre estudiantes de la Universidad de Saskatchewan*.

Alarcón D. y Barrera J. (2017). *Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016*. Colombia: Universidad Privada Norbert Wiener. Disponible en: http://repositorio.uwiener.edu.pe/bitstream/handle/123456789/1630/MAESTRO%20%20%20Barrera%20Bar%C3%B3n%2C%20Javier%20Antonio.pdf?sequence=1&isAllowed=y

Amaya Tario, T., Avalos Cisneros, A. y Jule Moreno, K. (2012). "*Respeto Al Derecho De Intimidad En La Estructura De La Ley Especial De Intervención De Telecomunicaciones*". San Salvador: Universidad de El Salvador. Disponible en: http://ri.ues.edu.sv/id/eprint/2671/

Aguilar, E. Suplantación de la identidad digital con fines de trata de personas en Facebook. México: INFOTEC centro de investigación e innovación en tecnologías de la información y comunicación. Recuperado de: https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/363/1/INFOTEC_MDTIC_EAB_26092019.pdf

Azcorra, P. y López, V. (2016). Investigación cualitativa en subjetividad. Psicoperspectivas, 15(1), 1-4. https://www.redalyc.org/pdf/1710/171043532001.pdf

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

Código Orgánico Integral Penal [COIP].10 de febrero de 2014 (Ecuador).

Código Penal. Ley Orgánica 10/1995 de 23 de noviembre (España).

Código Penal. Ley 599 de 2000. 24 de julio del 2000 (Colombia).

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

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

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

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

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

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

Gonzales, J. y Pasmiño, M. (2015). Cálculo e interpretación del Alfa de Cronbach para el caso de validación de la consistencia interna de un guía de entrevista, con dos posibles escalas tipo Likert. Revista Publicando. Ecuador: SSOAR, vol. 2, n. ° 1, pp. 62-77. ISSN 1390-9304. Disponible en: https://www.ssoar.info/ssoar/handle/document/42382.

Gómez Vásquez, J. (2020). "*El tratamiento jurídico penal por parte del fiscal en los delitos informáticos contra el patrimonio, distrito judicial de Lima Norte 2019*". Lima: Universidad Cesar Vallejo. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/53071

Hernández, R., et al., (2014). Metodología de la investigación. 6.^a ed. México, DF: Mc Graw Interamericana Editores. ISBN 9781456223960. Disponible en: http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf.

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

La Asamblea General (2019). *Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos*. Disponible en: https://database.girlsrightsplatform.org/es/entity/kxevttxrvxn?page=1

Lamperti, S. B. (2017). Aspectos Legales. Los Delitos Informáticos. *El rastro digital del delito: aspectos técnicos, legales y estratégicos de la Informática Forense*. Mar de Plata: Universidad FASTA Ediciones.

Ley 30096 de 2013. Regula y sanciona las conductas ilícitas que afectan los sistemas y datos informáticos. 22 de octubre de 2013. Diario Oficial El Peruano.

Mayer, L. y Oliver, G. (2020). *El delito de fraude informático: concepto y delimitación.* Chile: Rev. Derecho tecnológico vol.9 no.1**.** Disponible en: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000100151

Moscoso, L. F. y Díaz, L. P. (2018). Aspectos éticos en la investigación cualitativa con niños. Revista latinoamericana de bioética, 18(1), 51-68. Disponible en: https://www.redalyc.org/jatsRepo/1270/127054340004/127054340004.pdf

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

Oxman, N., (2013). *Estafas informáticas a través de internet: acerca de la imputación penal. Revista de Derecho*; Valparaíso N.º 41, 211-262. ISSN: 0718-6851. Disponible en: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-68512013000200007

Otzen, T. y Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. Int J. Morphol. Temuco: SCIELO, vol. 35, n°.1, pp. 227-232. ISSN 0717-9502. Disponible en: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0717-95022017000100037&lng=en&nrm=iso&tlng=en.

Páramo, D. (2015). La teoría fundamentada (Grounded Theory), metodología cualitativa de investigación científica Pensamiento & Gestión, núm. 39, 2015, pp. vii-xiii. ISSN: 1657-6276. Disponible en: https://www.redalyc.org/pdf/646/64644480001.pdf

Pavajeau, C., Barranco, M. (2017). *Nulidad de la actuación fundada en violación al debido proceso por actuaciones de la fiscalía general de la Nación en la delegación y asignación de funcionarios judiciales especiales para la investigación y acusación en el proceso penal. Derecho Penal y Criminología*;

Bogotá, Tomo 38, N.º 105, 37-75. ISSN: 01210483. https://dialnet.unirioja.es/servlet/articulo?codigo=6718111

Piccirilli, D. (2015). "*Protocolos A Aplicar En La Forensia Informática En El Marco De Las Nuevas Tecnologías (Pericia – Forensia Y Cibercrimen*)". Buenos Aires: Universidad Nacional de la Plata. Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/52212/Documento_completo.pdf-PDFA.pdf?sequence=3&isAllowed=y

Rincón Ríos, Jarvey (2015). *El delito en la cibersociedad y la justicia penal internacional*. Madrid: Universidad Complutense de Madrid. Disponible en: https://eprints.ucm.es/id/eprint/33360/

Rodríguez, J. (2021). *Estado de alarma y protección de la privacidad en tiempos de pandemia: licitud del tratamiento de categorías especiales de datos*. Revista de Derecho Político; Madrid N.º 110, 299-318. ISSN: 0211979X. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7824428

Rojas, J., (2016). *Análisis de la penalización del cibercrimen en países de habla hispana.* Revista Logos, Ciencia & Tecnología; Bogotá Tomo 8, N.º 1, 220-231. ISSN: 2145549X. Disponible en: https://www.redalyc.org/journal/5177/517752176020/

Ramírez, D. A., y Castro, E. F. (2018). *Análisis de la evidencia digital en Colombia como soporte judicial de delitos informáticos mediante cadena de custodia*. Villavicencio: Universidad Nacional Abierta y a Distancia "UNAD".

Santacruz, H., Hermoza, M. (2019). *Los delitos informáticos y su tipificación en la* legislación penal ecuatoriana. Revista Ibérica de Sistemas e Tecnologías de Informação; Lousada N.º 20, 391-400. ISSN:16469895. Disponible: https://www.proquest.com/docview/2318538897/abstract/896D7841D8334111PQ/1?accountid=37408

Santos, T. (2020). *Necesario estudiar y legislar sobre pruebas digitales en juicios electorales*. CE Noticias Financieras, Spanish ed. ContentEngine LLC, a Florida limited liability company; Miami. Disponible en: https://www.milenio.com/politica/juicios-electorales-necesario-legislar-pruebas-digitales

Julia Solari, M. (2018). *La Obtención De Evidencia Digital En Un Marco De Cooperación Internacion*al. Revista Electrónica de Estudios Penales y de la Seguridad ISSN: 2531-1565. Disponible en: https://www.ejc-reeps.com/SOLARI-1.pdf

Trochim, W. (2020). Inferential Statistics. In: Research Methods Knowledge Base [online]. Available in: https://conjointly.com/kb/inferential-statistics/

Tenorio Rojas, J. y Tuesta Gómez, M. (2012). "*Legislación Del Secreto Bancario Y Su Relación Con El Delito De Hurto Informático De Dinero Mediante La Violación De Claves Secretas, Iquitos- 2010"*. Disponible en: https://repositorio.unapiquitos.edu.pe/handle/20.500.12737/2193

Vilca, G. (2018). *Los Hackers: Delito Informático frente al Código Penal Peruano.* (Tesis para obtener el Título Profesional de Abogado). Universidad Nacional Santiago Antúnez de Mayolo, Perú.

Vílchez, R., (2020). *La ciberdelincuencia en el contexto de la pandemia del coronavirus. Una aproximación desde el marco convencional*. Ars Iuris Salmanticensis; Salamanca Tomo 8, N.º 2, 21-25. ISSN: 23405155.Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7931775

Anexo 1: Matriz de categorización

TÍTULO: La obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro 2021					
PROBLEMAS	OBJETIVOS	SUPUESTOS	CATEGORÍAS	SUBCATEGORÍAS	
Problema General	Objetivo General	Supuesto General	Categoría 1	Sub categ.1	Sub categ.2
¿De qué manera la actuación fiscal en la obtención de pruebas digitales afecta la investigación de los delitos cibernéticos en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima - Centro?	Analizar de qué manera la actuación fiscal en la obtención de pruebas digitales afecta la investigación de los delitos cibernéticos en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.	La actuación fiscal en la obtención de pruebas digitales si afecta la investigación de los delitos cibernéticos en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.	Actuación Fiscal	Delito de Suplantación de identidad	Delito de fraude informático
Problemas Específicos	Objetivos Específicos	Supuestos Específicos	Categoría 2	Sub categ.1	Sub categ.2
¿De qué manera la obtención de pruebas digitales influye en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro?	Determinar como la obtención de pruebas digitales influye en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.	La obtención de pruebas digitales influye negativamente en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.	Pruebas digitales	Obtención de pruebas digitales	Perennización de pruebas digitales
¿De qué manera la perennización de las pruebas digitales incide en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro?	Establecer como la perennización de las pruebas digitales incide en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro	La perennización de las pruebas digitales incide negativamente en el delito de suplantación de identidad y fraude informático en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.			

Anexo 2: Matriz de triangulación

Objetivo	Preguntas	ENTDO. 1	ENTDO. 2	ENTDO. 3	ENTDO. 4	ENTDO. 5	ENTDO. 6	ENTDO. 7	ENTDO. 8	Convergencia	Divergencia	Interpretación
Objetivo General	¿En su país ofrecen programas de capacitación en Ciberdelincuencia a la Policía Nacional, Ministerio Público y Órganos de Justicia en general?	Con la creación de fiscales especializados en ciberdelincuencia en el distrito fiscal de lima, se han iniciado con las capacitaciones a los integrantes de los despachos, pero no tengo conocimiento que se haga los mismo con la Policía Nacional.	Si, periódicamente, y por iniciativa de ellos, los organismos internacionales a los que nos encontramos adscritos.	En el Perú si ofrecen programas de capacitación a las instituciones antes referidas, pero más que capacitación se debería enseñar estrategias para resolver la problemática de manera certera.	Pese que a la ley de delitos informáticos N0 30094 fue publicada en el año 2013, aun es insípida el conocimiento que pueda tener la policía, el ministerio público o el poder judicial respecto a los ciberdelitos, no obstante, se están apreciando cambios como la creación de una fiscalía especializada en la investigación de	Con el paso del tiempo se están ofreciendo dichas capacitaciones y eso es una base de incremento de los delitos informáticos que sufren los ciudadanos.	Sí, la unidad Nacional de ciberdelincuencia del Ministerio Publico, se capacita progresivamente.	Actualmente, las Fiscalías especializadas en ciberdelincuencia vienen recibiendo capacitación de la oficina de Naciones Unidas contra la droga y delito.	En líneas generales, la capacitación no es generalizado, se da solo o en su mayoría para las áreas especializadas.	Todos los entrevistados concuerdan que las fiscalías de ciberdelincuencia están siendo capacitadas.	No existe divergencias entre los entrevistado.	Se interpreta que en el Perú si se están realizando programas de capacitación a las fiscalías especializadas en ciberdelincuencia; no obstante, no se tiene conocimiento de los otros órganos de justicia, por lo que se advierte una falta de comunicación interinstitucional.

					estos delitos.							
	¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos?	Nuestra legislación no ha establecido una política estratégica para prevenir la comisión de un delito informático, únicamente se tiene las recomendaciones realizadas por las entidades financieras y respecto a la sanción por estos delitos que se tiene en la ley N0 30096.	No, al ser delitos relativamente nuevos y complejos por el detalle de su ejecución, siguen teniendo grandes barreras en su prevención.	No, porque muchas de las instituciones encargadas de prevenir y sancionar el delito informático no unifican criterios ya que muchas veces ante un mismo caso utilizan criterios distintos	En mi opinión la mayoría de delitos que atentan contra el patrimonio, debería optarse por mecanismos alternativas de resolución de conflictos respecto a las políticas de prevención, son casi nulas, nuestro estado es ineficiente, por lo que siempre tiende a endurecer la incidencia delictivo, sin dar	Para la prevención opino que no las hay, porque inclusivo en las entidades bancarias no cuentan con suficientes medidas de seguridad, en cuanto a la sanción aún se trabaja en ello.	No, sigue habiendo ineficiencia en las instituciones encargados en dicho rol, ya que aún se presentan barreras para la prevención.	La implementación de la ley N0 30096 y su modificatoria por ley N0 30171 es una forma de prevención. Sin embargo, requiere adaptarse a los cambios sociales y el desarrollo tecnológico.	Considero que no existen adecuados programas de difusión por parte del Estado para prevenir delitos informáticos.	Los entrevistados coincidieron que no se tienen las adecuadas estrategias para la prevención y sanción de los delitos informáticos.	En cuanto a esta pregunta no existe divergencia puesto que todos consideraron que no existen estrategias adecuadas para la prevención y sanción de los delitos informáticos.	Se deduce que el Estado no ha propuesto estrategias adecuadas para la prevención de delitos informáticos; siendo que, la legislación nacional de delitos informáticos, no es suficiente tanto para su prevención o para la búsqueda de una sanción.

					ninguna solución.							
	¿Qué opina sobre la creación de las Fiscalías Especializadas en Ciberdelincuencia en el Perú, considera que se han visto cambios significativos en la actuación fiscal en la lucha contra los delitos informáticos?	Teniendo en cuenta el incremento de denuncias por delitos informáticos se crearon estos despachos fiscales especializados, que teniendo un criterio por competencia inmaterial y proyectando una estrategia de investigación adecuada, se lleve a cabo la investigación de manera eficiente para la lucha	Considero un gran avance en el sistema de justicia al crear la FCEC, pues resulta de mucha importancia los delitos, más aún los complejos.	Opino que la fiscalía especializada en la ciberdelincuencia tiene un rol muy importante, ya que ayuda significativamente a que no siga creciendo de manera acelerada el tipo de delito.	La creación de una fiscalía especializada es un gran avance, pero para dar cambios y resultados aún es muy pronto.	Me parece muy importante su creación, ya que al ser especializado solo se enfocan en los delitos cibernéticos, asimismo, los cambios han mejorado, aunque es un poco lento por el apoyo insuficiente de determinados establecimientos o entidades, ya que a ellos se le solicitan	Sí, los delitos informáticos tienen una estrategia de investigación diferente a los delitos comunes.	Sin duda simboliza un avance significativo en la lucha contra los ataques informáticos, la fiscalía especializada ha iniciado recientemente sus funciones, los cambios surgirán en un mediano plazo.	Considero que es un avance importante para reconocer la importancia del delito y la necesidad de establecer la especialización para la lucha del delito.	Los entrevistados coincidieron que la creación de las fiscalías especializadas en ciberdelincuencia es un gran avance.	Tres de los entrevistados señalaron que, si bien es un avance significativo, los cambios y resultados aparecerán posteriormente.	Tras lo mencionado, concuerdan que la creación de una fiscalía especializada en la ciberdelincuencia es primordial para la reducción de estos tipos de delitos, de tal forma haya investigación eficiente y resultados satisfactorios, además de contar con profesionales especializados en la materia. Sin embargo, aun los

		contra delitos.				información, pero demoran en contestar.						cambios no son observables, ya que la creación de estas fiscalías es reciente.
	¿Considera usted que la legislación sobre delitos informáticos en el Perú es eficiente para la obtención y perennización de material probatorio? ¿Por qué?	No, porque la ley N0 30096 únicamente en su primera disposición complementaria final establece sobre la conservación de material probatorio, después no se tiene una legislación específica.	Considero que no se encuentran brindada con la realidad y las leyes internas del país, puesto que se debe tener cuidado con los datos a los cuales se quiere y necesita acceder, sin vulnerar otra.	No, ya que no se cuentan con especialistas en esta materia, por la misma razón de que es una nueva materia para muchos aquellos que imparten justicia.	Si, es eficiente ya que se cuenta con las medidas de derechos para la conservación del material probatorio.	No es suficiente, ya que para ellos se necesita una especialización constante, puesto que la tecnología no va en progreso.	No es eficiente, ya que hace falta de especialización para esta materia, además no se tiene una legislación específica.	No, en la medida que no regulan los supuestos típicos del delito, más no el procedimiento para obtener la prueba.	Considero que existe ausencia de protocolos, de guías de actuación conjunta para el manejo de este material probatorio.	La mayoría de entrevistados señalan que la legislación sobre delitos informáticos no es eficiente para la obtención y perennización de material probatorio.	Solo uno de los entrevistados señala que la legislación de delitos informáticos es eficiente para la conservación de material probatorio.	Se contrasta que la legislación de delitos informáticos no es eficiente, por lo tanto, no aporta un procedimiento claro para la perennización y obtención del material probatorio.
	¿Considera usted que la	Si, porque a fin de la evidencia	Considero que sí, puesto	Si, ya que para poder	Es de suma importanc	Si, puesto que el	Definitivamente, es necesario	Sí, pues la evidencia digital	Sí, porque para la	Todos los entrevistados	No existe divergencias entre	Mediante la contrastac

	obtención y perennización de evidencias digitales requieren de una adecuada especialización? ¿Por qué?	digital posea valor necesario para el juicio penal, esto debe ser recibido por el perito informático forense de la oficina de Pericia.	que los datos a los cuales se necesitan acceder son de calidad personal y se podría vulnerar otros derechos fundamentales.	obtener resultados satisfechos es necesario tener especialistas en delitos de ciberdelincuencia, ya que su labor será más capaz y minucioso.	ia que las evidencias digitales encontradas sean conservadas y perennizadas por un perito especialista, dado que estas evidencias se encuentren en entornos digitales, por lo que su volatilidad requiere de un conocimiento especial, además que estas evidencias deberán constituirse en material probatorio.	uso de las TICS y con la globalización va en aumento. La tecnología va en un paso más allá y para eso la especialización cubre un papel muy importante.	que tanto el personal Fiscal, como administrativo se encuentren capacitados en la obtención y perennización de las evidencias, los mismos que deben ser ejecutaos con rapidez.	presenta determinadas características como la velocidad, volatilidad y fragilidad.	obtención de pruebas digitales se requiere un mayor conocimiento, manejo de concepto y procedimiento en cada caso.	concuerdan que para la obtención y perennización de evidencias digitales requieren de especialización.	los entrevistado.	ión de respuestas, se analiza que, si se requiere de una buena especialización ya que las evidencias digitales son la fuente del material probatorio, que será contrastada, de ser el caso, por un perito.
	¿Considera usted que el valor probatorio	En el caso específico de la evidencia	Si, puesto que, al ser incorpor	No, ya que para acreditar tal responsa	En relación a que estas evidencias digitales	Claro que sí, porque las evidencia	Sí, sobre todo en los delitos de suplantaci	Sí, en la medida que solo a través de la prueba,	Se estima que su corrido manejo es	La mayoría de entrevistados	Solo uno de los entrevistados señala	Se deduce que sí, las evidencias digitales

	de las evidencias digitales es determinante para acreditar la responsabilidad por delitos informáticos de fraude informático y suplantación de identidad? ¿Por qué?	digital sea el único medio probatorio para determinar que el imputado es el responsable de la comisión del ilícito penal, esta si es determinante.	ados de manera correcta, se podría tener claridad del responsable conlleva ndo a un adecuado proceso con carácter garantista.	bilidad se requiere conocer y valorar a otros medios de prueba.	se constituirán en material probatorio se puede elaborar la teoría del caso.	s digitales también pueden ser materia de falsificación y para ello se necesita acreditar su valor probatorio y su importancia en las investigaciones.	ón de identidad donde su medio son las redes sociales, correos electrónicos y otros elementos de comunicación.	en cualquier tipo de proceso o procedimiento, se puede acreditar la responsabilidad del sujeto activo.	importante porque es necesario obtener pronunciamientos adecuados.	concuerdan que las evidencias digitales son determinantes para acreditar la responsabilidad de los delitos informaticos	que, no es determinante la evidencia digital.	es el medio de valor probatorio de la comisión del ilícito penal para tener la claridad de los hechos y por lo tanto un adecuado proceso y solución del caso.
Objetivo Específico 1	¿La legislación de su país influye que los órganos de justicia permitan a las autoridades investigadoras (Fiscal) la obtención de medios de prueba	Los datos personales en Perú están protegidos institucionalmente y mediante la ley especial N.° 29733. Sin embargo, el persecutor del delito requiere	Si, una vez iniciada la investigación y esta se considere necesario, se formula las medidas restrictivas del derecho.	Si, ya que muchas veces hay derechos que favorecen a la persona que ha cometido un delito como lo señalado, impidiendo así el actuar inmediato de los fiscales.	El código penal contempla las medidas tentativas correspondientes, los cuales deben estar debidamente fundamentadas para que el juez de investigación	Si, ya que dichas medidas limitativas son requeridas en su oportunidad bajo ciertos fundamentos y con el resultado se logra contra con mayor	Sí, debido a que hay derechos de propicio a los que establecen un constitutivo delito, lo que genera al fiscal retraso en su actuación.	Sí, conforme ello lo precisa el artículo 202 del código proceso penal.	Estimo que sí, ya que existen herramientas que deben ser utilizados e interpretadas a la luz de los avances para que el fiscal proceda con el requerimiento.	Todos los entrevistados concuerdan que existe una legislación que les permite la obtención de medios probatorios.	No existe divergencias entre los entrevistado.	Se interpreta que la legislación si influye en los órganos de justicia para la obtención de medios de prueba con las medidas restrictivas de derechos para que

	mediante el uso de medidas limitativas de derecho en los delitos: contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?	la medida de estos derechos, cuando se presenten los presupuestos establecidos en la norma procesal.			prepare el requerimiento fiscal.	información.						el juez determine el requerimiento de la fiscalía.
	¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta obtención de material probatorio	Que el Ministerio Público por el poco presupuesto no tiene el suficiente material, logística necesaria y la Fiscalía Especializada en	Lo considero escasa, aun no se tiene un amplio manejo de la adecuada recolección de evidencias.	Si bien se puede tener el apoyo policial, pero aún falta las herramientas necesarias para obtener resultados inmediatos y	No, ya que no se cuenta con peritos informáticos necesarios ni la adecuada participación judicial.	No, ya que hay deficiencias y ciertos vacíos legales, aparte la policía no colabora inmediatamente con las diligencias que se le	Sí, además el Ministerio Público cuenta con la asistencia técnica del personal de la Unidad de Ciberdelincuencia de Lima.	Sí, contamos con una Policía Especializada la División de investigación de Delitos de Alta Tecnologías.	Considero que no, el acceso a la información es limitado y existen barreras para el tratamiento de información.	La mayoría de entrevistados concuerdan que las herramientas y colaboración policial son insuficientes y	Dos entrevistados señalan que cuentan con una policía especializada en ciberdelincuencia.	Se corroboró que las herramientas para la obtención de un material probatorio es escaza, es decir no es eficiente debido a

	por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático y contra la fe pública, en la modalidad de suplantación de identidad?	Ciberdelincuencia al estar recientemente creada carece de estas, además, es necesario contar con suficiente personal técnico para la ejecución de la parte técnica de estos delitos.		satisfactorios.		solicita, existe la falta de interés por estos tipos de delitos informáticos.				escazas, para la obtención de material probatorio.		que no hay presupuesto suficiente para la implementación de las medidas, además no se obtiene el material probatorio adecuado porque no hay participación seria de parte del personal policial.
	¿La legislación de su país obliga a una empresa y/o proveedor de servicios, revelar información personal – privada (por	No la obliga, pero el órgano jurisdiccional ordena el otorgamiento de esta información, cuando se ha efectuado un requerimiento	Solo si en el caso concreto existe la autorización expresa del titular de la cuenta, de lo contrario es denegada por ser	No, ya que, para obtener información personal-privada, se requiere previa autorización del titular, salvo en casos excepcionales.	Si, mediante el requerimiento del secreto de las comunicaciones, el cual debe estar debidamente concretado.	No exactamente, siempre hay limitaciones con los datos privados, ya que se busca proteger datos personales del usuario, pero para	Sí, siempre que dicha solicitud sea seguida y acompañada a la Resolución Judicial. También, puede ser solicitada acompañada de la carta de autorizaci	Sí, previa autorización judicial.	Sí existen cumplimientos de revelación de información, pero estimo que tiene que ser un proceso de demora para su obtención automátic	Todos los entrevistados concuerdan que, para la obtención de información personal-privada, se puede obligar al requerido mediante una	En cuanto a esta pregunta no existe divergencia puesto que todos consideraron que se puede obligar la obtención	Se deduce que, en el Perú, tras la autorización del titular, una empresa y/o proveedor de servicios, puede remitir informació

	ejemplo, datos de una cuenta, titular de una línea telefónica, información de movimiento de una cuenta bancaria, celda de ubicación de línea telefónica, la identidad de sus suscriptores, etc.)?	fundamentado por parte del Ministerio Público.	confidencial.			que ello sea requerido hay previa coordinación con el titular o con el poder judicial (depende de lo que se solicite).	ón de la parte agraviada.		a y rápida.	autorización judicial.	de información personal mediante una autorización judicial.	n personal, pero con ciertas limitaciones para respetar el espacio y seguridad del dato privado. Sin embargo, la legislación obliga a remitir la información, cuando existe una orden de medida limitativa de derecho, dictada por un órgano jurisdiccional.
Objetivo Específico 2	¿Considera usted que se tienen las adecuadas herramientas y colaboración policial	En cuanto a la perennización, únicamente se cuenta con los peritos de la oficina	De igual forma, lo considero escaso, no se tiene un buen manejo de ello, y	No, ya que muchas de los escases de estas herramientas hacen que los propios	No, el especialista informático requiere de un equipo más amplio y herramien	No, aún falta mucho por aprender y actualizarnos, así como por parte de	No, existen programas que por su costo no son de acceso libre, de igual manera,	No, ya que aún no se obtiene las herramientas adecuadas tanto la División	No, considero que existen deficiencias en la capacitación y en el material logístico.	Los entrevistados coincidieron que no se tienen las adecuadas herramie	No existe divergencias entre los entrevistado.	Según las respuestas de los encuestados, se menciona que aún no se obtienen las

	para una correcta perenniza ción de material probatorio por parte del fiscal contra el delito informátic o contra el patrimoni o, en la modalida d de fraude informátic o; y contra la fe pública en la modalida d de suplantaci ón de identidad ?	de peritajes del Ministerio Publico.	se llega a alterar la evidenci a.	policías y personas encargad as de la investigac ión filtren el material obtenido,	tas potenciale s y actualizad as.	la PNP tener mayor comprom iso con su colabora ción con el fiscal.	el personal fiscal y policial necesita más formación en el delito informátic o, pero la elevada carga no lo hace posible.	Policial y la Fiscalía Especializ ada de Ciberdelin cuencia.		ntas y colaborac ión policial para la perennaci ón de material probatori o.		adecuada s herramien tas para la perenniza ción y la PNP no participa de manera comprom etida, lo que genera una investigac ión deficiente en los delitos informátic os, perjudican do la perenniza ción del material probatorio .
	¿Conside ra necesaria la perenniza ción de datos digitales, al existir la posibilida	Justament e esa es la finalidad de la perenniza ción de los digitales, utilizando para ello,	Lo consider o necesari a, sin embargo , se debe conocer de manera adecuad	Si, es necesario la perenniza ción de datos digitales, las mismas que deberían	Dada las caracterís ticas de las evidencia s, estas deben efectuars e por un perito	Se consider a que sea necesari o, para estos actos solo se podrían realizar	SI es necesario , deben ser ejecutada s por profesion ales especialis tas utilizando	Es necesario conservar y perennizar los datos digitales o prueba digital ya que dada a su	Sí, por la propia naturalez a de la prueba digital, ello debe ser procesad a de	Todos los entrevista dos coincidier on que es necesaria la perenniza ción de datos digitales.	No existe divergenci as entre los entrevista do.	Se concuerd a que, si es necesario, ya que la evidencia digital es todo registro informátic

	d que se alteren, clonen, modifiquen o borren los datos almacenados en fuentes digitales, si fuera así determine si estos actos lo pueden realizar cualquier persona? Explique	las herramientas como el código Hash, entre otros.	a a que TIC esta más accediendo, debiendo ser un profesional capacitado para ello.	ser realizados por profesionales especialistas capacitados para tal situación.	informático.	personas que sean especialistas, peritos a que tenga conocimientos solo en ello.	las herramientas correspondientes para el caso.	naturaleza puede ser manipulado, borrado o suprimido dentro de un proceso penal la perenniza ción tiene que ser realizada por un agente de la ley para que tenga validez legal.	forma oportuna.			o almacenado en un dispositivo informático con la finalidad de tener material probatorio para una investigación. Asimismo, concuerdan que los actos de perenniza ción deben ser realizados por un especialista en la materia.
	¿En la perenniza ción de las evidencias digitales en los delitos informáticos de fraude informático y suplantación de	Si, porque lo que se efectúa en la conservación, lo cual será emitida previa resolución judicial que los autorice, de igual modo el	Se considera correcto garantizar la privacidad de las partes, por lo que se debe manejar los procesos	Sí, toda vez que las evidencias obtenidas de manera digital son reservadas y de conocimientos únicamente de las	SI, toda la información obtenida en el desarrollo de una investigación tiene el carácter de reservarlo.	No exactamente, ya que no se mide en si el contenido de las evidencias digitales, ya que normalmente se busca	Sí, se garantiza el derecho a la privacidad, pero debe ser ejecutado de manera correspondiente para la obtención	Sí, conforme lo estipula la ley de Protección de datos es una exigencia legal. Además, la intimidad es un derecho	Considero que sí, porque es una sola preservación para obtención judicial a futuro, la intimidad no se ve afectada el solo preservar informaci	La mayoría de entrevistados indicaron que en la perenniza ción de evidencias digitales si se garantiza el derecho a	Solo uno de los entrevistados, señala que no exactamente se garantiza el derecho a la privacidad, puesto que no se	Se interpreta que, si se garantiza el derecho a la privacidad e intimidad porque la evidencia digital es un registro

	identidad se garantiza el derecho a la privacidad e intimidad? ¿Por qué?	juez evalúa porque se ven afectados los derechos fundamentales.	adecuados para la obtención de información, salvaguardando la vida privada no competente al caso concreto.	partes del proceso.		identificar a los responsables de dichos delitos, pero no se enfocan en los derechos que se evidencian.	de datos, sin perjudicar los derechos reservados.	fundamental.	ón, su gestión es mínima al fin del proceso.	la intimidad y privacidad.	enfocan en los derechos que se evidencian.	de información guardada para que sea utilizada como una prueba en el proceso judicial, donde el juez evalúa la originalidad de la evidencia digital

Anexo 04: Solicitud de validación de instrumentos

Certificado de validación de Instrumentos

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: Dr. VILDOSO CABRERA Erick Daniel

1.2. Cargo e institución donde labora: Docente de la Universidad César Vallejo

1.3. Nombre del instrumento motivo de evaluación: Guía de Entrevista

1.4. Autor del instrumento: Hernández Ayala, Nancy y Patricio Rojas, Alejandro Efraín

I. ASPECTO DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MÍNIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. Claridad	Esta formulada con lenguaje comprensible												X	
2. Objetividad	Esta adecuado a las leyes y principios científicos												X	
3. Actualidad	Esta adecuado a los objetivosy a las necesidades reales de la investigación												X	
4. Organización	Existe una organización lógica												X	
5. Suficiencia	Toma en cuenta los aspectos metodológicos esenciales												X	
6. Intencionalidad	Esta adecuado para valorar las variables de la hipótesis												X	
7. Consistencia	Se respalda en fundamentos técnicos y/o científicos												X	
8. Coherencia	Existe coherencia entre los problemas, objetivos, hipótesis, variables e indicadores												X	
9. Metodología	La estrategia responde una metodología y diseño aplicados para lograr probar las hipótesis												X	
10. Pertinencia	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al método científico												X	

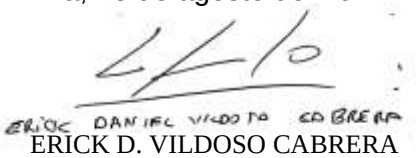
II. Opinion de aplicabilidad

a. El instrumento cumple con los requisitos para su aplicación. — X

b. El instrumento no cumple con los requisitos para su aplicación.

III. Promedio de valoración — 95%

Lima, 18 de agosto del 2021



ERICK D. VILDOSO CABRERA
DNI. N°09949028- Telf. 999698841

Certificado de validación de Instrumentos

VALIDACIÓN DE INSTRUMENTO

II. DATOS GENERALES

1.1. Apellidos y Nombres: Mgtr. Curi Urbina Ignacio

1.2. Cargo e institución donde labora: Docente de la Universidad César Vallejo

1.3. Nombre del instrumento motivo de evaluación: Guía de Entrevista

1.4. Autor del instrumento: Nancy Hernández Ayala y Alejandro Efraín Patricio Rojas

IV. ASPECTO DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MÍNIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. Claridad	Esta formulada con lenguaje comprensible												X	
2. Objetividad	Esta adecuado a las leyes y principios científicos												X	
3. Actualidad	Esta adecuado a los objetivosy a las necesidades reales de la investigación												X	
4. Organización	Existe una organización lógica												X	
5. Suficiencia	Toma en cuenta los aspectos metodológicos esenciales												X	
6. Intencionalidad	Esta adecuado para valorar las variables de la hipótesis												X	
7. Consistencia	Se respalda en fundamentos técnicos y/o científicos												X	
8. Coherencia	Existe coherencia entre losproblemas, objetivos, hipótesis, variables e indicadores												X	
9. Metodología	La estrategia responde una metodología y diseño aplicados para lograr probar las hipótesis												X	
10. Pertinencia	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al método científico												X	

V. Opinion de aplicabilidad

a. El instrumento cumple con los requisitos para su aplicación. X

b. El instrumento no cumple con los requisitos para su aplicación.

VI. Promedio de valoración 95%

Lima, 18 de agosto del 2021

IGNACIO CURI URBINA
DNI. N° 23865997 - Telf. 975618556

Certificado de validación de Instrumentos

VALIDACIÓN DE INSTRUMENTO

III. DATOS GENERALES

1.1. Apellidos y Nombres: Mgtr. Namuche Cruzado Clara Isabel

1.2. Cargo e institución donde labora: Docente de la Universidad César Vallejo

1.3. Nombre del instrumento motivo de evaluación: Guía de entrevista

1.4. Autor del instrumento: Hernández Ayala Nancy y Patricio Rojas Alejandro Efraín

VII. ASPECTO DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MÍNIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. Claridad	Esta formulada con lenguaje comprensible											X		
2. Objetividad	Esta adecuado a las leyes y principios científicos											X		
3. Actualidad	Esta adecuado a los objetivosy a las necesidades reales de la investigación											X		
4. Organización	Existe una organización lógica											X		
5. Suficiencia	Toma en cuenta los aspectos metodológicos esenciales											X		
6. Intencionalidad	Esta adecuado para valorar las variables de la hipótesis											X		
7. Consistencia	Se respalda en fundamentos técnicos y/o científicos											X		
8. Coherencia	Existe coherencia entre losproblemas, objetivos, hipótesis, variables e indicadores											X		
9. Metodología	La estrategia responde una metodología y diseño aplicados para lograr probar las hipótesis											X		
10. Pertinencia	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al método científico											X		

VIII. Opinion de aplicabilidad

a. El instrumento cumple con los requisitos para su aplicación. — X

b. El instrumento no cumple con los requisitos para su aplicación.

IX. Promedio de valoración — 90%

Lima, 18 de agosto del 2021

CLARA I. NAMUCHE CRUZADO
DNI. N° 0858 0729 - Telf. 0858 0129

Anexo 05: Guía de entrevista

DATOS PERSONALES DEL ENTREVISTADO

- NOMBRE COMPLETO:

- LUGAR DE TRABAJO:

- FUNCIÓN QUE DESEMPEÑA:

- FECHA DE ENTREVISTA:

TÍTULO: ENCUESTA DE LA ACTUACIÓN FISCAL EN LA OBTENCIÓN DE PRUEBAS DIGITALES EN LA FISCALÍA CORPORATIVA ESPECIALIZADA EN CIBERDELINCUENCIA DE LIMA – CENTRO

Objetivo General: Analizar la afectación de la actuación fiscal en la obtención de pruebas digitales en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿En su país ofrecen programas de capacitación en Ciberdelincuencia a la Policía Nacional, Ministerio Público y Órganos de Justicia en general?

……
……
……

2- ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos?

……
……
……

3- ¿Qué opina sobre la creación de las Fiscalías Especializadas en Ciberdelincuencia en el Perú, considera que se han visto cambios significativos en la actuación fiscal en la lucha contra los delitos informáticos?

……
……
……

4- ¿Considera usted que la legislación sobre delitos informáticos en el Perú es eficiente para la obtención y perennización de material probatorio? ¿Por qué?

……
……
……

5- ¿Considera usted que la obtención y perennización de evidencias digitales requieren de una adecuada especialización? ¿Por qué?

……
……
……

6- ¿Considera usted que el valor probatorio de las evidencias digitales es determinante para acreditar la responsabilidad por delitos informáticos de fraude informático y suplantación de identidad? ¿Por qué?

……
……
……

Objetivo Especifico 1: Determinar como la *obtención de pruebas digitales influye en el delito de suplantación de identidad y fraude informático* en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro

1- ¿La legislación de su país influye que los órganos de justicia permitan a las autoridades investigadoras (Fiscal) la obtención de medios de prueba mediante el uso de medidas limitativas de derecho en los delitos: contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

……
……
……

2- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta obtención de material probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático y contra la fe pública, en la modalidad de suplantación de identidad?

……
……
……

3- ¿La legislación de su país obliga a una empresa y/o proveedor de servicios, revelar información personal – privada (por ejemplo, datos de una cuenta, titular de una línea telefónica, información de movimiento de una cuenta bancaria, celda de ubicación de línea telefónica, la identidad de sus suscriptores, etc.)?

……
……
……

Objetivo Especifico 2: Establecer como *la perennización de las pruebas digitales incide en el delito de suplantación de identidad y fraude informático* en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta perennización de material probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

……
……
……

2- ¿Considera necesaria la perennización de datos digitales, al existir la posibilidad que se alteren, clonen, modifiquen o borren los datos almacenados en fuentes digitales, si fuera así determine si estos actos lo pueden realizar cualquier persona? Explique.

……
……
……

3- ¿En la perennización de las evidencias digitales en los delitos informáticos de fraude informático y suplantación de identidad se garantiza el derecho a la privacidad e intimidad? ¿Por qué?

……
……
……

Anexo 06: Instrumentos de validación de expertos

ESCUELA DE POSTGRADO

CARTA DE PRESENTACIÓN

Señor: Dr. Erick Daniel Vildoso Cabrera

Presente
Asunto: VALIDACIÓN DE INSTRUMENTO A TRAVÉS DE JUICIO DE EXPERTO.

Nos es muy grato comunicarme con usted para expresarle nuestros saludos y así mismo, hacer de su conocimiento que, siendo estudiantes de la Facultad de Derecho y Humanidades y Escuela de Derecho de la Universidad Cesar Vallejo, en la Filial Callao, promoción 2021-II, requerimos validar el instrumento con el cual recogeremos la información necesaria para poder desarrollar nuestra investigación y con la cual optaremos el grado de Abogado.

El título nombre de nuestra investigación es: La obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro 2021, y siendo imprescindible contar con la aprobación de docentes especializados en la materia, a efectos de poder aplicar el instrumento en mención, hemos considerado conveniente recurrir a usted, ante su connotada experiencia en temas de investigación jurídica.

El expediente de validación, que le hago llegar contiene:

- Carta de presentación.
- Matriz de Categorización.
- Guía de entrevista
- Certificado de validez de contenido de los instrumentos.

Expresándole nuestros sentimientos de respeto y consideración nos despedimos de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente,

Hernández Ayala Nancy
DNI N°46880163

Patricio Rojas Alejandro Efraín
DNI N° 73053403

ESCUELA DE POSTGRADO

CARTA DE PRESENTACIÓN

Señor: Mgtr. Curi Urbina Ignacio.

Presente
Asunto: VALIDACIÓN DE INSTRUMENTO A TRAVÉS DE JUICIO DE EXPERTO.

Nos es muy grato comunicarme con usted para expresarle nuestros saludos y así mismo, hacer de su conocimiento que, siendo estudiantes de la Facultad de Derecho y Humanidades y Escuela de Derecho de la Universidad Cesar Vallejo, en la Filial Callao, promoción 2021-II, requerimos validar el instrumento con el cual recogeremos la información necesaria para poder desarrollar nuestra investigación y con la cual optaremos el grado de Abogado.

El título nombre de nuestra investigación es: La obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro 2021 y siendo imprescindible contar con la aprobación de docentes especializados en la materia, a efectos de poder aplicar el instrumento en mención, hemos considerado conveniente recurrir a usted, ante su connotada experiencia en temas de investigación jurídica.

El expediente de validación, que le hago llegar contiene:

- Carta de presentación.
- Matriz de Categorización.
- Guía de entrevista
- Certificado de validez de contenido de los instrumentos.

Expresándole nuestros sentimientos de respeto y consideración nos despedimos de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente,

Hernández Ayala Nancy
DNI N° 46880163

Patricio Rojas Alejandro Efraín
DNI N° 73053403

ESCUELA DE POSTGRADO

CARTA DE PRESENTACIÓN

Señor(a): Mgtr. Namuche Cruzado Clara Isabel

Presente

Asunto: VALIDACIÓN DE INSTRUMENTO A TRAVÉS DE JUICIO DE EXPERTO.

Nos es muy grato comunicarme con usted para expresarle nuestros saludos y así mismo, hacer de su conocimiento que, siendo estudiantes de la Facultad de Derecho y Humanidades y Escuela de Derecho de la Universidad Cesar Vallejo, en la Filial Callao, promoción 2021-II, requerimos validar el instrumento con el cual recogeremos la información necesaria para poder desarrollar nuestra investigación y con la cual optaremos el grado de Abogado.

El título nombre de nuestra investigación es: La obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro 2021 y siendo imprescindible contar con la aprobación de docentes especializados en la materia, a efectos de poder aplicar el instrumento en mención, hemos considerado conveniente recurrir a usted, ante su connotada experiencia en temas de investigación jurídica.

El expediente de validación, que le hago llegar contiene:

- Carta de presentación.
- Matriz de Categorización.
- Guía de entrevista
- Certificado de validez de contenido de los instrumentos.

Expresándole nuestros sentimientos de respeto y consideración nos despedimos de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente,

Hernández Ayala Nancy
DNI N°46880163

Patricio Rojas Alejandro Efraín
DNI N° 73053403

Anexo 07: Consentimiento informado de los entrevistados

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CARTA DE PRESENTACIÓN

Señor(a): Marilyn Rocío Narváez Morán

Presente

Nos es muy grato comunicarme con usted para expresarle nuestros saludos y así mismo, hacer de su conocimiento que, nos encontramos realizando una investigación que lleva por título: "La obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro 2021."

La importancia de vuestra participación en este estudio proporcionará datos útiles con fines académicos.

Sin otro particular, expresamos nuestro sentimiento de respeto y consideración, no sin antes agradecerle por la atención.

Atentamente,

Hernández Ayala Nancy
DNI N°46880163

Patricio Rojas Alejandro Efraín
DNI N° 73053403

ESCUELA DE POSTGRADO

CARTA DE PRESENTACIÓN

Señor(a): Kimberly Madueño Oscorima

Presente

Nos es muy grato comunicarme con usted para expresarle nuestros saludos y así mismo, hacer de su conocimiento que, nos encontramos realizando una investigación que lleva por título: "La obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro 2021."

La importancia de vuestra participación en este estudio proporcionará datos útiles con fines académicos.

Sin otro particular, expresamos nuestro sentimiento de respeto y consideración, no sin antes agradecerle por la atención.

Atentamente,

Hernández Ayala Nancy
DNI N°46880163

Patricio Rojas Alejandro Efraín
DNI N° 73053403

ESCUELA DE POSTGRADO

CARTA DE PRESENTACIÓN

Señor(a): Jhonatan Cachique Abundo

Presente

Nos es muy grato comunicarme con usted para expresarle nuestros saludos y así mismo, hacer de su conocimiento que, nos encontramos realizando una investigación que lleva por título: "La obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro 2021."

La importancia de vuestra participación en este estudio proporcionará datos útiles con fines académicos.

Sin otro particular, expresamos nuestro sentimiento de respeto y consideración, no sin antes agradecerle por la atención.

Atentamente,

Hernández Ayala Nancy
DNI N°46880163

Patricio Rojas Alejandro Efraín
DNI N° 73053403

ESCUELA DE POSTGRADO

CARTA DE PRESENTACIÓN

Señor(a): Jesús Pedro Ojeda Valdiviezo

Presente

Nos es muy grato comunicarme con usted para expresarle nuestros saludos y así mismo, hacer de su conocimiento que, nos encontramos realizando una investigación que lleva por título: "La obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro 2021."

La importancia de vuestra participación en este estudio proporcionará datos útiles con fines académicos.

Sin otro particular, expresamos nuestro sentimiento de respeto y consideración, no sin antes agradecerle por la atención.

Atentamente,

Hernández Ayala Nancy
DNI N°46880163

Patricio Rojas Alejandro Efraín
DNI N° 73053403

ESCUELA DE POSTGRADO

CARTA DE PRESENTACIÓN

Señor(a): Jessica Pamela Cajo Rodas

Presente

Nos es muy grato comunicarme con usted para expresarle nuestros saludos y así mismo, hacer de su conocimiento que, nos encontramos realizando una investigación que lleva por título: "La obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro 2021."

La importancia de vuestra participación en este estudio proporcionará datos útiles con fines académicos.

Sin otro particular, expresamos nuestro sentimiento de respeto y consideración, no sin antes agradecerle por la atención.

Atentamente,

Hernández Ayala Nancy
DNI N°46880163

Patricio Rojas Alejandro Efraín
DNI N° 73053403

ESCUELA DE POSTGRADO

CARTA DE PRESENTACIÓN

Señor(a): Angélica Lorena Pérez Ascencio

Presente

Nos es muy grato comunicarme con usted para expresarle nuestros saludos y así mismo, hacer de su conocimiento que, nos encontramos realizando una investigación que lleva por título: "La obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro 2021."

La importancia de vuestra participación en este estudio proporcionará datos útiles con fines académicos.

Sin otro particular, expresamos nuestro sentimiento de respeto y consideración, no sin antes agradecerle por la atención.

Atentamente,

Hernández Ayala Nancy
DNI N°46880163

Patricio Rojas Alejandro Efraín
DNI N° 73053403

ESCUELA DE POSTGRADO

CARTA DE PRESENTACIÓN

Señor(a): Mónica Rocío Vargas Carpio

Presente

Nos es muy grato comunicarme con usted para expresarle nuestros saludos y así mismo, hacer de su conocimiento que, nos encontramos realizando una investigación que lleva por título: "La obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro 2021."

La importancia de vuestra participación en este estudio proporcionará datos útiles con fines académicos.

Sin otro particular, expresamos nuestro sentimiento de respeto y consideración, no sin antes agradecerle por la atención.

Atentamente,

Hernández Ayala Nancy
DNI N°46880163

Patricio Rojas Alejandro Efraín
DNI N° 73053403

ESCUELA DE POSTGRADO

CARTA DE PRESENTACIÓN

Señor(a): Jonathan Portillo Vela

Presente

Nos es muy grato comunicarme con usted para expresarle nuestros saludos y así mismo, hacer de su conocimiento que, nos encontramos realizando una investigación que lleva por título: "La obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro 2021."

La importancia de vuestra participación en este estudio proporcionará datos útiles con fines académicos.

Sin otro particular, expresamos nuestro sentimiento de respeto y consideración, no sin antes agradecerle por la atención.

Atentamente,

Hernández Ayala Nancy
DNI N°46880163

Patricio Rojas Alejandro Efraín
DNI N° 73053403

Anexo 7: Evidencias – guías de entrevista

DATOS PERSONALES DEL ENTREVISTADO

- **NOMBRE COMPLETO:** Marilyn Rocio Narvaez Moran
- **LUGAR DE TRABAJO:** Fiscalia Corporativa en Ciberdelincuencia de Lima Centro
- **FUNCIÓN QUE DESEMPEÑA:** Fiscal Adjunto Provincial
- **FECHA DE ENTREVISTA:** 01-10-2021

TÍTULO: ENCUESTA DE LA ACTUACIÓN FISCAL EN LA OBTENCIÓN DE PRUEBAS DIGITALES EN LA FISCALÍA CORPORATIVA ESPECIALIZADA EN CIBERDELINCUENCIA DE LIMA – CENTRO

Objetivo General: Analizar la afectación de la actuación fiscal en la obtención de pruebas digitales en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿En su país ofrecen programas de capacitación en Ciberdelincuencia a la Policía Nacional, Ministerio Público y Órganos de Justicia en general?

Con la creación de las Fiscalías Especializadas en Ciberdelincuencia en el Distrito Fiscal de Lima, se han iniciado con las capacitaciones a los integrantes de estos despachos, pero no tengo conocimiento que se haya lo mismo con la Policía Nacional.

2- ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos?

Nuestra legislación no ha establecido una política estratégica para prevenir la comisión de un delito informático, únicamente se toma las recomendaciones realizadas por los entidades financieras y respecto a la sanción por estos delitos se toma la Ley N° 30096

3- ¿Qué opina sobre la creación de las Fiscalías Especializadas en Ciberdelincuencia en el Perú, considera que se han visto cambios significativos en la actuación fiscal en la lucha contra los delitos informáticos?

Teniendo en cuenta el incremento de denuncias por delitos informáticos se crearon estos despachos fiscales especializados, que teniendo un contexto...

por competencia material y procediendo de una estrategia de investigación adecuada, se lleva a cabo la investigación de manera eficiente

4- ¿Considera usted que la legislación sobre delitos informáticos en el Perú es eficiente para la obtención y perennización de material probatorio? ¿Por qué?

No, porque la ley Nº 30096 únicamente en su primera disposición complementaria final establece sobre la conservación de material probatorio, después no se tiene otra legislación específica respecto de ello.

5- ¿Considera usted que la obtención y perennización de evidencias digitales requieren de una adecuada especialización? ¿Por qué?

Si, porque a fin de que la evidencia digital tenga valor necesario para el juicio oral, esta debe ser recabada por el perito informático forense de la oficina de peritos.

6- ¿Considera usted que el valor probatorio de las evidencias digitales es determinante para acreditar la responsabilidad por delitos informáticos de fraude informático y suplantación de identidad? ¿Por qué?

En el caso específico que la evidencia digital sea el único medio probatorio para determinar que el imputado es el responsable de la comisión del ilícito penal, esta si es determinante.

Objetivo Especifico 1: Determinar como la *obtención de pruebas digitales influye en el delito de suplantación de identidad y fraude informático* en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro

1- ¿La legislación de su país influye que los órganos de justicia permitan a las autoridades investigadoras (Fiscal) la obtención de medios de prueba mediante el uso de medidas limitativas de derecho en los delitos: contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

Los datos personales en Perú están protegidos constitucionalmente y mediante ley especial N° 29733, sin embargo el persecutor del delito requiere la medida limitativa de estos derechos, cuando se presenten los presupuestos establecidos en la norma procesal para ello.

2- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta obtención de material probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático y contra la fe pública, en la modalidad de suplantación de identidad?

Que el Ministerio Público por el poco presupuesto no tiene el suficiente material logístico necesario y la Fiscalía Especializada en Ciberdelincuencia es esta recientemente creada, carece de estos y además es necesario contar con suficiente personal técnico para la ejecución de la parte técnica en estos delitos

3- ¿La legislación de su país obliga a una empresa y/o proveedor de servicios, revelar información personal – privada (por ejemplo, datos de una cuenta, titular de una línea telefónica, información de movimiento de una cuenta bancaria, celda de ubicación de línea telefónica, la identidad de sus suscriptores, etc.)?

No la obliga, para el órgano jurisdiccional si ordena el otorgamiento de esta información, una vez se a efectuado un requerimiento fundamentado por parte del Ministerio Público.

Objetivo Especifico 2: Establecer como *la perennización de las pruebas digitales incide en el delito de suplantación de identidad y fraude informático* en la Fiscalia Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta perennización de material

probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

En cuanto a perennización únicamente se cuenta con los peritos de la Oficina de Peritajes del Ministerio Público

2- ¿Considera necesaria la perennización de datos digitales, al existir la posibilidad que se alteren, clonen, modifiquen o borren los datos almacenados en fuentes digitales, si fuera así determine si estos actos lo pueden realizar cualquier persona? Explique.

Si, debido a la volatilidad de los mismos

3- ¿En la perennización de las evidencias digitales en los delitos informáticos de fraude informático y suplantación de identidad se garantiza el derecho a la privacidad e intimidad? ¿Por qué?

MARILYN ROCIO NARVAEZ MORAN
Fiscal Adjunto Provincial
2° Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

DATOS PERSONALES DEL ENTREVISTADO

- **NOMBRE COMPLETO:** Kimberly Dakini Madueño Oscorima
- **LUGAR DE TRABAJO:** Ministerio Público
- **FUNCIÓN QUE DESEMPEÑA:** Asistente Administrativa (Sist. Fiscal)
- **FECHA DE ENTREVISTA:** 29 de setiembre de 2021

TÍTULO: ENCUESTA DE LA ACTUACIÓN FISCAL EN LA OBTENCIÓN DE PRUEBAS DIGITALES EN LA FISCALÍA CORPORATIVA ESPECIALIZADA EN CIBERDELINCUENCIA DE LIMA – CENTRO

Objetivo General: Analizar la afectación de la actuación fiscal en la obtención de pruebas digitales en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿En su país ofrecen programas de capacitación en Ciberdelincuencia a la Policía Nacional, Ministerio Público y Órganos de Justicia en general?

Sí, periodicamente; y por iniciativa de los Organismos Internacionales a los que nos encontramos adscritos.

2- ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos?

No, al ser delitos relativamente nuevos, y complejos por el detalle de su ejecución, siguen teniendo grandes barreras en su prevención.

3- ¿Qué opina sobre la creación de las Fiscalías Especializadas en Ciberdelincuencia en el Perú, considera que se han visto cambios significativos en la actuación fiscal en la lucha contra los delitos informáticos?

Considero un gran avance en el sistema de justicia al crear las FCEC, pues resulta de mucha importan

a individualizar los delitos, más aun complejos.....
.....

4- ¿Considera usted que la legislación sobre delitos informáticos en el Perú es eficiente para la obtención y perennización de material probatorio? ¿Por qué?

Considero que no se encuentra armonizada con la realidad y las leyes internacionales del país, puesto que se debe tener cuidado con los datos a los cuales se quiere y necesita acceder, sin vulnerar otra.

5- ¿Considera usted que la obtención y perennización de evidencias digitales requieren de una adecuada especialización? ¿Por qué?

Considero que sí, puesto que los datos a los cuales se necesitan acceder son de calidad personalísima y se podría vulnerar otros derechos fundamentales.

6- ¿Considera usted que el valor probatorio de las evidencias digitales es determinante para acreditar la responsabilidad por delitos informáticos de fraude informático y suplantación de identidad? ¿Por qué?

Sí, puesto que al ser incorporados de manera correcta, se podrá tener claridad de del responsable. Conllevando a un adecuado proceso con carácter garantista.

Objetivo Específico 1: Determinar como la *obtención de pruebas digitales influye en el delito de suplantación de identidad y fraude informático* en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro

1- ¿La legislación de su país influye que los órganos de justicia permitan a las autoridades investigadoras (Fiscal) la obtención de medios de prueba mediante el uso de medidas limitativas de derecho en los delitos: contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

Sí, una vez iniciada la investigación, y esta se considere necesario, se formula las medidas restrictivas de derecho.

2- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta obtención de material probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático y contra la fe pública, en la modalidad de suplantación de identidad?

La considero escasa, aun no se tiene un amplio manejo de la adecuada recolección de evidencia.

3- ¿La legislación de su país obliga a una empresa y/o proveedor de servicios, revelar información personal – privada (por ejemplo, datos de una cuenta, titular de una línea telefónica, información de movimiento de una cuenta bancaria, celda de ubicación de línea telefónica, la identidad de sus suscriptores, etc.)?

Sólo si en el caso concreto existe la autorización expresa de la/el titular de la cuenta, de lo contrario es denegada por ser confidencial.

Objetivo Especifico 2: Establecer como *la perennización de las pruebas digitales incide en el delito de suplantación de identidad y fraude informático* en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta perennización de material

probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

De igual forma, la considero escasa, no se tiene un buen manejo de ello y se llega a alterar la evidencia

2- ¿Considera necesaria la perennización de datos digitales, al existir la posibilidad que se alteren, clonen, modifiquen o borren los datos almacenados en fuentes digitales, si fuera así determine si estos actos lo pueden realizar cualquier persona? Explique.

La considero necesaria, sin embargo se debe conocer de manera adecuada a que TIC estamos accediendo, debiendo ser un profesional capacitado para ello.

3- ¿En la perennización de las evidencias digitales en los delitos informáticos de fraude informático y suplantación de identidad se garantiza el derecho a la privacidad e intimidad? ¿Por qué?

Se considera correcto garantizar la privacidad de las partes; por lo que se debe manejar los procesos adecuados para la obtención de información, salvaguardando la vida privada no competente al caso concreto.

KIMBERLY [illegible] MADUEÑO OSCORIMA
Asistente Administrativo
2° Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

DATOS PERSONALES DEL ENTREVISTADO

- **NOMBRE COMPLETO:** Jhonatan Cachique Abundo
- **LUGAR DE TRABAJO:** Fiscalía Especializada en Ciberdelincuencia
- **FUNCIÓN QUE DESEMPEÑA:** Asistente en Función Fiscal
- **FECHA DE ENTREVISTA:** 01/10/2021

TÍTULO: ENCUESTA DE LA ACTUACIÓN FISCAL EN LA OBTENCIÓN DE PRUEBAS DIGITALES EN LA FISCALÍA CORPORATIVA ESPECIALIZADA EN CIBERDELINCUENCIA DE LIMA – CENTRO

Objetivo General: Analizar la afectación de la actuación fiscal en la obtención de pruebas digitales en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿En su país ofrecen programas de capacitación en Ciberdelincuencia a la Policía Nacional, Ministerio Público y Órganos de Justicia en general?

En el Perú si ofrecen programas de capacitación a las instituciones antes referidas, pero mas q capacitación se debería enseñar estrategias para la resolver la problemática de manera mas certera.

2- ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos?

No, toda vez que muchas las instituciones encargadas de prevenir y sancionar el delito informático no unifican criterios ya que muchas veces ante un mismo caso utilizan criterios distintos.

3- ¿Qué opina sobre la creación de las Fiscalías Especializadas en Ciberdelincuencia en el Perú, considera que se han visto cambios significativos en la actuación fiscal en la lucha contra los delitos informáticos?

Desde mi punto de vista la fiscalía Especializada en Ciberdelincuencia tiene un rol muy importante, ya que ayuda significativamente a que

no siga creciendo de manera acelerada este tipo de delito.....
.....

4- ¿Considera usted que la legislación sobre delitos informáticos en el Perú es eficiente para la obtención y perennización de material probatorio? ¿Por qué?

NO, ya que no se cuenta con especialistas en esta materia, por la misma razón que es una materia nueva para muchos de aquellos que imparten justicia.....
.....

5- ¿Considera usted que la obtención y perennización de evidencias digitales requieren de una adecuada especialización? ¿Por qué?

Sí, ya que para poder obtener resultados satisfactorios es necesario tener especialistas en delitos de ciberdelincuencia, ya que su saber será más capaz y minucioso.....
.....

6- ¿Considera usted que el valor probatorio de las evidencias digitales es determinante para acreditar la responsabilidad por delitos informáticos de fraude informático y suplantación de identidad? ¿Por qué?

NO, ya que para acreditar tal responsabilidad se requiere conocer y valorar otros medios de prueba.
.....
.....

Objetivo Especifico 1: Determinar como la *obtención de pruebas digitales influye en el delito de suplantación de identidad y fraude informático* en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro

1- ¿La legislación de su país influye que los órganos de justicia permitan a las autoridades investigadoras (Fiscal) la obtención de medios de prueba mediante el uso de medidas limitativas de derecho en los delitos: contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

Si, ya que muchos veces hay derechos que favorecen a la persona que ha cometido un delito como lo señalado, comprendiendo así el actuar inmediato de los fiscales.

2- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta obtención de material probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático y contra la fe pública, en la modalidad de suplantación de identidad?

Si bien se puede tener el apoyo policial, pero aún faltan las herramientas necesarias para obtener resultados, tener datos y otros factores.

3- ¿La legislación de su país obliga a una empresa y/o proveedor de servicios, revelar información personal – privada (por ejemplo, datos de una cuenta, titular de una línea telefónica, información de movimiento de una cuenta bancaria, celda de ubicación de línea telefónica, la identidad de sus suscriptores, etc.)?

No, ya que para obtener información personal - privada se requiere previa autorización del titular, salvo en casos excepcionales.

Objetivo Especifico 2: Establecer como *la perennización de las pruebas digitales incide en el delito de suplantación de identidad y fraude informático* en la Fiscalia Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta perennización de material

probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

No, ya que muchas las veces de estas herramientas hacen que las pruebas policiales y personas encargadas de la investigación alteren el material obtenido.

2- ¿Considera necesaria la perennización de datos digitales, al existir la posibilidad que se alteren, clonen, modifiquen o borren los datos almacenados en fuentes digitales, si fuera así determine si estos actos lo pueden realizar cualquier persona? Explique.

Sí es necesaria la perennización de datos digitales, las mismas que deberían ser realizadas por profesionales especialistas capacitados para tal situación.

3- ¿En la perennización de las evidencias digitales en los delitos informáticos de fraude informático y suplantación de identidad se garantiza el derecho a la privacidad e intimidad? ¿Por qué?

Sí, toda vez que las evidencias obtenidas de manera digital son resguardas y documentadas de las partes del proceso.

Jhonatan Cachique Abundo
Asistente en Función Fiscal
1° Despacho Provincial de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro

DATOS PERSONALES DEL ENTREVISTADO

- **NOMBRE COMPLETO:** Jesús Pedro Ojeda Valdivieso
- **LUGAR DE TRABAJO:** Ministerio Público
- **FUNCIÓN QUE DESEMPEÑA:** Fiscal Adjunto Provincial
- **FECHA DE ENTREVISTA:** 30 Sep 2021

TÍTULO: ENCUESTA DE LA ACTUACIÓN FISCAL EN LA OBTENCIÓN DE PRUEBAS DIGITALES EN LA FISCALÍA CORPORATIVA ESPECIALIZADA EN CIBERDELINCUENCIA DE LIMA – CENTRO

Objetivo General: Analizar la afectación de la actuación fiscal en la obtención de pruebas digitales en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿En su país ofrecen programas de capacitación en Ciberdelincuencia a la Policía Nacional, Ministerio Público y Órganos de Justicia en general?

Pese a que la ley de delitos informáticos N° 30096 fue publicada en el año 2013, aún es insipiente el conocimiento que puede tener la policía, el ministerio público o el poder judicial respecto a los ciber delitos, no obstante se están apreciando cambios con la creación de una fiscalía especializada en la investigación de estos delitos que en la actualidad son de gran frecuencia.

2- ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos?

En mi opinión al ser delitos que en su mayoría atentan contra el patrimonio, debería optarse por mecanismos alternativos de resolución de conflictos. Respecto a las políticas de prevención, son casi nulas, nuestro Estado es deficiente y reactivo, por lo que siempre tiende a endurecer las penas creyendo que esta medida atacará la incidencia delictiva sin embargo es evidente que esta no ha sido la solución.

3- ¿Qué opina sobre la creación de las Fiscalías Especializadas en Ciberdelincuencia en el Perú, considera que se han visto cambios significativos en la actuación fiscal en la lucha contra los delitos informáticos?

La creación de una fiscalía especializada es un gran avance, pero para hablar de cambios y resultados aún es muy pronto.

JESÚS PEDRO OJEDA VALDIVIEZO
Fiscal Adjunto Provincial
1° Despacho Provincial de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro

4- ¿Considera usted que la legislación sobre delitos informáticos en el Perú es eficiente para la obtención y perennización de material probatorio? ¿Por qué?

Si es eficiente ya que se cuenta con las medidas limitativas de derechos las que permiten recabar indicios evidencias de convicción.

5- ¿Considera usted que la obtención y perennización de evidencias digitales requieren de una adecuada especialización? ¿Por qué?

Es de vital importancia que las evidencias digitales encontradas sean conservadas y preservadas por un perito especialista, dado que estas evidencias se encuentran en entornos digitales, y por lo que su volatilidad requiere de un conocimiento especial además que estas evidencias deberán constituirse en material probatorio.

6- ¿Considera usted que el valor probatorio de las evidencias digitales es determinante para acreditar la responsabilidad por delitos informáticos de fraude informático y suplantación de identidad? ¿Por qué?

En relación que estas evidencias digitales se constituirán en material probatorio lo que resulta determinante para poder obtener la teoría del caso.

Objetivo Especifico 1: Determinar como la *obtención de pruebas digitales influye en el delito de suplantación de identidad y fraude informático* en la Fiscalia Corporativa Especializada en Ciberdelincuencia de Lima – Centro

1- ¿La legislación de su país influye que los órganos de justicia permitan a las autoridades investigadoras (Fiscal) la obtención de medios de prueba mediante el uso de medidas limitativas de derecho en los delitos: contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

JESUS PEDRO QUESQUEN VALDIVIEZO
Fiscal Adjunto Provincial
2° Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

El Código Procesal contempla las medidas limitativas correspondientes, las cuales deben estar debidamente fundamentadas para que el juez de investigación preparatoria decida fundadamente el requerimiento fiscal

2- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta obtención de material probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático y contra la fe pública, en la modalidad de suplantación de identidad?

No, ya que no se cuenta con peritos informáticos necesarios, ya que la competencia de la UFEC es nacional.

3- ¿La legislación de su país obliga a una empresa y/o proveedor de servicios, revelar información personal – privada (por ejemplo, datos de una cuenta, titular de una línea telefónica, información de movimiento de una cuenta bancaria, celda de ubicación de línea telefónica, la identidad de sus suscriptores, etc.)?

Se mediante el requerimiento del secreto de las comunicaciones el cual debe estar debidamente fundamentado.

Objetivo Especifico 2: Establecer como *la perennización de las pruebas digitales incide en el delito de suplantación de identidad y fraude informático* en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta perennización de material

probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

Dada la especialidad y volatilidad de la información esta requiere de un equipo mas amplio.

2- ¿Considera necesaria la perennización de datos digitales, al existir la posibilidad que se alteren, clonen, modifiquen o borren los datos almacenados en fuentes digitales, si fuera asi determine si estos actos lo pueden realizar cualquier persona? Explique.

Dada las características de las evidencias, estas deben ser realizadas por un perito informático.

3- ¿En la perennización de las evidencias digitales en los delitos informáticos de fraude informático y suplantación de identidad se garantiza el derecho a la privacidad e intimidad? ¿Por qué?

No existe derecho absoluto, sin embargo la información obtenida en el desarrollo de una investigación tiene el carácter de reservado.

JESUS PEDRO QUEDA VALDIVIEZO
Fiscal Adjunto Provincial
Coordinador Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

DATOS PERSONALES DEL ENTREVISTADO

- **NOMBRE COMPLETO:** Jessica Pamela Cajo Rodas
- **LUGAR DE TRABAJO:** Ministerio Público - Fiscalía Especializada en Ciberdelincuencia
- **FUNCIÓN QUE DESEMPEÑA:** Asistente en Función Fiscal
- **FECHA DE ENTREVISTA:** 29-09-21

TÍTULO: ENCUESTA DE LA ACTUACIÓN FISCAL EN LA OBTENCIÓN DE PRUEBAS DIGITALES EN LA FISCALÍA CORPORATIVA ESPECIALIZADA EN CIBERDELINCUENCIA DE LIMA – CENTRO

Objetivo General: Analizar la afectación de la actuación fiscal en la obtención de pruebas digitales en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿En su país ofrecen programas de capacitación en Ciberdelincuencia a la Policía Nacional, Ministerio Público y Órganos de Justicia en general?

Con el paso del tiempo se están ofreciendo dichas capacitaciones, y eso se da en base al incremento de los delitos informáticos que sufren los ciudadanos.

2- ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos?

Para la prevención creo que no los hay, porque inclusive en las entidades bancarias no cuentan con suficientes medidas de seguridad; en cuanto a la sanción aún se trabaja en ello.

3- ¿Qué opina sobre la creación de las Fiscalías Especializadas en Ciberdelincuencia en el Perú, considera que se han visto cambios significativos en la actuación fiscal en la lucha contra los delitos informáticos?

Me parece muy importante su creación, ya que al ser especializado solo se enfoca en esos delitos cibernéticos,

JESSICA PAMELA CAJO RODAS
Asistente en Función Fiscal
1° Despacho Provincial de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro

asimismo la comisión han mejorado, aunque es un poco lento por... el apoyo suficiente de determinados establecimientos o entidades, ya que a ellos se le solicita información, pero demoran en contestar.

4- ¿Considera usted que la legislación sobre delitos informáticos en el Perú es eficiente para la obtención y perennización de material probatorio? ¿Por qué?

No es eficiente, ya que para ello se necesita una especialización constante, puesto que la tecnología va en progreso.

5- ¿Considera usted que la obtención y perennización de evidencias digitales requieren de una adecuada especialización? ¿Por qué?

Si, puesto que el uso de las TICS y con la globalización va en aumento; la tecnología va a un paso más allá y para ello la especialización cubre un papel muy importante

6- ¿Considera usted que el valor probatorio de las evidencias digitales es determinante para acreditar la responsabilidad por delitos informáticos de fraude informático y suplantación de identidad? ¿Por qué?

Claro que sí, porque las evidencias digitales también pueden ser materia de falsificación, y para ello se necesita acreditar su valor probatorio y su importancia en las investigaciones.

Objetivo Especifico 1: Determinar como la *obtención de pruebas digitales influye en el delito de suplantación de identidad y fraude informático* en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro

1- ¿La legislación de su país influye que los órganos de justicia permitan a las autoridades investigadoras (Fiscal) la obtención de medios de prueba mediante el uso de medidas limitativas de derecho en los delitos contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

JESSICA PAMELA CAJO RODAS
Asistente en Función Fiscal
2° Despacho Provincial de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro

Por supuesto, ya que dichas medidas limitativas son requeridas en su oportunidad bajo ciertos fundamentos y con el mismo/todo se logra contar con mayor información.

2- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta obtención de material probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático y contra la fe pública, en la modalidad de suplantación de identidad?

No, ya que hay diferencias y ciertos vacíos legales, aparte la policía no colabora inmediatamente con las diligencias que se le solicita, existe la falta de interés por estos tipos de delitos informáticos.

3- ¿La legislación de su país obliga a una empresa y/o proveedor de servicios, revelar información personal – privada (por ejemplo, datos de una cuenta, titular de una línea telefónica, información de movimiento de una cuenta bancaria, celda de ubicación de línea telefónica, la identidad de sus suscriptores, etc.)?

No exactamente, aunque hay limitaciones con los datos privados, ya que se busca proteger datos personales del usuario, pero para que ello sea requerido hay previa coordinación con el titular o con el poder judicial. (depende de lo que se solicite)

Objetivo Especifico 2: Establecer como *la perennización de las pruebas digitales incide en el delito de suplantación de identidad y fraude informático* en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta perennización de material

probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

No, aun nos falta mucho por aprender, por actualizarnos, así como por parte de la PNP tener mayor compromiso con su colaboración con el fiscal.

2- ¿Considera necesaria la perennización de datos digitales, al existir la posibilidad que se alteren, clonen, modifiquen o borren los datos almacenados en fuentes digitales, si fuera así determine si estos actos lo pueden realizar cualquier persona? Explique.

Si considero que sea necesario. Pero estos datos solo lo podrían realizar personas que sean especialistas, peritos o que tenga conocimiento sobre ello.

3- ¿En la perennización de las evidencias digitales en los delitos informáticos de fraude informático y suplantación de identidad se garantiza el derecho a la privacidad e intimidad? ¿Por qué?

No exactamente, ya que no se mide en si del contenido de las evidencias digitales, ya que normalmente se busca identificar a los responsables de dichos delitos, pero no se enfocan en los derechos que se vulneran.

JESSICA PAMELA CAJO RIVERA
Asistente en Función Fiscal
2° Despacho Provincial de la Fiscalía Corporativa

DATOS PERSONALES DEL ENTREVISTADO

- **NOMBRE COMPLETO:** Angelica Lorena Perez Asencio
- **LUGAR DE TRABAJO:** Ministerio Público - Fiscalía Corporativa Especializada en Ciberdelincuencia
- **FUNCIÓN QUE DESEMPEÑA:** Fiscal Adjunto Provincial
- **FECHA DE ENTREVISTA:** 01 de octubre del 2021.

TÍTULO: ENCUESTA DE LA ACTUACIÓN FISCAL EN LA OBTENCIÓN DE PRUEBAS DIGITALES EN LA FISCALÍA CORPORATIVA ESPECIALIZADA EN CIBERDELINCUENCIA DE LIMA – CENTRO

Objetivo General: Analizar la afectación de la actuación fiscal en la obtención de pruebas digitales en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿En su país ofrecen programas de capacitación en Ciberdelincuencia a la Policía Nacional, Ministerio Público y Órganos de Justicia en general?

Sí, la Unidad Ejecutora de Ciberdelincuencia del Ministerio Público capacita permanentemente.

2- ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos?

No.

3- ¿Qué opina sobre la creación de las Fiscalías Especializadas en Ciberdelincuencia en el Perú, considera que se han visto cambios significativos en la actuación fiscal en la lucha contra los delitos informáticos?

Sí, los delitos informáticos tienen una estrategia de investigación diferente a los delitos comunes.

Angelica Lorena Perez Asencio
Fiscal Adjunta Provincial

4- ¿Considera usted que la legislación sobre delitos informáticos en el Perú es eficiente para la obtención y perennización de material probatorio? ¿Por qué?

No

5- ¿Considera usted que la obtención y perennización de evidencias digitales requieren de una adecuada especialización? ¿Por qué?

Definitivamente, es necesario que tanto el personal fiscal, como administrativo se encuentren capacitados en la obtención y perennización de las evidencias, las mismas que deben ser recabadas con rapidez.

6- ¿Considera usted que el valor probatorio de las evidencias digitales es determinante para acreditar la responsabilidad por delitos informáticos de fraude informático y suplantación de identidad? ¿Por qué?

Sí, sobre todo en los delitos de suplantación de identidad, donde sus medios son las redes sociales, correo electrónico, y otros elementos de comunicación.

Objetivo Especifico 1: Determinar como la *obtención de pruebas digitales influye en el delito de suplantación de identidad y fraude informático* en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro

1- ¿La legislación de su país influye que los órganos de justicia permitan a las autoridades investigadoras (Fiscal) la obtención de medios de prueba mediante el uso de medidas limitativas de derecho en los delitos: contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

Angélica Lorena Pérez Asencio
Fiscal Adjunta Provincial
2° Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

2- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta obtención de material probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático y contra la fe pública, en la modalidad de suplantación de identidad?

Sí, además el Ministerio Público cuenta con la asistencia técnica del personal de la Unidad de Ciberdelincuencia de Lima y peritos.

3- ¿La legislación de su pais obliga a una empresa y/o proveedor de servicios, revelar información personal – privada (por ejemplo, datos de una cuenta, titular de una línea telefónica, información de movimiento de una cuenta bancaria, celda de ubicación de línea telefónica, la identidad de sus suscriptores, etc.)?

Sí, siempre que dicha solicitud sea requerida y acompañada a una Resolución Judicial. También puede ser solicitada acompañando la Carta de autorización de la parte agraviada.

Objetivo Especifico 2: Establecer como *la perennización de las pruebas digitales incide en el delito de suplantación de identidad y fraude informático* en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta perennización de material

Angélica Lorena Pérez Asencio
Fiscal Adjunta Provincial
3° Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

No, existen programas que por su costo no son de acceso libre, de igual forma, el personal fiscal y policial, no cuenta una formación en el rubro informático, para lo cual [illegible] cargo no lo hace posible.

2- ¿Considera necesaria la perennización de datos digitales, al existir la posibilidad que se alteren, clonen, modifiquen o borren los datos almacenados en fuentes digitales, si fuera así determine si estos actos lo pueden realizar cualquier persona? Explique.

Justamente, esa es la finalidad de la perennización de datos digitales, utilizando para ello, las herramientas como el código HASH, entre otros.

3- ¿En la perennización de las evidencias digitales en los delitos informáticos de fraude informático y suplantación de identidad se garantiza el derecho a la privacidad e intimidad? ¿Por qué?

Sí, porque lo que se efectúa es la conservación, la cual será [illegible] previa resolución judicial que lo autorice, de igual modo, el Juez evaluará porque no se vean afectados derechos fundamentales.

Angélica Lorena Pérez Asencio
Fiscal Adjunta Provincial
2° Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

DATOS PERSONALES DEL ENTREVISTADO

- **NOMBRE COMPLETO:** [illegible] Rocío Vargas [illegible]
- **LUGAR DE TRABAJO:** Ministerio Público
- **FUNCIÓN QUE DESEMPEÑA:** Fiscal Adjunta Provincial
- **FECHA DE ENTREVISTA:** 30 de septiembre de 2021

TÍTULO: ENCUESTA DE LA ACTUACIÓN FISCAL EN LA OBTENCIÓN DE PRUEBAS DIGITALES EN LA FISCALÍA CORPORATIVA ESPECIALIZADA EN CIBERDELINCUENCIA DE LIMA – CENTRO

Objetivo General: Analizar la afectación de la actuación fiscal en la obtención de pruebas digitales en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿En su país ofrecen programas de capacitación en Ciberdelincuencia a la Policía Nacional, Ministerio Público y Órganos de Justicia en general?

Actualmente los fiscales especializados en ciberdelincuencia vienen recibiendo capacitación de la Oficina de las Naciones Unidas contra la Droga y el Delito.

2- ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos?

La implementación de la ley Nº 30096 y su modificatoria por ley Nº 30171 es una forma de prevención. Sin embargo, requiere mejoras acordes con los cambios sociales y el desarrollo tecnológico.

3- ¿Qué opina sobre la creación de las Fiscalías Especializadas en Ciberdelincuencia en el Perú, considera que se han visto cambios significativos en la actuación fiscal en la lucha contra los delitos informáticos?

Sin duda existe un avance significativo en la lucha contra los delitos informáticos, la fiscalía especializada ha iniciado eficientemente

sus funciones, los cambios surgieron a un mediano plazo.

4- ¿Considera usted que la legislación sobre delitos informáticos en el Perú es eficiente para la obtención y perennización de material probatorio? ¿Por qué?

No, en la medida que solo regulan los aspectos típicos del delito, mas no el procedimiento para obtener la prueba.

5- ¿Considera usted que la obtención y perennización de evidencias digitales requieren de una adecuada especialización? ¿Por qué?

Sí, por la evidencia digital presenta determinadas características como la velocidad, volatilidad y fragilidad.

6- ¿Considera usted que el valor probatorio de las evidencias digitales es determinante para acreditar la responsabilidad por delitos informáticos de fraude informático y suplantación de identidad? ¿Por qué?

Sí, en la medida que sólo a través de la prueba, en cualquier tipo de proceso o procedimiento, se puede vincular la responsabilidad del sujeto activo.

Objetivo Especifico 1: Determinar como la *obtención de pruebas digitales influye en el delito de suplantación de identidad y fraude informático* en la Fiscalia Corporativa Especializada en Ciberdelincuencia de Lima – Centro

1- ¿La legislación de su país influye que los órganos de justicia permitan a las autoridades investigadoras (Fiscal) la obtención de medios de prueba mediante el uso de medidas limitativas de derecho en los delitos: contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

Sí, conforme lo precisa el artículo 202 en adelante del Código Procesal Penal.

2- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta obtención de material probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático y contra la fe pública, en la modalidad de suplantación de identidad?

Sí, contamos con una Policía especializada, la División de Investigación en Delitos de Alta Tecnología.

3- ¿La legislación de su país obliga a una empresa y/o proveedor de servicios, revelar información personal – privada (por ejemplo, datos de una cuenta, titular de una línea telefónica, información de movimiento de una cuenta bancaria, celda de ubicación de línea telefónica, la identidad de sus suscriptores, etc.)?

Sí, previa autorización judicial.

Objetivo Especifico 2: Establecer como *la perennización de las pruebas digitales incide en el delito de suplantación de identidad y fraude informático* en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta perennización de material

probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

No, ya que aún tanto la División Policial y la Fiscalía Especializada en Ciberdelincuencia

2- ¿Considera necesaria la perennización de datos digitales, al existir la posibilidad que se alteren, clonen, modifiquen o borren los datos almacenados en fuentes digitales, si fuera así determine si estos actos lo pueden realizar cualquier persona? Explique.

Es necesario remover y perennizar los datos digitales o prueba digital ya que dada su naturaleza puede ser manipulado, borrado o suplantado. Dentro de un proceso penal la perennización tiene que ser realizada por un agente de la ley para que tenga validez legal.

3- ¿En la perennización de las evidencias digitales en los delitos informáticos de fraude informático y suplantación de identidad se garantiza el derecho a la privacidad e intimidad? ¿Por qué?

Sí, conforme lo estipula la Ley de Protección de Datos es una obligación legal. Además la intimidad es un derecho fundamental tutelado.

MONICA ROCIO VARGAS CARPIO
Fiscal Adjunta Provincial
2° Despacho Provincial de la Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

DATOS PERSONALES DEL ENTREVISTADO

- **NOMBRE COMPLETO:** Jonathan Carlo Padilla Vela
- **LUGAR DE TRABAJO:** Ministerio Público
- **FUNCIÓN QUE DESEMPEÑA:** Fiscal Provincial
- **FECHA DE ENTREVISTA:** 30/01/23

TÍTULO: ENCUESTA DE LA ACTUACIÓN FISCAL EN LA OBTENCIÓN DE PRUEBAS DIGITALES EN LA FISCALÍA CORPORATIVA ESPECIALIZADA EN CIBERDELINCUENCIA DE LIMA – CENTRO

Objetivo General: Analizar la afectación de la actuación fiscal en la obtención de pruebas digitales en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿En su país ofrecen programas de capacitación en Ciberdelincuencia a la Policía Nacional, Ministerio Público y Órganos de Justicia en general?

En líneas generales la capacitación no es generalizada, si da solo o en su mayoría para los áreas especializadas

2- ¿Dentro de su consideración, cree Ud. que existen estrategias adecuadas para la prevención y sanción de los delitos informáticos?

Considero que no existen adecuados programas de difusión por parte del Estado para prevenir delitos informáticos, es el entorno existe una participación del sector privado, público y colectivo.

3- ¿Qué opina sobre la creación de las Fiscalías Especializadas en Ciberdelincuencia en el Perú, considera que se han visto cambios significativos en la actuación fiscal en la lucha contra los delitos informáticos?

Considero que es un avance importante para reconocer la importancia del delito y la necesidad de establecer especialización para la lucha del delito

4- ¿Considera usted que la legislación sobre delitos informáticos en el Perú es eficiente para la obtención y perennización de material probatorio? ¿Por qué?

Considero que existe ausencia de protocolos, de guías y de educación conjunta para el manejo de este material probatorio

5- ¿Considera usted que la obtención y perennización de evidencias digitales requieren de una adecuada especialización? ¿Por qué?

Si, porque es una prueba especializada q' requiere un mayor conocimiento y manejo de conceptos y procedimientos en cada caso

6- ¿Considera usted que el valor probatorio de las evidencias digitales es determinante para acreditar la responsabilidad por delitos informáticos de fraude informático y suplantación de identidad? ¿Por qué?

Si, estimo que su correcto manejo es importante para obtener pronunciamientos adecuados en informes sugeridos

Objetivo Especifico 1: Determinar como la *obtención de pruebas digitales influye en el delito de suplantación de identidad y fraude informático* en la Fiscalia Corporativa Especializada en Ciberdelincuencia de Lima – Centro

1- ¿La legislación de su país influye que los órganos de justicia permitan a las autoridades investigadoras (Fiscal) la obtención de medios de prueba mediante el uso de medidas limitativas de derecho en los delitos: contra el patrimonio, en la modalidad de fraude informático; y contra la fe pública en la modalidad de suplantación de identidad?

Estimo que si, existen herramientas que deben ser utilizadas e interpretadas a la luz de los nuevos avances

2- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta obtención de material probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de fraude informático y contra la fe pública, en la modalidad de suplantación de identidad?

Considero que no, el acceso a la información es limitado y existen barreras para su tratamiento o exposición

3- ¿La legislación de su país obliga a una empresa y/o proveedor de servicios, revelar información personal – privada (por ejemplo, datos de una cuenta, titular de una línea telefónica, información de movimiento de una cuenta bancaria, celda de ubicación de línea telefónica, la identidad de sus suscriptores, etc.)?

Si, con requerimiento de la SBS y de Osiptel, pero estimo q tiene deficiencias para su obtención automática y rápida

Objetivo Específico 2: Establecer como *la perennización de las pruebas digitales incide en el delito de suplantación de identidad y fraude informático* en la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima – Centro.

1- ¿Considera usted que se tienen las adecuadas herramientas y colaboración policial para una correcta perennización de material

probatorio por parte del fiscal contra el delito informático contra el patrimonio, en la modalidad de traude informático; y contra la fe pública en la modalidad de suplantación de identidad?

No, Considero que existen deficiencias en la capacitación y en el material logístico

2- ¿Considera necesaria la perennización de datos digitales, al existir la posibilidad que se alteren, clonen, modifiquen o borren los datos almacenados en fuentes digitales, si fuera así determine si estos actos lo pueden realizar cualquier persona? Explique.

Si, por la propia naturaleza de la prueba digital ella debe ser preservada de forma oportuna

3- ¿En la perennización de las evidencias digitales en los delitos informáticos de fraude informático y suplantación de identidad se garantiza el derecho a la privacidad e intimidad? ¿Por qué?

Considero que si, pues solo una preservación para obtención judicial a futuro, la intimidad no se ve afectada al solo preservar información y se ofrecerá en primera el fin del proceso

JONATHAN C. PORTILLO VELA
Fiscal Provincial (P)
2° Despacho Provincial de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro