UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTORES:

Martel Melgarejo, Joseph Alexander (ORCID: 0000-0002-0365-5729)

Quispe Vara, Diana Dolores (ORCID: 0000-0002-1371-4032)

ASESORES:

Mgtr. Palomino Gonzales, Lutgarda (ORCID: 0000-002-5948-341X)

Mtro. Guerra Campos, Jefferson Williams (ORCID: 0000-0003-0158-7248)

LINEA DE INVESTIGACIÓN:

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

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la Democracia, Liderazgo y Ciudadanía

LIMA – PERÚ

2022

Dedicatoria

Esta tesis es dedicada a nuestras familias, la cual fue nuestra inspiración y sustento para culminar satisfactoriamente nuestras carreras. Agradezco especialmente a Mathias, quien llego en un momento especial y nos motivó lograr esta meta.

Agradecimiento

Primeramente, damos gracias a Dios por permitirnos desarrollar nuestra tesis de manera profesional y exitosa, asimismo, nuestra gratitud con la Universidad Cesar Vallejo por habernos brindado los valores de los cuales nos inculcaron durante el transcurso de nuestra formación como profesionales.

Índice de contenido

Índice de tablas

Resumen

Esta presente tesis, tuvo como objetivo general determinar si la actuación de las entidades persecutoras de los delitos informáticos fueron las adecuadas durante pandemia por covid-19, en tal sentido se tomó antecedes nacionales e internacionales y dos teorías bases a fin proponer posibles soluciones al problema que es materia de investigación teniéndose en cuenta la experticia de los entrevistados, quienes laboran en el Ministerio Publico, División de Investigación de Delitos de Alta Tecnología (DIVINDAT) y una letrada independiente. Por otro lado, se destaca que la presente tesis es de enfoque cualitativo de tipo base, con diseño fenomenológico y de método inductivo, teniendo como herramienta de investigación para el procesamiento de análisis datos el programa ATLAS.ti 9. Finalmente, se evidencio en la tesis problemas como la falta de personal capacitado en ambos órganos, así también, la insuficiencia de herramientas digitales y tecnológicos para llevar a cabo una correcta investigación; y finalmente cursos, capacitación por parte del Gobierno Peruano a todo el personal, pues a raíz de la pandemia la Fiscalía Especializada en Ciberdelincuencia y la Divindat no se abastece ante la indagación de los delitos informáticos.

Palabras clave: Delitos Informáticos, DIVINDAT, Fiscalía Especializada, Covid-19, Herramientas Digitales, Herramientas Tecnológicos.

Abstract

The general objective of this thesis was to determine whether the actions of the entities prosecuting computer crimes were adequate during the covid-19 pandemic. In this sense, national and international antecedents and two basic theories were taken in order to propose possible solutions to the problem under investigation, taking into account the expertise of the interviewees, who work in the Public Ministry, High Technology Crimes Investigation Division (DIVINDAT) and an independent lawyer. On the other hand, it should be noted that the present thesis has a qualitative approach, with a phenomenological design and an inductive method, using ATLAS.ti 9 as a research tool for the processing of data analysis. Finally, the thesis evidenced problems such as the lack of trained personnel in both bodies, as well as the insufficiency of digital and technological tools to carry out a proper investigation; and finally courses, training by the Peruvian Government to all staff, because as a result of the pandemic the Specialized Prosecutor's Office on Cybercrime and Divindat is not supplied to the investigation of cybercrime.

Keywords: Computer Crimes, DIVINDAT, Specialized Prosecutor's Office, Covid-19, Digital Tools, Technological Tools.

I. INTRODUCCIÓN

El 15 de marzo del año 2020, el Estado Peruano declaró el estado de emergencia y aislamiento social obligatorio mediante el Decreto Supremo N° 044-2020-PCM, impidiendo así las labores económicas y administrativas del país, la cual genero limitaciones razonables y proporcionales de los derechos humanos, fundamentales e individuales como los derechos relativos a la libertad, entre otros, ocasionando disminución en la comisión de los delitos tradicionales como el robo agravado, lesiones, homicidios, etc., no obstante ello, incremento los delitos de la ciberdelincuencia en todas sus modalidades acarreando perjuicios económicos y sociales, teniendo como instrumento principal el uso de la redes sociales y el internet.

Por consiguiente, el aislamiento social obligo a la ciudadanía a adaptarse al teletrabajo, compras mediante plataformas web y/o reuniones virtuales permitiendo que se comentan hechos ilícitos configurados como ciberdelincuencia a través de uso de la tecnología vía redes sociales y del internet en su sentido más amplio; se evidencio la comisión de los ilícitos como el fraude informático, suplantaciones de páginas web, sabotajes informáticos, suplantación de identidad, transferencias de dinero y otros que fueron denunciados en algunos casos mediante los medios de comunicación, alarmando a la sociedad de los supuestos nuevos riesgos para las personas, así también, como para las entidades financieras y el propio Estado Peruano.

Empero a lo anterior, se entendió que los delitos informáticos estaban a la orden del día y las entidades persecutoras de estos tipos de delitos recibieron grandes cantidades de denuncias, pero, no recibieron ayuda económica por parte del Estado, dificultando posiblemente las investigaciones de estos actos ilícitos. En consecuencia, diversos medios sociales difundieron masivamente las falsificaciones de páginas web del estado, transferencias fraudulentas y las suplantaciones de identidad de las entidades bancarias y plataformas digitales. Ahora bien, observando la vía judicial se logró percibir que los delincuentes se valen de la impunidad ante la comisión de este tipo de delitos ya que muchas veces son cometidos en la red bajo el anonimato y la actuación de los fiscales revela un carecimiento de medios, personal y capacidad de actuar ante las modalidades de

los delitos informáticos perjudicando a las víctimas en el entendido de que la probabilidad que se recupere el bien extraído es muy poco probable.

Los especialistas del Observatorio Nacional de Política Criminal, (2020) señalaron que existe una relación de los delitos informáticos y las víctimas. Preciso además que tan solo en el año 2019 las denuncias netamente por fraude informáticos superaron los más de dos mil casos, tiempo antes de pandemia. No obstante, manifiesto que las principales víctimas de este tipo de delitos son personas que oscilan la edad de 30 a 44 años.

Los estudiosos de la revista digital Actualidad Penal, (2021) informaron que en el periodo de enero a abril del año 2021 la División de investigación de alta tecnología (DIVINDAT) ha recibido 1200 denuncias por delitos cibernéticos vinculadas estrechamente al fraude electrónico y la suplantación de identidad duplicando las cifras del año que antecede con un total 580 denuncias de las cuales a la fecha de la publicación del articulo solo 296 fueron atendidas.

No obstante, en el país de Ecuador en el año 2009 inició una etapa por ingesta de los delitos informáticos y a promediados del 2013, se dieron a conocer un total de 3,143 casos, es de precisar que este resultado solo versa el 20% pues se conocer que el 80% de las víctimas no reportan este tipo de incidencia, por lo que, ecuador se ubica en el tercer país seguido de México y Bolivia. La ONU señalo que en los países de Latinoamérica como Centro América carecen de cultura para denunciar (Saltos et al., 2021).

De modo que, como problema general se tiene por conveniente plantear lo siguiente: ¿La actuación de las entidades persecutoras de los delitos informáticos fueron las adecuadas durante pandemia por covid-19? Como problemas específicos se tuvo: (a) ¿los delitos informáticos incrementaron durante la pandemia por covid-19? (b) ¿Cuáles son las entidades persecutoras de los delitos informáticos creados por el Estado?

Como justificación práctica, se entiende la presente investigación es útil y pertinente pues se desea exponer que gran porcentaje de la población peruana ha sido víctima de los delitos informáticos en todas sus modalidades durante el Estado de emergencia por la covid-19.

Por justificación teórica de entiende que la misma permite realizar una innovación con el fin de establecer un balance en el problema que se investiga puesto que como resultado se obtuvo si la investigación resulta factible en otras investigaciones. Una investigación se justifica en la medida de la ampliación de las fronteras de la ciencia (Ñaupas et al., 2018).

En referencia a la justificación metodológica, esta referida a la exposición del uso o de las propuestas de métodos, técnicas y estrategias que puedan ayudar al conocimiento valido y confiable con el fin aportar a los investigadores con realidades problemáticas similares al presente trabajo de investigación. (Gallardo, 2017, p.33.)

En ese mismo sentido, como objetivo general se tuvo: Determinar si la actuación de las entidades persecutoras de los delitos informáticos fueron las adecuadas durante pandemia por covid-19, como objetivos específicos se tuvo: (a) Explicar porque los delitos informáticos incrementaron durante la pandemia por covid-19. (b) Identificar cuáles son las entidades persecutoras de los delitos informáticos creadas por el Estado.

Finalmente, resulta relevante hacer mención que la salud colectiva demanda cuidados, nuevas medidas y sacrificios, los cuales deben también incluir la preocupación por la incrementación de los delitos que deviene con el avance de la tecnología pues muchas veces estos delincuentes abusan de su conocimiento escudándose tras una pantalla.

II. MARCO TEÓRICO

En el presente apartado, se desarrollará los antecedentes nacionales e internacionales las cual son coetáneos al presente proyecto de investigación.

Zambrano (2021) tuvo como objetivo señalar si la utilidad de la Banca Móvil genero fraudes informáticos que afectaron la esfera patrimonial en la ciudad de Arequipa; Fue un estudio de tipo básica; Utilizó como muestra a diez especialistas, entre ellos, personal del Departamento de Alta Tecnología en Arequipa, especialistas en delitos informáticos; Desarrolló el enfoque cualitativo en base al diseño no experimental - descriptivo; Implementó la entrevista para el procedimiento de recolectar los datos; Por lo que concluyo, que la Banca Móvil promueve los delitos informáticos, debido al uso masificados durante 2020 en pandemia pues los ciberdelincuentes lograron despojar los fondos monetarios de clientes tanto financieros como bancario bancarios, pues estas son de fácil acceso.

Adarmes y Ortiz (2020) tuvieron como objetivo identificar la intervención de los que operan la administración de justicia ante el incremento de delitos informáticos o ciberdelitos durante el estado de emergencia; Fue un estudio de tipo básica; Utilizó como muestra a operadores de justicia que hayan intervenido en casos de delitos informáticos, así como, al Ministerio Público y abogados; Desarrolló el enfoque cualitativo en base al diseño conocido como teoría fundamentada; Implementó la entrevista como técnica de recolección de datos; Por lo que concluyo, que frente al ataque masivo por los delitos informáticos el gobierno debió invertir más en seguridad informática, así mismo, entendió que el ilícito se comete mayormente por el descuido de la propia víctima, finalmente evidencio que el gobierno peruano no brindo adecuadas herramientas tecnológicas para combatir estos delitos.

Huaman (2020) tuvo como objetivo identificar los efectos producidos por la suscripción al convenio de Budapest; Fue un estudio de tipo básica, Utilizó como muestra a especialistas; Desarrolló el enfoque cualitativo en base al diseño descriptivo, jurídico y comparativo; Implementó la entrevista como técnica de recolección de datos; Por lo que concluyo, que se requiere políticas orientadas a destinar recursos económicas para un equipamiento de la tecnología adecuada e

informativa la que ceda el uso adecuado al momento de combatir los delitos informáticos.

Cangalaya (2020) tuvo como objetivo evidenciar el nivel de sucesos de fraudes informáticos en los subsidios otorgados en Chanchamayo; Fue un estudio de tipo sustantivo; Utilizo como muestra a 15 denunciantes de un total de 1,317, 10 jueces, 10 Fiscales, 5 policías y 5 abogados litigantes; Desarrolló el enfoque cualitativo en base al diseño de investigación descriptiva simple; Implementó la encuesta como técnica de recolección de datos; Por lo que concluye, que los incidentes de fraudes informáticos incrementó un 59% a raíz de los subsidios bridados en pandemia en la ciudad de Chanchamayo y que la Corte Superior de Justicia Penal de Selva Central no cuenta con la capacidad de atender las masivas denuncia por su escasa implementación y logística tecnológica con la que trabajan.

Ormache (2019) tuvo como objetivo proponer estrategias de ciberseguridad, para fortalecer la seguridad nacional en el Perú en cuanto a las experiencias internacionales exitosas; Fue un estudio de tipo interpretativo - hermenéutico; Desarrolló el enfoque cualitativo en base al diseño teoría fundamentada; Implementó el análisis documental; Por lo que concluyo, que uno de las limitaciones que se pudo evidenciar son la debilidades estructurales y las fluctuaciones del gobierno virtual y se requieren de la implementación de plataformas virtuales.

Urpeque (2019) tuvo como objetivo determinar cuáles son los aspectos más determinantes sobre las protección de los bienes jurídicos para considerar eficaz la normatividad que regula los delitos informático en Huaura 2018; Fue un estudio de tipo aplicada; Utilizó como muestra a profesionales de especialidad, miembro de la Policía Nacional y abogados del área penal; Desarrolló el enfoque cualitativo en base al diseño metodológico; Implementó la entrevista como técnica de recolección de datos, encuestas, análisis documental y la observación científica; Por lo que concluyo, que la norma contenida en la Ley 30096, esta desactualizada y que los criterios establecidos no son prácticos, además que la actividad humana ha evolucionado, pero el fin de victimar de formas tan simples como es a través de los correo y sitios web.

Cotrina (2018) tuvo como objetivo determinar analizar los factores que impiden la aplicación de la Ley N° 30171 en Lima Norte 2016; Fue un estudio de tipo fenomenológico; Utilizó como muestra a conocedores y/o especialista sobre los Delitos Informáticos, tales como colegiados especialistas y DIVINDAT; Desarrolló el enfoque cualitativo en base al diseño teoría fundamentada; Implementó la entrevista como técnica de recolección de datos y análisis documental; Por lo que concluyo, que los principales factores que impiden la implementación son la falta de capacitación de los magistrados, fiscales, PNP, pese a que la quinta disposición complementaria de la Ley 30096 detalla las "Capacitaciones", pero que no se ha aplicado.

Moreno (2020) tuvo como objetivo evaluar aquellas actuaciones de investigación que se deba realizar en el Ministerio Público, con el apoyo de la Policía y peritos cuyo propósito sea obtener medios probatorios logrando establecer el delito informático fiscal, utilizaron método analítico y deductivo, mediante estudio documental de diversidad de fuentes de datos, concluyendo que es de necesidad la creación de protocolos para la actuación del ministerio público, siendo una guía en base a los principios que establece la constitución, para que así pueda demostrarse la existencia del delito y la probabilidad de que el autor del ilícito haya participado en dicha actividad.

Prieto y Vargas (2020) tuvo como objetivo examinar la ciberdelincuencia dirigida a la adquisición de informes por las formas electrónicas siendo probable deducción para el accionar de estos delitos cibernéticos y el manejo de la legislatura ecuatoriana; fue una investigación tipo descriptiva; utilizando recopilar datos de ciberdelincuencia y la apropiación de las informaciones y sus conductas; empleando la metodología de exploración conceptual siendo estos a través de entrevistas; concluyendo que en Ecuador no se cuenta con fiscalías especializadas en delitos informáticos, tramitándose estos casos ante la Unidad de Patrimonio Ciudadano y los otros delitos identificando al bien jurídico tutelado requiriéndose de la creación de un Organismo Especializado en Ciberdelincuencia.

Montaño (2019) tuvo como objetivo mostrar la necesidad de que se incorpore al código penal los delitos informáticos; Fue un estudio tipo descriptivo; se utilizó como muestra fichas bibliográficas a través de libros y documentos, desarrolló el

método mixto; implemento la entrevista y la revisión documental; por lo que se concluye la importancia de resaltar respecto a la sociedad de la información la carencia de profesionales en derecho o expertos relacionados al derecho informático, asimismo, un grupo de personal profesional en derecho e informática que cuenten con material novedoso de tecnología, realizando labores conjuntamente teniendo como fin luchar contra la delincuencia informática.

Linares y Flores (2017) tuvo como objetivo efectuar una investigación del cual motive un documento de utilidad cuyo fin sea de guía para distinguir los delitos informáticos; desarrollo un enfoque documental utilizando técnica o metodología de recolección de evidencias; por lo que concluye, que el país Salvador intenta tener sus inicios en los ilícitos penales, no obstante, se tiene que tener en cuenta que se debe mejorar, desarrollar e implementar herramientas que coadyuven a los investigadores mediante tecnología y que se desarrolle mediante especialistas empeñados en la persecución de estos ilícitos.

Ruiz (2016) Tuvo como objetivo analizar y conocer de manera crítica y jurídica la realidad de los Delitos Informáticos y la violación de los derechos constitucionales de los ciudadanos ecuatorianos, fue un tipo de investigación científica, desarrollo en el enfoque cuantitativo, utilizando entrevistas a 30 profesionales de la abogacía, concluyendo que ante la carencia de conocimientos respecto a la tecnología de información y comunicación, es la razón primigenia para magistrados, profesionales del derecho y legisladores en la materia, obviando los elementos que deben adherirse a la ley de ecuador.

Bruno (2016) tuvo como objetivo el estudio de la realización de delitos, usando nuevos medios tecnológicos, asimismo, el marco jurídico en el que se rige, así conocer los inconvenientes que presentan los investigadores judiciales; Fue un tipo de estudio descriptivo; Utilizó exposiciones de la legislación vigente; Desarrolló en el foque cualitativo en el cual se realizó a través de experiencias vividas para la obtención de sus datos, concluyendo que tratándose de recursos humanos, estos son útiles para coordinación de las capacitaciones del poder judicial así como las fuerzas de seguridad, detectar la configuración de un delito informático, realizar investigación eficiente y lograr su individualización del o de aquellos imputados.

Ribero (2016) tuvo como objetivo preparar un estudio referente a los delitos informáticos, así como la legislación colombiana en su perspectiva tecnológica y social; se desarrolló el enfoque cualitativo del cual se utilizó la recolección de datos ello con la finalidad de definir preguntas para la investigación, implementando la entrevista como método para recabar datos; concluyendo que en la legislación colombiana respecto a delitos informáticos se encuentra avanzada, en la práctica se conoce carencias en la prevención y lucha de la ciberdelincuencia ya que las entidades estatales que realizan la investigación criminal y entes encargados de la justicia no cuenta con especialistas en la rama, perjudicando la investigación.

Posada (2017) señaló a los cibercrímenes y afectaciones en la teoría de tipicidad de realidad presencial a una vivencia virtual de los ciberdelincuentes, los mismos que se caracterizan particularmente correspondiendo a la acción, tanto del sujeto como la del resultado y los cargos, debiendo de plantearse de manera completa en ciertos aspectos así poder exponer y utilizar estas fenomenologías digitales que se suscitan en realidades virtuales, del cual se aconseja un poco actividad del ser humano, tomando en cuenta la teoría de la tipicidad ante los patrones de delitos informáticos.

Chinchón (2014) refirió que la inmunidad al momento de administra justicia y el vínculo que se tiene con los delitos informáticos, se soslayan entre un estado deterioro y la falta de conocimiento del poder legislativo en el ciberespacio lo que resulta inaplicable las reglas o normas que se dan en un área territorial

Izaga (2021) arribo en que las entidades persecutoras públicas son de gran importancia para la obtención de un ambiente organizacional idóneo para el trabajo, pues como resultado de la observación se tendría resultados óptimos. Es de suma necesidad que su finalidad sea aportar a la persecución de los objetivos.

Leyva (2021) enmarco al delito informático como aquella conducta dolosa que genera una afectación al ciudadano o entidades, sin que se reciba un aprovechamiento material para el sujeto activo, sino que, antes bien, genera un lucro ilegal al autor aun sin que este no genere afectaciones de forma inmediata o directa a los usuarios, cuya realización a los dispositivos mayormente utilizados intervienen en la conducta ilícita informática.

Cotrina (2018) manifestó que la administración de justicia, resulta ser un factor determinante, teniendo en cuenta que los magistrados tienen la carga de evaluar, motivar y de hacer cumplir lo establecido en la ley y el desconocimiento en los delitos informáticos impediría la función correcta de la misma manera.

Guerrero (2018) señala que en los cuerpos normativos nos encontramos con varios factores en el entorno de la sociedad los cuales realizan diferentes labores, para darse así el objetivo de análisis, el encargado de optar por medidas normativas para frenar la ciberdelincuencia es el gobierno, es el caso, que se debe crear fiscalías y también juzgados especializados en estos delitos el cual es necesario para cumplir con el fin que se plantea, siendo que para una correcta función por las autoridades, es esencial contar con un personal eficiente y altamente capacitado.

Mayer y Oliver (2020) precisaron que el delito de fraude informático anuncia la perpetuación en contra netamente de un bien patrimonial a través de la manipulación o alteración, es decir, interrumpir el normal desarrollo de un sistema informativo el cual almacena datos o programas ya sea de uno o varias personas ya sea natural o jurídica.

Pardo (2018) define que el fraude informático es aquel daño patrimonial que se crea a un tercero a través de manipulaciones de los datos informáticos o bien la deficiencia en la finalidad de un sistema de informática, en el cual su fin es el obtener de manera ilegítima un provecho económico para sí mismo o de algunas terceras personas.

La Ley N°30096 en su artículo 9° (2013) tipificó a la suplantación de identidad como al que, a través del uso de las tecnologías por la información, además de la comunicación incurre en suplantación de la identidad de una persona ya sea natural o jurídica, precisar que la conducta si tiene como resultado de perjuicio, material o moral tendrá una pena privativa no menor de tres años hasta cinco años.

Montaperto (2018) mencionó que la suplantación de identidad es una actividad que se despliega por el delincuente teniendo como finalidad en dañar la esfera patrimonial de la víctima, refiriéndose a la propiedad, como así también a la espera extra patrimonial, siendo realizado estas acciones por individuos de los

cuales tienen conocimiento y capacitaciones sobre sistemas informáticos, manejo de dispositivos móviles o conocedores de la tecnología.

Los especialistas del Ministerio Público (2020) describieron al Ministerio Público como una entidad previsora y persecutora de los delitos, así también, como el defensa de la legalidad salvaguardando el tesoro público y privado que se encuentran tutelados en la ley. Asimismo, también son considerados como los representantes del conjunto social y los comisionados a fin de velar por la recta y efectiva administración de justicia.

Los voceros del Poder Judicial (2021) señalaron que de acuerdo con la Constitución Política de Perú y las leyes, el Poder Judicial sería la institución encargada o tiene la función de administrar justicia vía sus órganos jerárquicos, como los Juzgados de Paz no Letrados, Juzgados de Paz Letrados, Cortes Superiores y finalmente la Corte Suprema, no obstante precisar que es un órgano autónomo.

Pereyra y Turpo (2020) concluyeron que La División de Investigación de Delitos de Alta Tecnología (DIVINDAT), es aquel órgano de la Dirección de Investigación Criminal de la Policía Nacional del Perú (DIRINCRI), quienes tiene como misión la investigación, proceder con las denuncias, así como, la de combatir el crimen organizado transnacional y en especial aquellos que atenten contra la libertad, el patrimonio, la seguridad pública, la fe pública y otros, los cuales se cometen a través del uso de la tecnología en busca de la información y comunicación, captando indicios, evidencias, además de pruebas para identificar, ubicar y que finalmente se logre detener a los autores mediatos de estos ilícitos, con la finalidad de que se pongan a derecho y a disposición a la autoridad que es competente.

Becker y Viollier (2020) manifestaron que el Convenio de Budapest tiene por objeto desarrollar una política criminal enfrentado a la ciberdelincuencia, a través de la homologación de las conceptualizaciones y de la conducta a través de la legislación sustantiva, penal y más aún procesal para lograr una sistema célere y eficaz conjuntamente con la cooperación internacional.

En el Perú, Ley de Delitos Informáticos tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia, asimismo se contaría con la Ley que modifica la ley 30096, ley de delitos informáticos la modificatoria de los artículos de la presente. (Ley n° 30096, 2013)

No obstante, con el fin de contribuir al concepto de los delitos cibernéticos, se recoge lo establecido el “Convenio de Budapest”, la “Ley de delitos informáticos N° 30096” y la Ley “Ley que modifica la Ley 30096, Ley de delitos informáticos N° 30171”, en la cual precisa que “el que deliberada e ilegítimamente procura para si o para otro un provecho ilícito en perjuicio, de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación, de datos informático cualquier interferencia o manipulación en el funcionamiento de un sistema informático”. (Ley N° 30171, 2014)

Oziomek (2021) manifestó que el patrimonio de la víctima se puede entender como un instrumento personal o de uso laboral, la pérdida o sustracción del mismo busca la finalidad de indemnizar especialmente a consecuencia de la perpetración del bien.

Díaz y Dávila (2018) manifestaron que el sistema informático es aquello se comprende al conjunto de dispositivos, recursos, materiales, partes e inmateriales que realizan almacenamiento, ordenan, procesan información y datos a la ejecución de los programas, sistema operativo orientado a la ayuda de cierta actividad humana.

En el convenio de Budapest, resolvió la definición de “Sistema Informático” la cual se comprenderá a todo dispositivo, cuya función sea el procesamiento automático de datos. Por “Datos informáticos” se entenderá a toda figura que transmite información incluido los programas diseñados para llevar a cabo una función (Convenio de Budapest, 2001).

Acurio del Pino (S/F) sostuvo que la manipulación de datos informáticos representa el delito informático más común ya que es fácil de cometer y difícil de

descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

Acuerdo plenario 7-2006 (2006) estipulo como regla de interpretación que la individualización es un requisito indispensable para la imputación de un delito conforme a la Ley 28117. En un sentido procesal refiere a un motivo específico de inadmisión ante su falta de implementación, prolongando el tiempo y afectando al perdicado.

Davila (S/F) preciso que el Hardware es el equipo o dispositivos físicos que componen un computador, mientras que el software es el sistema de procesamiento de información intangible, ya se una base de datos, programas y todo lo que se pueda almacenar.

Los estudiosos de la Plataforma única del Estado Peruano (2002) preciaron que la persona natural, es cualquier sujeto de derecho que tenga una actividad económica propia y ejerce sus acciones a título personal. Por otro lado, como persona jurídica no ejerce sus acciones a título personal, sino que una empresa de cierta forma le brinda derechos y obligaciones a raíz de las celebraciones contractuales y extracontractuales. Una Persona Jurídica participa a través de sus representantes legales.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

El presente proyecto de investigación empleó un enfoque cualitativo ya que este busca dar respuestas al modo en que se realiza una investigación abocándose a la realidad problemática y hallando posibles respuestas conforme se va investigando conjuntamente con la perspectiva y propósitos encaminados a entender una situación problemática.

Enfoque cualitativo refiere a la obtención y estudio de datos a fin de centrar las preguntas en base a la investigación o demostrar las recientes incógnitas en el transcurso de la investigación. Los investigadores realizan sus hipótesis, pero la misma no recorre un sendero concretado certeramente. Sus planteamientos de un inicio no son claros a diferencia del enfoque cuantitativo y las interrogantes de investigación no son conceptualizadas ni definidas completamente. (Fernández y Baptista, 2014)

El método que se utilizó es inductivo, el mismo que se origina de lo particular a lo general necesitándose conocer a fondo el terreno que se estudiara. El enfoque cualitativo tiene carácter inductivo y en este se pueden dar similitudes a partir de un fenómeno dado que se pueden encontrar, entendiendo el proceso, de experiencias y cambios. No obstante, se somete a un proceso inductivo bajo una serie de sucesos que los mismos son observados, descritos, explorados e incurren de lo particular a lo general, que se crea “al final del día” perspectivas teóricas; entendiéndose que, se avanza situación por situación, informe por informe, hasta finalizar a una perspectiva general (Mendoza, 2018).

El tipo de diseño que se implemento es el fenomenológico, ya que este busca explorar, comprender y describir las experiencias que tuvieran los ciudadanos en relación a un fenómeno y encontrar los componentes comunes en razón a las experiencias ante un determinado fenómeno. En la fenomenología el investigador labora de forma directa con las declaraciones o unidades de los que participan dando a conocer sus experiencias (Mendoza, 2018).

3.2 Categorías, subcategorías y matriz de categorización

Tabla 1

Matriz de categorización apriorística

Categorías	**Subcategorías**	**Criterio 1**	**Criterio 2**	**Criterio 3**
Entidades persecutoras	Administración de Justicia	Ministerio Público	Poder Judicial	Divindat
	Cuerpos normativos	Convenio de Budapest	Ley n° 30096	Ley n° 30171
Delitos Informáticos	Fraude informático	Patrimonio	Sistema Informático	Manipulación de Datos Informáticos
	Suplantación de identidad	Individualización	Software y Hardware	Persona natural y jurídica

3.3 Escenario de estudio

El escenario competente en el presente proyecto de investigación son la División de investigación de Alta Tecnología (DIVINDAT), por ser la entidad que trabaja conjuntamente con la Dirección Nacional de Investigación Criminal (DIRNIC) pues son quienes realizan las investigaciones a nivel policial, ya que cuentan con los medios que les brinda el estado para actúen conforme a sus atribuciones. Otra entidad competente es el Ministerio Público, pues ellos son quienes según la doctrina tienen la carga de prueba, por ende, el iniciar los procesos y acusar el cual está dentro de sus funciones. Finalmente, el Poder Judicial también es una entidad competente pues tiene la facultad y juzgar y penalizar las conductas ilícitas. Entendiéndose que las tres son entidades y estudios que cuentan con profesionales y estudiosos del tema materia de investigación.

3.4 Participantes

Mendoza (2018) refiere que aquellos participes son orígenes internos de informes que investigador obtiene asimismo siendo participante, así como medios u observados en todo momento y tiempo, de modo que, el estudio cuenta con la participación de profesionales y estudiosos que se investiga.

Acorde con lo anterior, se tomó la información de la normatividad legal de Ley 30096°, Ley 30171°, Convenio de Budapest, la Constitución Política del Perú entre otros.

Tabla 2

Lista de participantes

Nombres Completos	**Profesión**	**Centro Laboral**	**Cargo**
Asenet Scarlett Muro Delgado	Abogado	Independiente	Litigante
Moisés Fernández Benites	Abogado	Ministerio Publico	Fiscal Provincial del Primer Despacho de la Primera Fiscalía Corporativa Penal de la Victoria San Luis
Rogers Vicentico Arbulu Valdez	Abogado	Ministerio Publico	Fiscal Adjunto del Tercer Despacho de la Sexta Fiscalía Corporativa Penal de Cercado de Lima – Breña – Rímac – Jesús María
Jorge Venegas Rivera	Abogado	Ministerio Publico Especializada en Ciberdelincuencia	Fiscal Adjunto del Primer Despacho de la Primera Fiscalía Especializada en Ciberdelincuencia de Lima Centro

Wuilman Zabarburu Vargas	PNP	DIRINCRI	Analístico Informático Forense de la División de Investigación de los Delitos de Alta Tecnología

3.5 Técnica e instrumentos de recolección de datos

El enfoque se tuvo en cuenta a los métodos de recolectar muestras no estandarizados ni completamente establecidas al comienzo. Los datos cualitativos se constituyen principalmente en narrativas de diferenciadas categorías: visuales (como imágenes y fotografías), verbales, auditivas (grabación de sonido y audio), trascripción de audios y de videos, artefactos tecnológicos, entre otros. Por lo que, se usa de forma flexible y en relación a lo que se necesita la investigación mediante procedimientos en el cual se pueda recolectar informes, siendo la verificación de material documentario, observando no estructurada, entrevistas más a fondo, evaluación de experiencias individuales y compartidas (Mendoza, 2018).

Con forme a lo expuesto en las líneas anterior, el instrumento aplicado fue la entrevista, la cual será puesta en ejercicio para comprender cada uno de las respuestas brindada por los participantes.

3.6 Procedimiento

En la investigación cualitativa informan sobre lo investigado con el propósito de demostrar las múltiples formas en la cual se encuentra realizando por los investigadores. Primero se tiene el contexto de los que realizan la investigación se tiene como un tema a tener en consideración. La vinculación de los indagadores con el objetivo que se estudia, con los que participan y junto con adecuados acuerdos vinculados, todo influye en el procedimiento que se tiene de una investigación. Como segundo paso, los investigadores cualitativos detallan a entorno en el cual se está creando un fenómeno o asunto de estudio, como tercer paso, se puntualizan el contexto de sus centros de información, igualmente, el de realizar una descripción los fenómenos, los orígenes de información. En conceptos de encontrarse, tanto como al tiempo y a los períodos, aquellos que investigan de

forma cualitativa pretenden poner aquellos factores que tengan vinculaciones dinámicas comunes e importantes. (Levitt, 2018).

Por lo que se debe tener uniformidad a fin de centrar un sistema útil y entrelazado para así aportar a la enseñanza del hecho o hechos a los cuales se indican o que tiene representación. De modo que, las categorías del presente trabajo será materia de la formulación de las preguntas que se efectuaran al momento de la aplicación del instrumento, esto es, la entrevista. Cabe precisa, que las categorías además son elementos que nos ayudaran a comparar y mediante las cuales demostraremos algo (Muñoz, 2016).

3.7 Rigor Científico

Los especialistas del National Institutes of Health (2021) refirieron que el rigor científico en el estudio cualitativo, es muy riguroso en cuanto a método científico ya que fija aquellos como el diseño experimental, la parte metodología, el estudio, la interpretación y el contenido de todos los resultados firmes y sólidos, así como imparciales. Quiere decir una total claridad al hacer saber los pormenores resultantes para que así las demás personas puedan propagar y ampliar los que se pueda obtener.

Tabla 3

Tabla de validación de los entrevistados

Nombres Completos	**Profesión**
Asenet Scarlett Muro Delgado	Abogado
Moisés Fernández Benites	Abogado
Rogers Vicentico Arbulu Valdez	Abogado
Jorge Venegas Rivera	Abogada
Wuilman Zabarburu Vargas	PNP

3.8 Método de análisis de datos

Hernández (2019) refirió aquel instrumento Atlas T.I es un programa para su uso de tecnología, originada cuyo fin sería el de coadyuvar la estructura, el estudio y esclarecimiento del material recabado en las investigaciones cualitativas. El aplicativo facilita el trabajo y organización en mayores cantidades de información teniendo una amplia variedad de formatos digitales. Así mismo, luego de realizar selección y similitudes, mejorando el transcurrir de una investigación así creando un beneficio a la obtención de la información, el recabar los datos y el del trabajo en conjunto.

Para el análisis de los datos cualitativos, el procedimiento aconseja tres facetas para un óptimo desarrollo, teniendo como primer punto de carácter generalmente descriptivo en el cual mediante la codificación despejada serviría para individualizar las categorías, teniendo como segundo punto el de analizar situaciones que se encontrarían relacionadas con las categorías y estas junto a las subcategorías, a través de la codificación axial, y como tercer punto se tendría que entablar con características que refinen aquellas categorías que integran son identificables a través de una selectiva codificación.

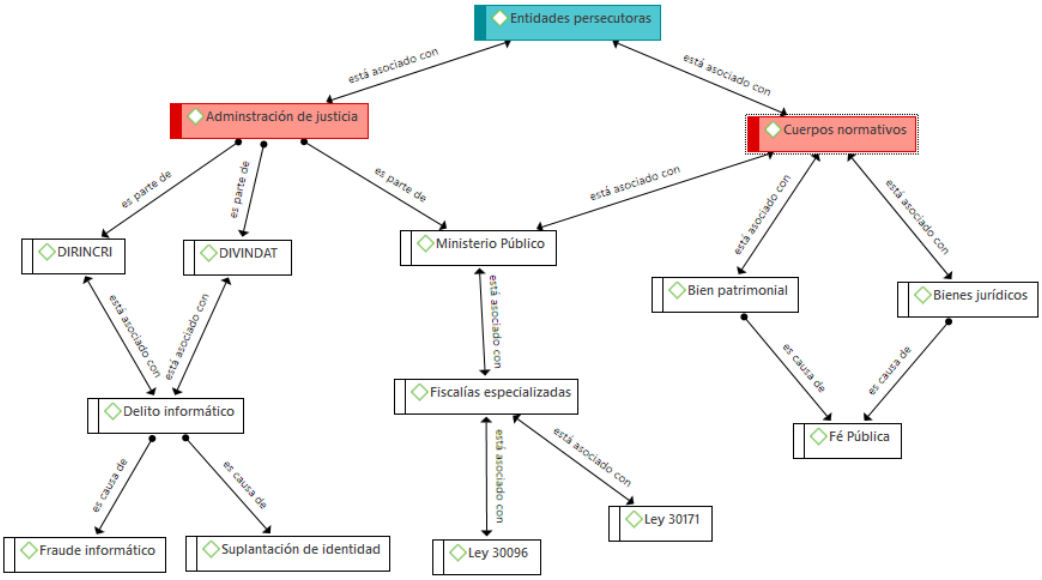
3.9 Aspectos éticos

La investigación científica peticiona al investigador un comportamiento ético, en este lugar no hay paso a conductas indecorosas las cuales pueden afectar aquellos procedimientos de un investigador y pervertir la ciencia en razón a ambiciones y particularidades de agradecimiento; la incertidumbre es complicada, ya que este trata de sucesos vinculados estrechamente al valor moral que tiene que tener el investigador, aunque la misma no tuviera reglas definitivas con el propósito de frenar este mal, conocer las particularidades, los procedimientos, las técnicas y los métodos que sean para recabar información, las bases éticas de las etapas investigadoras, así como de la apariencia ética relativa al asunto son decisivos, y de suma importancia para el investigador cualitativo ya que este asume una postura ético política teniendo un compromiso al respetar los derechos humanos de aquellos que sean partícipes (Ocaña & Reyes, 2017).

IV. RESULTADOS Y DISCUSIÓN

4.1. Resultados

Figura 1
Categoría 1: Entidades persecutoras



Se ha puesto en evidencia que, en líneas generales, las entidades percutoras pueden ser consideradas como aquellas que se encargan de hacer frente hacia los bien conocidos como delitos informáticos dentro de nuestro país, incidiendo con ello en entidades como las representadas por el Ministerio Público, en congruencia con los esfuerzos realizados por las fiscalías especializadas en cuanto a la Ley 30096 y la ley 30171; así como, organizaciones como la DIRINCRI y DIVINDAT, las cuales buscan mitigar la prevalencia de delitos informáticos, sobre los cuales se puede acontecer a la existencia del bien comprendido como fraude informático y la suplantación de identidad. Mientras que, no se puede dejar de lado la necesidad que se tiene hoy en día de la conformación de cuerpos normativos que puedan ofrecer un respaldo íntegro hacia el bien patrimonial y los bienes jurídicos, sobre los cuales acontece a la afectación hacia la fe pública.

En ese sentido, los entrevistados ASMD1, MFB2, RVAV3, JVR4, WZV5 señalaron que la entidad persecutora del delito mediante el marco de principio de legalidad es correspondiente al Ministerio Público, en apoyo de la Policía Nacional

del Perú y el Poder Judicial, dicho ello los entrevistados MFB2, RVAV3, JVR4, WZV5 refirieron que la unidad encargada de investigar los delitos informáticos es correspondiente a las Fiscalías de Ciberdelincuencia, el cual mediante Resolución N° 843-2020-Fiscalía de la Nación, quienes a partir del 15 de junio del 2021, tomo competencia respecto a los delitos informáticos a nivel nacional, realizando investigaciones para lograr una responsabilidad penal a los sujetos autores de estos delitos.

Adarmes y Ortiz refirieron que frente al ataque masivo por los delitos informáticos el gobierno debió invertir más en seguridad informática, así mismo, entendió que el ilícito se comete mayormente por el descuido de la propia víctima, finalmente evidencio que el gobierno peruano no brindo adecuadas herramientas tecnológicas para combatir estos delitos, dicho esto, los entrevistados MFB2, RVAV3, JVR4, WZV5 expresaron que dicha actuación de las entidades siendo el Ministerio Público en apoyo de la Policía Nacional del Perú es la de prevenir, combatir, investigar y denunciar bajo la estricta dirección fiscal cometidos por delincuentes comunes u organizaciones criminales que puedan generarse en todo el país.

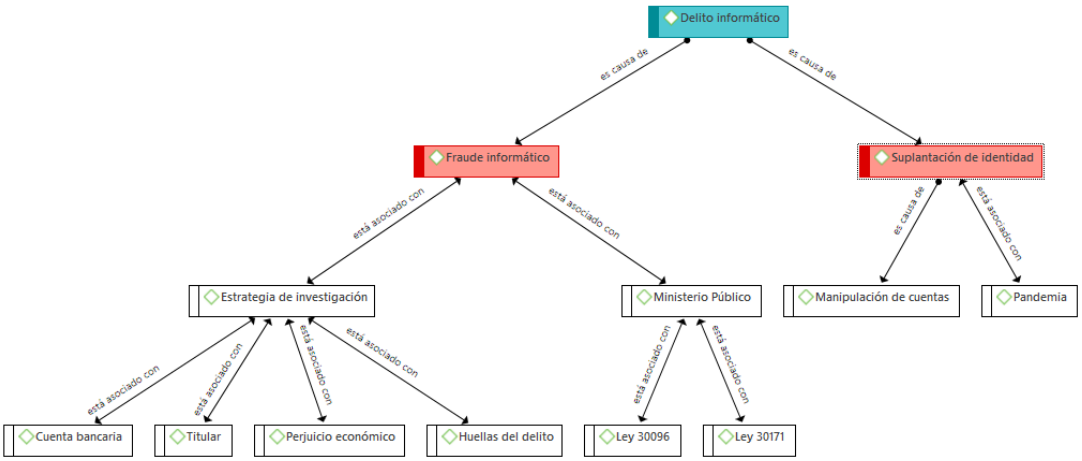
Asimismo, Montaño concluyeron que la importancia de resaltar respecto a la sociedad de la información la carencia de profesionales en derecho o expertos relacionados al derecho informático, asimismo, un grupo de personal profesional en derecho e informática que cuenten con material novedoso de tecnología, realizando labores conjuntamente teniendo como fin luchar contra la delincuencia informática, el entrevistado JVR4 refiere que respecto al manejo del código penal y procesal este delito aún falta un manejo idóneo para establecer estrategias ya que estos delitos son una modalidad compleja ya que implica el uso de software especializados de los sistemas informáticos.

Barrutia señaló que una de las limitaciones que se pudo evidenciar son la debilidades estructurales y las fluctuaciones del gobierno virtual y se requieren de la implementación de plataformas virtuales, al respecto los entrevistados ASMD1, MFB2, RVAV3, JVR4, WZV5 refirieron que si bien la ley actual siendo 30171 se encuentra modificada de la 30096, esta misma no se encontraría del todo adecuada ante la lucha y prevención de los delitos informáticos, puesto que la delincuencia

en material informática está más avanzada no logrando suplir la protección de los ciudadanos y la persecuciones de los mismos.

Figura 2

Categoría 2: Delitos informáticos



Los delitos informáticos fueron incrementados progresivamente en pandemia por la Covid-19 a partir del 2020 y su gran apogeo fue evidenciado a través de los medios de comunicación en el 2021, la cual fue identificada por los entrevistados como el delito más concurrente y que no discriminaba a sus víctimas, es decir, que sus víctimas eran mujeres y hombre desde los dieciocho hasta personas de la tercera edad en razón a que los entrevistados precisan que el sujeto activo en este tipo de delitos hace uso de su habilidad, conocimiento y capacidad de conocimiento para poder invadir los dispositivos tecnológicos.

En ese sentido, los entrevistados ASMD1, MFB2, RVAV3, JVR4, WZV5 señalaron que los delitos informáticos incrementaron considerablemente a través de la pandemia a raíz de que la población peruana se encontraba atravesando una coyuntura sanitaria y con la extrema necesidad de comunicarse a través de los aparatos tecnológicos sin mediar por el desconocimiento los riesgos a los que expondrían.

En ese sentido, se pasa a discutir el resultado de la segunda categoría en base a los antecedentes y teorías que sostiene la presente investigación:

Dicho lo anterior, Adarmes y Ortiz refirieron que frente al ataque masivo por los delitos informáticos el gobierno debió invertir más en seguridad informática, así mismo, se entiende que el ilícito se comente mayormente por el descuido de la propia víctima, finalmente evidencio que el gobierno peruano no brindo adecuadas herramientas tecnológicas para combatir estos delitos

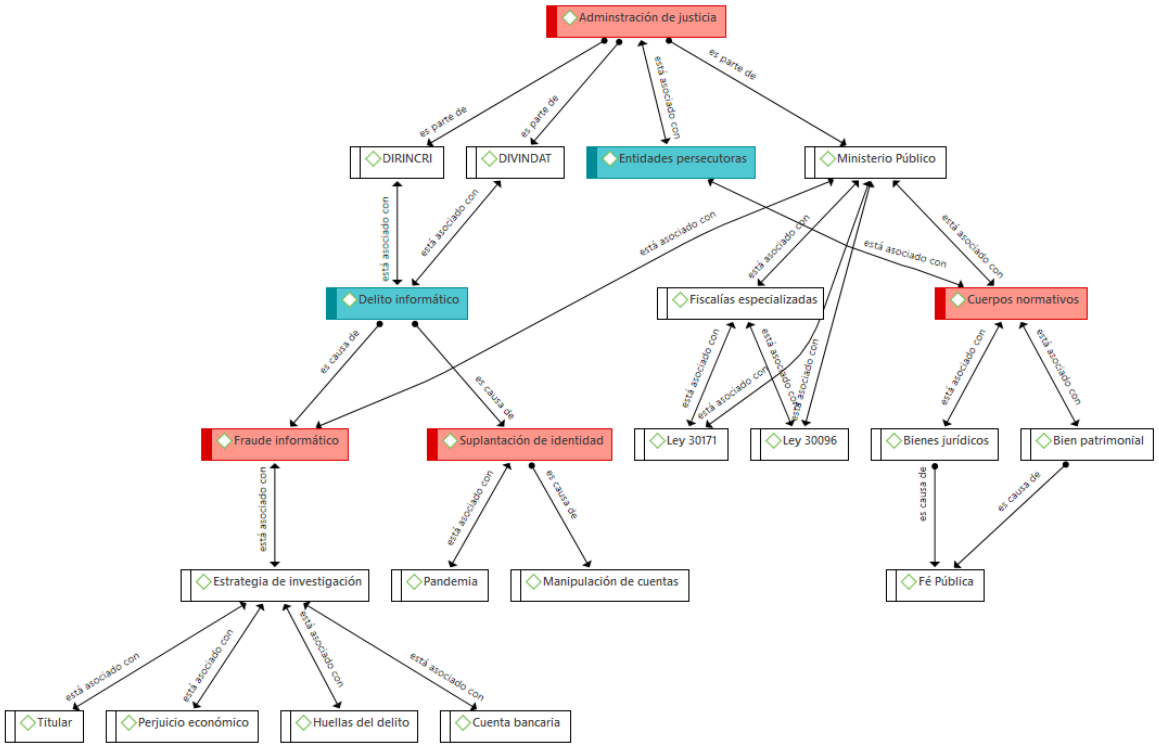
Cangalaya tuvo como objetivo evidenciar el nivel de incidencia del delito de fraude informático en Chanchamayo; En ese sentido, los entrevistados MFB2, WZV5, JVR4 coincidieron que durante cuarentena la concurrencia de este tipo de delito informático se incrementó desmesuradamente en sus diversas modalidades, siendo el más concurrente el “phishing”, cuya modalidad no se encuentra tipificada conforme el Convenio de Budapest prevé. Por otro lado, se evidencio a través de los medios de comunicaciones en múltiples oportunidades denuncias por transferencias bancarias de grandes cantidades de dinero donde los propios bancos y las victimas por falta de conocimiento fueron victimados por los ciberdelincuentes.

Al respecto, los investigadores del Gobierno de Perú evidencio que en el año 2021 el Ministerio Público registro alrededor de 21 mil denuncias por delitos informáticos en todas sus modalidades a raíz de un estudio técnico que fue realizado en el 2020 y que las mismas serán tramitadas con la Ley N° 30096 concordante con la Ley N° 30171, ley que modifico los artículos 2°, 3°, 4°, 5°, 7°, 8°, y 10° de su legislación predecesora.

Finalmente, con los delitos informáticos, se puede señalar que estos han estado relacionados directamente con la prevalencia del fraude informático y la suplantación de identidad, entendiendo que el fraude informático ha buscado ser controlado mediante la implementación de estrategias de investigación que han estado basadas en la evaluación y seguimiento de la cuenta bancaria, la detección de la persona titular y la inspección de la misma, en donde la persona sobre la que se ha cometido un prejuicio informático tiene que estar en orden activo para proceder con la indagación y poder detectar las huellas del delito, entendiendo que ello puede deberse a un proceso de suplantación de identidad, en donde el individuo afectante tiende a realizar la manipulación de cuentas y ello se ha visto

agravado a causa de la pandemia, en donde el control informático se ha visto perjudicado significativamente.

Figura 3
Red de información



En base a los resultados expuestos anteriormente, se ha podido demostrar que la administración de justicia no solo ha incidido directamente en mantener el control sobre el fraude informativo o la suplantación de identidad, sino que esta incide directamente en el control integral del delito informático, entendiendo que las entidades persecutoras más incidentes dentro del ámbito nacional, se encuentran conformadas por DIRINCRI, DIVINDAT, Ministerio Público y en compañía de las fiscalías especializadas, las cuales toman como referencia a la Ley 30171 y la Ley 30096, con la intención de poder preservar los bienes jurídicos, el bien patrimonial propiamente dicho, en cuanto a la no afectación de la fe pública, considerando a cuatro estrategias de investigación que han tenido que ser mejoradas con la progresión de la pandemia, siendo las siguientes: la evaluación del titular de la cuenta, la evaluación del prejuicio económico, el seguimiento hacia las huellas del

delito y el análisis de los movimientos que se han realizado en las cuentas bancarias.

Figura 4
Nube de palabras

Las palabras que han sido más recurrentes dentro de las guías de entrevista aplicadas y expuestas en la nube de palabras, han tenido que ver con “Informáticos” y “Delitos”; entendiendo que estas palabras llegan a ser incidentes dentro del ámbito de estudio, debido a que la prevalencia de los delitos informáticos que se ha alcanzado en los últimos años, como consecuencia de la pandemia, ha acreditado la existencia de robos informáticos, afectación hacia los sistemas bancarios o la suplantación de identidad, teniendo que ver directamente con la afectación tecnológica hacia los sujetos o afectados, entendiendo que se requiere del esfuerzo de los organismos nacionales de control o bien entendidos como entidades persecutoras, con la finalidad de administrar justicia y fortalecer los cuerpos normativos en control con los bien conocidos como delitos informáticos.

V. CONCLUSIONES

1. Se determinó, que son diversas las entidades persecutoras de los delitos informáticos, siendo la más conocida la División de Investigación de Alta Tecnología (Divindat); No obstante, el 15 de Junio del 2021 conjuntamente con la implementación del Nuevo Código Procesal Penal del 2004 en Lima centro, dio origen a la Fiscalía Especializada en Ciberdelincuencia con competencia nacional, sin embargo, se evidencio problemas como la falta de personal capacitado en ambos órganos, así también, la insuficiencia de herramientas digitales y tecnológicos para llevar a cabo una correcta investigación; y finalmente cursos, capacitación por parte del Gobierno Peruano a todo el personal, pues a raíz de la pandemia la Fiscalía Especializada en Ciberdelincuencia y la Divindat no se abastece ante la indagación de los delitos informáticos.
2. Se estableció, que los delitos informáticos incrementaron masivamente en razón a que debido a la inmovilización social obligatoria causado por la covid-19, generando así que las labores cotidianas se realizaran a través de dispositivos móviles y de todo aparato tecnológico, dando pie al teletrabajo o trabajos remotos originando compras online, negocios vía redes sociales, masivas transferencias bancarias, entre otros, dejando en exposición a todos los usuarios quienes además desconocen sobre estas nuevas modalidades delictivas. Determinar si la actuación de las entidades persecutoras de los delitos informáticos fueron las adecuadas durante pandemia por covid-19, como objetivos específicos se tuvo: (a) Explicar porque los delitos informáticos incrementaron durante la pandemia por covid-19. (b) Identificar cuáles son las entidades persecutoras de los delitos informáticos creadas por el Estado.
3. Se estableció, que las entidades persecutoras de los delitos informáticos son la Fiscalía Especializada en Ciberdelincuencia creada mediante Resolución N° 843-2020, con competencia a nivel nacional desde el 15 de junio del 2022. Por otro, lado se cuenta también con División de Investigación de Alta Tecnología (Divindat) creada en agosto del 2005, precisar que antes los delitos informáticos eran tratados por la DIRINCRI en su División de Estafa,

sin embargo, los especialistas expresan que ambas entidades carecen de personal y evidencian que no cuentan con un presupuesto económico que logre dar buenos resultados ante los delitos informáticos.

VI. RECOMENDACIONES

Debido a que ambas entidades persecutoras no cuenta con personal proporcional, adecuado y capacitado es que se debería de proponer un presupuesto anual al gobierno peruano y que la misma sea invertida en cursos, talleres, capacitaciones, convocatorias a personal permanente que cuente con el perfil adecuado y finalmente la compra de herramientas y plataformas tecnológicas del extranjero para la actuación, persecución, hallazgo, tratamiento y procese que se le debe de dar a los delitos informáticos.

Se recomienda, que a través de la televisión, radio, periódicos, revistas y redes sociales se transmita como actuar al ser víctima de los ciberdelincuentes y también como evitar ser víctimas concientizando los riesgos y perjuicios que generaría el acceder a plataformas desconocidas o al brindar información a desconocidos

Se recomienda, finalmente crear una Corte Especializada en Ciberdelincuencia en cuanto al masivo incremento de las denuncias por delitos informáticos en pandemia, pues actualmente estos delitos se procesan como un delito común sin darle un tratamiento especial. No obstante, ello se tiene que descentralizar la Fiscalía Especializada en Ciberdelincuencia ya que asume los delitos informáticos a nivel nacional por lo que no se abastece.

REFERENCIAS

Instituto Pacifico Actualidad Penal (2021). *Crece las denuncias por delitos informáticos*. Publicado el 02 de junio de 2021. https://actualidadpenal.pe/noticia/crecen-las-denuncias-por-delitos-informaticos/fe1e7c1c-dce6-4230-9a85-032347a6f906/1

Latto, A. (2021). *¿Qué es el ciberdelito y cómo puede prevenirlo?.* Publicado el 17 de abril de 2017. https://www.avast.com/es-es/c-cybercrime#gref

Menezes, P. D'ribeiro, M. Heitman, E. (2021). *Rigor científico y ciencia abierta: desafíos éticos y metodológicos en la investigación cualitativa.* Publicado el 5 de febrero de 2021. https://blog.scielo.org/es/2021/02/05/rigor-cientifico-y-ciencia-abierta-desafios-eticos-y-metodologicos-en-la-investigacion-cualitativa/#.YsswkXa23IV

El peruano (2021) *Ciberdelitos en el Perú: se elevan denuncias de fraude informático y suplantación de identidad.* Publicado el 02 de febrero de 2021. https://elperuano.pe/noticia/121876-ciberdelitos-en-el-peru-se-elevan-denuncias-de-fraude-informatico-y-suplantacion-de-identidad

Saltos, M. F., Robalino, J. L. y Pazmiño, L. D. (2021). Análisis conceptual del delito informático en Ecuador. *Revista Conrado*. F http://scielo.sld.cu/pdf/rc/v17n78/1990-8644-rc-17-78-343.pdf

Izaga, P. (2021). *La comunicación interna y su influencia en el desempeño laboral de los colaboradores de una entidad pública* (Tesis de pregrado, Universidad Ricardo Palma, Lima, Perú). https://repositorio.urp.edu.pe/discover

Oziomek, M. (2021). La reparación de los daños extrapatrimoniales y el principio de reparación integral en el derecho argentino. *Ratio Iuris. Revista de Derecho Privado (9)* 1. https://publicacionescientificas.uces.edu.ar/index.php/ratioiurisB/article/view/1191

Zambrano, A. (2021). *El uso de banca móvil en los delitos informáticos contra el patrimonio en la ciudad de Arequipa, 2020* (Tesis de pregrado, Universidad Cesar Vallejo, Lima, Perú). https://repositorio.ucv.edu.pe/handle/20.500.12692/62306

Leyva. C, (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales*. Lucerna Iuris Et Investigatio,1,29-4.* https://doi.org/10.15381/lucerna.v0i1.18373

Decreto Supremo N° 044-2020-PCM de 2020. (2020, 15 de marzo). El Peruano N° 1864948-2.

Flores, C. C., Mosquera, H. G., Rodriguez, V. T., Cervantes, Z. M., Guerra, P. L., Urbizagástegui, M. J. (2020). *Diagnóstico situacional multisectorial sobre la ciberdelincuencia en el Perú*. Observatorio Nacional de Política Criminal. https://www.gob.pe/es/institucion/minjus/informes-publicaciones/1430016-diagnostico-situacional-multisectorial-sobre-la-ciberdelincuencia-en-el-peru

Plataforma digital única del Estado Peruano (2020) *"Convenio sobre la Ciberdelincuencia" permite a jueces y fiscales realizar requerimientos de cooperación internacional.* Publicado el 15 de setiembre de 2020. https://www.gob.pe/institucion/mpfn/noticias/302628-convenio-sobre-la-ciberdelincuencia-permite-a-jueces-y-fiscales-realizar-requerimientos-de-cooperacion-internacional

Mayer, L. y Oliver, G. (2020) El delito de fraude informático: Concepto y delimitación. *Revista Chilena de Derecho y Tecnología, 9*(1), 151-184. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000100151

Becker, S. y Viollier, B. (2020) La implementación del convenio de Budapest en Chile: Un análisis a propósito del Proyecto Legislativo que modifica la Ley 19.223. *Revista de Derecho Universidad de Concepción 88* (248), 75-112. https://www.scielo.cl/scielo.php?pid=S0718_591X2020000200075&script=sci_abstract

Pereyra, L. y Turpo, J. (2020). *Instrumentos normativos que se deben adecuar en nuestra legislación según el marco del Convenio de Budapest como mecanismo legal de protección a la intimidad personal frente a las TICS* (Tesis de pregrado, Universidad Tecnológica del Perú, Lima, Perú). https://repositorio.utp.edu.pe/handle/20.500.12867/3579

Huaman, M. (2020). *Los delitos informáticos en Perú y la suscripción del Convenio de Budapest* (Tesis de pregrado, Universidad Andina de Cusco, Cusco, Perú). https://repositorio.uandina.edu.pe/handle/20.500.12557/4116

Adarmes, L y Ortiz, A. (2020). *Intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19* (Tesis de pregrado, Universidad Cesar Vallejo, Lima, Perú). https://repositorio.ucv.edu.pe/handle/20.500.12692/62306

Prieto, N. y Vargas, G. (2020). *Ciberdelincuencia, enfocada en la apropiación de información a través de medios electrónicos y su influencia en el cometimiento de delitos informáticos* (Tesis de pregrado, Universidad de Guayaqui, Guayaquil, Ecuador). http://repositorio.ug.edu.ec/handle/redug/50396

Mayer, L. y Vera J. (2020). El delito de espionaje informático: Concepto y delimitación. *Revista Chilena de Derecho y Tecnología, 9* (2), 221-250. https://scielo.conicyt.cl/pdf/rchdt/v9n2/0719-2584-rchdt-9-2-00221.pdf

Espinoza, E. E. (2020). La investigación cualitativa, una herramienta ética en el ámbito pedagógico. *Revista Conrado, 16* (75), 103-110. http://scielo.sld.cu/pdf/rc/v16n75/1990-8644-rc-16-75-103.pdf

Ipanaque. L, (2020). *Canales alternativos digitales y su influencia en el comportamiento del cliente en la empresa Mibanco, agencia Talara - Piura 2019.* (Tesis de pregrado, Universidad Cesar Vallejo, Piura, Perú). https://repositorio.ucv.edu.pe/handle/20.500.12692/55806

Arevalo, F., Ordoñez, I., Peñaherrera, M. y Suarez, V. (2020) Importancia de la seguridad de los sistemas de información frente el abuso, error y hurto de

información. *Revista Ciencia de la computación, 6(*2), 835-846. https://dialnet.unirioja.es/descarga/articulo/7425694.pdf

Urpeque, C. (2019). *Análisis de la adecuación de la Ley N°30096, al marco del convenio internacional de Budapest 2001, y su incidencia en la reducción de los delitos informáticos. Huaura 2018* (Tesis de pregrado, Universidad Nacional José Faustino Sánchez Carrión, Huacho, Perú). http://repositorio.unjfsc.edu.pe/handle/UNJFSC/4632

Ormache, J. (2019). *Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional* (Tesis de posgrado, Centro de Altos Estudios Nacionales, Lima, Perú). https://renati.sunedu.gob.pe/handle/sunedu/1336266

Montaño, R. (2019). *La tipificación penal del phishing, como medida de seguridad informática para contener delitos informáticos* (Tesis de grado, Universidad Mayor de San Andres, La Paz, Bolivia). http://200.7.168.217/biblioteca/wp-content/uploads/2021/03/T-5570.pdf

Bernal, T., Guerrero, C., Gomez, M. P. y Useche, V. (2019). *Curso de especial interés - perfilación criminal aplicada a la investigación del delito violento.* (Tesis de grado, Universidad Católica, Bogotá, Colombia) https://repository.ucatolica.edu.co/handle/10983/23991

Medina, F. (2018). *Seguridad Informática: virus ransomware, el Secuestro virtual de datos es Posible.* (Tesis de grado, Universidad Empresarial, Cordova, Argentina) https://repositorio.uesiglo21.edu.ar/handle/ues21/13925

Ñaupas, P. H., Valdivia, D. M., Palacios, V. J., Romero, D. H. (2018) *Metodología de la Investigación cuantitativa – cualitativa y Redacción de la Tesis.* (5ª ed.). Bogotá: Ediciones de la U.https://corladancash.com/wp-content/uploads/2020/01/Metodologia-de-la-inv-cuanti-y-cuali-Humberto-Naupas-Paitan.pdf

Yucra, S. (2018). *Los factores principales que impiden la aplicación de la ley n°30171- lima norte en el año 2016* (Tesis de pregrado, Universidad Cesar

Vallejo, Lima, Perú). https://repositorio.ucv.edu.pe/handle/20.500.12692/20714

Cotrina, S. (2018). *Los factores principales que impiden la aplicación de la Ley N°30171- Lima Norte en el año 2016* (Tesis de pregrado, Universidad Cesar Vallejo, Lima, Perú). https://repositorio.ucv.edu.pe/handle/20.500.12692/20714

Beermann, K. L. (2018*). La problemática de la interceptación informática en Panamá* (Tesis de pregrado, Universidad de Panamá, Panamá). http://up-rid.up.ac.pa/1683/1/kurt%20beermann.pdf

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

Montoya. F, (2018). *Regulación expresa del delito informático de clonación de tarjetas - sede Divindat, 2017* (Tesis de pregrado, Universidad Cesar Vallejo, Lima, Perú). https://cutt.ly/dTMj2pM

Pardo. A, (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018 (*Tesis de postgrado, Universidad Cesar Vallejo, Lima, Perú). https://repositorio.ucv.edu.pe/handle/20.500.12692/20372

Carrillo, C. y Montenegro, D. (2018). *La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos* (Tesis de pregrado, Universidad Señor de Sipan, Pimentel, Perú). https://repositorio.uss.edu.pe/handle/20.500.12802/4514

Montaperto, (2018). *Un análisis sobre su falta de regulación en el ordenamiento jurídico argentino* (Tesis de pregrado, Universidad Siglo 21, argentino) https://repositorio.uesiglo21.edu.ar/handle/ues21/15652

Posada, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad 2017. *La responsabilidad penal por el hecho colectivo. Aspectos de derecho chileno y comparado* https://dialnet.unirioja.es/metricas/documentos/ARTREV/6074006

Espinoza. M (2017). *Derecho penal informático: Deslegitimación del poder punitivo en la sociedad de control* (Tesis de pregrado, Universidad Nacional del Antiplano Puno, Puno, Perú). http://repositorio.unap.edu.pe/handle/UNAP/6309

Gallardo, E. E. (2017). *Metodología de la Investigación.* Universidad Continental.

Alarcon, 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.* (Tesis de postgrado, Universidad Norbert Wiener, Lima, Perú). http://repositorio.uwiener.edu.pe/handle/123456789/1630

Ministerio del Interior (2016). *Ciberpolicias contra delitos informáticos*. Publicado el 27 de abril de 2017. https://www.mininter.gob.pe/content/ciberpolic%C3%AD-contra-delitos-inform%C3%A1ticos

Costa, M. y Ruiz, C. (2016). *Análisis de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos* (Tesis de grado, Universidad Nacional de Loja, Loja, Ecuador). https://dspace.unl.edu.ec/jspui/handle/123456789/17916

Bruno, N. (2016). *La evolución tecnológica utilizada como medio delictivo y su legislación vigente* (Tesis de grado, Universidad Empresarial Siglo 21, Buenos Aires, Argentina). https://repositorio.uesiglo21.edu.ar/handle/ues21/14340

Ribero, S. (2016*). Delitos informáticos y su legislación en el contexto colombiano. retos sociales y tecnológicos* (Tesis de grado, Universidad Autónoma de Bucaramanga – UNAB, Bucaramanga, Colombia). http://hdl.handle.net/20.500.12749/1305

Muñoz, C. I. (2016). *Metodológica de la investigación.* Editorial OXFORD.

Morales. D, (2016). *La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el perú-2015*

(Tesis de pregrado, Universidad Señor de Sipan, Pimentel, Perú). https://repositorio.uss.edu.pe/handle/20.500.12802/3161

Aguirre, O. y Sevillano, J. (2015). *Desafíos a enfrentar en la aplicación de leyes sobre delitos informáticos en El Salvador* (Tesis de grado, Universidad Bosco, San Salvador, El Salvador). http://rd.udb.edu.sv:8080/jspui/handle/11715/958

Chinchon. J. (2014). Impunidad, sistema de Justicia, estado de Derecho y democracia. ¿Es peor la impunidad que el crimen en sí mismo? *Espacio Abierto-Revista del Centro de Investigación y Estudios Judiciales* (20), 18-22. https://core.ac.uk/download/pdf/33100204.pdf

Hernández. R, (2014). *Metodología de la investigación.* Editorial McGraw-Hill Interamericana.

Hugo, S. (2014). Tipificación de los delitos informáticos patrimoniales en la nueva ley de delitos informáticos N° 30096. Revista UNMSM, 69-80.https://revistasinvestigacion.unmsm.edu.pe/index.php/alma/article/view/11870/10592

Perú, Ley 30171 de 2014. Ley que modifica la Ley 30096, Ley de Delitos Informáticos. Febrero 17 de 2014. 1059231-2

Perú, Ley 30096 de 2013. Ley de Delito Informáticos. Setiembre 27 de 2013.1003117-1

Suarez, M.E. (2007). El saber pedagógico de los profesores de la Universidad de los Andes Tachira y sus implicaciones en la enseñanza. *UNIVERSITAT ROVIRA I VIRGILI*, 645-654. https://tdx.cat/bitstream/handle/10803/8922/10CapituloXElcaracterCientificodelainvestigaciontfc.pdf?sequence=3&isAllowed=y

Mamani, R. (2007). *La tipificación del daño o sabotaje informático para la protección de la industria y el comercio en Bolivia (*Tesis de pregrado, Universidad Mayor de San Andrés, La Paz, Bolivia). http://repositorio.umsa.bo/xmlui/handle/123456789/18935

Acuerdo Plenario 7-2006/CJ-116. (2006, 13 de octubre). Corte Suprema de Justicia de la Republica. https://www.pj.gob.pe/wps/wcm/connect/CorteSuprema/s_cortes_suprema_home/as_poder_judicial/as_corte_suprema/as_salas_supremas/as_sala_penal_permanente/as_acuerdos_plenarios_y_sentencias_vinculantes_spp/as_acuerdos_plenarios/as_2006/

Convenio de Ciberdelincuencia de Budapest. (2001). Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Acurio, S. (s.f). Delitos Informáticos: Generalidades. http://148.202.167.116:8080/xmlui/handle/123456789/599

Davila, P. (s.f) Software y Hardware https://www.buenastareas.com/ensayos/Software-y-Hardware/38909173.html

Ministerio Publico. (s.f) ¿Quiénes somos? Defensores de la Legalidad. https://www.mpfn.gob.pe/?K=138

Poder Judicial. (s.f) ¿Qué es el Poder Judicial? https://www.pj.gob.pe/wps/wcm/connect/CorteSupremaPJ/s_Corte_Suprema/as_Conocenos/definiciones

Estrada, R. y Somellera, R. (s.f). *Delitos Informáticos.* Editorial Informática y Derecho.

Acurio. S, (s/f). Delitos informáticos: Generalidades. Editorial Astrea. http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/599

ANEXOS

Anexo A

Tabla 3

Matriz de categorización

Titulo	Problema de Investigación	Preguntas de la Investigación	Objetivo General	Objetivos Específicos	Categorías	Sub categorías
Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19	¿La actuación de las entidades persecutoras de los delitos informáticos fueron las adecuadas durante pandemia por covid-19?	¿los delitos informáticos incrementaron durante la pandemia por covid-19?	Determinar la actuación de las entidades persecutoras de los delitos informáticos fueron las adecuadas durante pandemia por covid-19	Explicar porque los delitos informáticos incrementaron durante la pandemia por covid-19.	Entidades persecutoras	Administración de Justicia Cuerpos normativos Fraude informático
		¿Cuáles son las entidades persecutoras de los delitos informáticos creados por el Estado?		Identificar cuáles son las entidades persecutoras de los delitos informáticos creadas por el Estado.	Delitos Informáticos	Suplantación de identidad

Anexo B

DECLARACIÓN DE CONSENTIMIENTO INFORMADO

Por medio del presente documento confirmo mi consentimiento para participar en la investigación denominada: **“Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19”**

Se me ha explicado que mi participación consistirá en lo siguiente:

Entiendo que debo responder con la verdad y que la información que brindan mis compañeros también es confidencial.

Se me ha explicado también que si decido participar en la investigación puedo retirarme en cualquier momento o no participar en una parte del estudio.

Acepto voluntariamente participar en esta investigación y comprendo qué cosas voy a hacer durante la misma.

18 de mayo del 2022

Nombre del participante:

DNI:

Investigadora

Diana Dolores Quispe Vara

DNI: 48252678

Investigador

Joseph Alexander Martel Melgarejo

DNI: 75648664

Anexo B

DECLARACIÓN DE CONSENTIMIENTO INFORMADO

Por medio del presente documento confirmo mi consentimiento para participar en la investigación denominada: **"Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19"**

Se me ha explicado que mi participación consistirá en lo siguiente:

Entiendo que debo responder con la verdad y que la información que brindan mis compañeros también es confidencial.

Se me ha explicado también que si decido participar en la investigación puedo retirarme en cualquier momento o no participar en una parte del estudio.

Acepto voluntariamente participar en esta investigación y comprendo qué cosas voy a hacer durante la misma.

Lima, 18 de mayo del 2022

Nombre del participante: Jorge Luis Venegas Rivera

DNI: 45565807

Cargo: Fiscal Adjunto Provincial Ministerio Público

JORGE LUIS VENEGAS RIVERA
FISCAL ADJUNTO PROVINCIAL
FISCALIA PROVINCIAL CORPORATIVA ESPECIALIZADA
EN CIBERDELINCUENCIA DE LIMA - PRIMER DESPACHO

FIRMA

Investigadora
Diana Dolores Quispe Vara
DNI: 48252678

Investigador
Joseph Alexander Martel Melgarejo
DNI: 75648664

Anexo B

DECLARACIÓN DE CONSENTIMIENTO INFORMADO

Por medio del presente documento confirmo mi consentimiento para participar en la investigación denominada: **"Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19"**

Se me ha explicado que mi participación consistirá en lo siguiente:

Entiendo que debo responder con la verdad y que la información que brindan mis compañeros también es confidencial.

Se me ha explicado también que si decido participar en la investigación puedo retirarme en cualquier momento o no participar en una parte del estudio.

Acepto voluntariamente participar en esta investigación y comprendo qué cosas voy a hacer durante la misma.

Lima, 13 de mayo del 2022

Nombre del participante: Moisés Fernández Benites (Contratado)

DNI: 40085263

CARGO: Fiscal Provincial

FIRMA

Investigadora

Diana Dolores Quispe Vara

DNI: 48252678

Investigador

Joseph Alexander Martel Melgarejo

DNI: 75648664

Anexo B

DECLARACIÓN DE CONSENTIMIENTO INFORMADO

Por medio del presente documento confirmo mi consentimiento para participar en la investigación denominada: **“Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19”**

Se me ha explicado que mi participación consistirá en lo siguiente:

Entiendo que debo responder con la verdad y que la información que brindan mis compañeros también es confidencial.

Se me ha explicado también que si decido participar en la investigación puedo retirarme en cualquier momento o no participar en una parte del estudio.

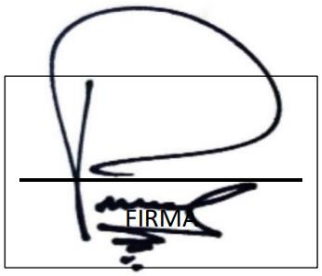
Acepto voluntariamente participar en esta investigación y comprendo qué cosas voy a hacer durante la misma.

Lima, 12 de mayo del 2022

Nombre del participante: Wuilman Zabarburu Vargas

DNI: 40072448

CIP: 31298388



Investigadora

Diana Dolores Quispe Vara

DNI: 48252678

Investigador

Joseph Alexander Martel Melgarejo

DNI: 75648664

Anexo B

DECLARACIÓN DE CONSENTIMIENTO INFORMADO

Por medio del presente documento confirmo mi consentimiento para participar en la investigación denominada: **“Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19”**

Se me ha explicado que mi participación consistirá en lo siguiente:

Entiendo que debo responder con la verdad y que la información que brindan mis compañeros también es confidencial.

Se me ha explicado también que si decido participar en la investigación puedo retirarme en cualquier momento o no participar en una parte del estudio.

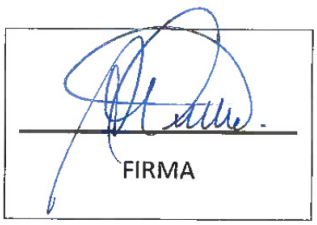
Acepto voluntariamente participar en esta investigación y comprendo qué cosas voy a hacer durante la misma.

Lima, 17 de mayo del 2022

Nombre del participante: Rogers Vicentico Arbulú Valdez

DNI: 40443599

Cargo: Fiscal adjunto provincial



Investigadora

Diana Dolores Quispe Vara

DNI: 48252678

Investigador

Joseph Alexander Martel Melgarejo

DNI: 75648664

ANEXO C

FICHA DE ENTREVISTA 1

Dirigido a especialistas, abogados titulados, colegiados que ejercen la profesión y son expertos en relación a derecho penal, civil, constitucional, especialista Psicólogos y efectivo policial.

Título: Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19

Nombre del entrevistado: Asenet Scarlett Muro Delgado

Código de la entrevista: ASMD1

Sexo: Femenino

Ocupación: Abogada particular

Fecha de entrevista:

Entrevistadores: Joseph Alexander Martel Melgarejo y Diana Dolores Quispe Vara

Cuestionario

1. **¿Cuáles son las entidades persecutoras encargadas de hacerle frente a los delitos informáticos en el Perú?**
   Las entidades persecutoras encargadas de hacerle frente a los delitos informáticos en nuestro país son el Ministerio Público y la Policía Nacional del Perú.

2. **En su opinión, ¿considera usted que el sistema de administración de justicia actual ha evolucionado a fin de frenar los delitos informáticos?**
   Si, ya que nuestro sistema de administración de justicia actualmente se preocupa y busca realizar cambios innovadores para contrarrestar el alto índice de delitos informáticos perpetrados en el Perú, muestra de ello es la creación de leyes, divisiones especiales tales como la DIVINDAT encargada de verificar estos ilícitos y la creación de fiscalías especializadas en Ciberdelincuencia que opera a nivel Nacional los cuales son encargadas de ser persecutoras de estos delitos.

3. **¿Conoce los cuerpos normativos vigentes que regulan los delitos informáticos en el Perú?**

   Sí, hay una la ley especial la ley N°30096 ley de delitos informáticos y su modificatoria la ley N°30171 la cual modifica artículos de la ley 30096 ley de delitos informáticos.

4. **¿Cómo es el procedimiento de la individualización del sujeto activo en los delitos informáticos?**

   Bueno en el caso de los delitos informáticos y a diferencia de los delitos comunes, en este caso el sujeto activo es quien posee unas ciertas habilidades o características especiales y estas habilidades que son el manejo de los sistemas informáticos para que así con ello puedan realizar el manejo del sistema y cometer estos actos ilícitos logrando evitar ser descubiertos, por lo que en la mayoría de los casos no se puede lograr identificar al sujeto activo de estos delitos, por lo que los casos fiscales son archivados, no obstante en la ley especial se aplican mecanismos para individualizar al sujeto activo, con la tipicidad y todo ello y también con las fiscalías especializadas en ciberdelincuencia las cuales realizan una ardua labor ya que ellos cuentan con implementos tecnológicos avanzados, para así poder identificar a los sujetos activos pero no lo obtienen de manera sencilla.

5. **A su experticia ¿Cuándo podemos hablar que se ha configurado el delito de Fraude informático?**

   Con respecto al delito de Fraude informático como figura en la ley especial, establece que estos delitos se configuran cuando el sujeto activo empleando los medios electrónicos realiza la manipulación de sistemas informáticos con que o para qué, pero tienen su finalidad, la finalidad que ellos tienen es obtener algún provecho ilícito en perjuicio de un tercero, por ello se dice que son delitos patrimoniales por lo que se afecta el patrimonio del sujeto pasivo mediante el empleo malicioso de tecnología.

6. **Para usted, ¿a qué se debe el incremento de los delitos informáticos en Pandemia?**

   Bueno debido a la pandemia y al contexto actual en el que nos encontramos del cual la población de manera general se encuentra manipulando en todo momento los servicios electrónicos para así adquirir servicios, vender productos y realizarlos estos a través de internet e incluso transferimos nuestra información personal, nuestros datos, entre otras actividades cotidianas que realizamos, entonces esto hace que nosotros nos veamos expuestos y vulnerables a ser víctimas de estos tipos de ilícitos porque los sujetos activos a través de la manipulación del sistema informático lo que hacen es tener acceso a nuestros datos y con ello realizar estafas, suplantaciones de identidad, entre otros ilícitos.

ANEXO C

FICHA DE ENTREVISTA 2

Dirigido a especialistas, abogados titulados, colegiados que ejercen la profesión y son expertos en relación a derecho penal, civil, constitucional, especialista Psicólogos y efectivo policial.

Título: Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19

Nombre del entrevistado: Moises Fernandez Benites
Código de la entrevista: MFB2
Sexo: Masculino
Ocupación: Fiscal Provincial de la Primera Fiscalía Penal Corporativa de la Victoria San Luis – Primer Despacho
Fecha de entrevista: 13 de mayo del 2022
Entrevistadores: Joseph Alexander Martel Melgarejo y Diana Dolores Quispe Vara

Cuestionario

1. **¿Cuáles son las entidades persecutoras encargadas de hacerle frente a los delitos informáticos en el Perú?**
   Bueno en líneas generales la investigación del delito siempre va recaer en el ministerio público por ende independientemente de que delito se presente investigar, la legitimidad siempre va a recaer en el ministerio público, ahora esta labor se requiere de un apoyo técnico por así decirlo en estos casos por tratarse de delitos informáticos, lo llevan o lo realizan la división de delitos de alta tecnología, en la practica la investigación podría realizarla esta división policial, sin embargo la legitimidad o la titularidad de la investigación va a recaer siempre en el Ministerio Público, en ese entendido lógicamente cuando se tiene una ocurrencia delictiva de esa naturaleza el ministerio publico dirige la investigación y decidirá si un caso concreto lo realiza de manera directa o a través de la división especializada antes mencionada, ya como parte final, para precisar que desde el 15 de junio del 2021, existen ya fiscalías especializadas en ciberdelincuencia cuya competencia territorial es

estrictamente al distrito fiscal de lima o lima centro como un hecho delictivo de esta naturaleza lo conoce las fiscalías especializadas que te he precisado, si ocurre por ejemplo en lima norte o en lima sur, o en cualquier otro distrito del Perú, lo va a conocer una fiscalía común, una fiscalía penal común, yo creo que la división de delitos de alta tecnología está centralizada en lima, a nivel de provincias, entiendo que el fiscal decidirá si lo hace una comisaría o una DEPINCRI.

2. **En su opinión, ¿considera usted que el sistema de administración de justicia actual ha evolucionado a fin de frenar los delitos informáticos?**
   Si, sin duda, una cuestión palpable es la creación de fiscalías especializadas en donde se entiende que el personal fiscal que labora allí y también el administrativo, llevan la capacidad y una participación permanente para afrontar este tipo de hechos delictivos, los delitos en ciberdelincuencia como su propio termino lo dice se cometen a través de uso de los medios tecnológicos y estos cada vez son o evolucionan, entonces, si la delincuencia por así decirlo evoluciona, lógicamente el Estado tiene que dar una respuesta a la par de esos avances en los cuales se realiza la delincuencia, entonces, definitivamente si ha habido un avance a través de la creación de fiscalías especializadas, mecanismos de incorporación interna para lograr identificar o acceder a unas páginas que se puedan crear para cometer este tipo de delitos y respecto al Poder Judicial, me parece que no existe un juzgado especializado en esa materia, sin embargo en virtudes a los elementos que le pueda aportar el Ministerio Público, perfectamente la adjudicatura puede dar una respuesta inmediata al planteamiento que realiza el fiscal, en conclusión si considero que ha habido una evolución no a la par del avance de la delincuencia en estos tipos de delitos, pero creo que se están haciendo esfuerzos para afrontar este tipo de delitos.

3. **¿Conoce los cuerpos normativos vigentes que regulan los delitos informáticos en el Perú?**
   Estos tipos de ley también han sufrido una evolución, porque la ley de los delitos informáticos que es la 30096 ha sufrido o es consecuencia de una

evolución porque si analizamos esta ley advertimos que existen determinados tipos penales que implican una afectación de ciertos bienes jurídicos que pueden ser tutelados por otros delitos, por ejemplo contra la fe pública, contra el bien patrimonial, pero al advertirse que durante el ínterin o durante el desarrollo de estos tipos de delitos, se recurría a medios informáticos o medios tecnológicos que eran necesarios establecer el tipo penal independiente, precisamente para analizar la estructura del tipo, establecer una conducta especifica que implicaba el uso de estos medios para cometer estos tipos de delitos y también una sanción que corresponde que es distinta por ejemplo a que un delito informático en la cual se logra sustraer un patrimonio es distinto dentro del hurto porque los medios empleados hacen que el hecho sea más grave y por ende requieran de una mayor sanción, en resumen, la ley que rige estos delitos es la ley 30096 y establece los tipos penales que configuran lo que se llama delitos informáticos.

4. **¿Cómo es el procedimiento de la individualización del sujeto activo en los delitos informáticos?**

   La estrategia de investigación va a depender del tipo de delito en particular que se cometa, por ejemplo si es un delito informático denominado contra datos y sistemas informáticos va a depender de cuál ha sido la modalidad especifica en la cual el autor ha concretado este ilícito, si por ejemplo se ha querido acceder de manera ilegal a un sistema informático es probable que hayan dejado huellas del delito y esto posibilitaría la identificación del autor, en realidad es una labor muy complicada como se hace el empleo de los medios tecnológicos en delitos informáticos normalmente en la realidad para la generalidad de estos delitos, por ejemplo la suplantación de identidad, se suele emplear cabinas, bueno ya no hay tantos como ahora lo que se usaba eran las cabinas de internet, a través del rastreo de IP podemos identificar por ejemplo de que PC habría cometido este delito, podemos identificar que PC por ejemplo, pero no vamos a poder vincular cual sería la persona que ha empleado o utilizado, si es una cabina propiamente pero es probable que existan videos donde registren la fluencia del público, algunos lugares que

quizás no tengan control efectivo de ello y anotan en cuaderno que supuestamente le dictan la persona que estará usando esa cabina pero en realidad es un poco difícil determinar cuál sería el autor en este caso en específico, va depender de tipo de delitos, cuando es contra el patrimonio, normalmente se señala una cuenta de destino a través de la cual te hacen una transferencia ilegal aquí por ejemplo es mucho más factible y que tenemos una cuenta bancaria que se puede identificar a través del sistema bancario en el cual se sabe del titular de la cuenta o impresión de Boucher o de repente levantar el secreto bancario, eso puede ser por ejemplo una forma para poder identificar, normalmente suelen emplear WhatsApp la o llamadas telefónicas y una posibilidad es oficiar a Osiptel o levantar el secreto de las comunicaciones para poder determinar a quién le correspondería ese número, pero luego se presentan problemas, porque luego aparece la persona que se presenta como titular de la línea normalmente use ese número, por ende, en realidad es un poco complicado, pero esas son las estrategias o mecanismos que podemos emplear para identificar a estos autores de estos ilícitos, en resumidas cuentas, la estrategia va a depender del tipo de delito realizado, la información que se puede recabar, cuáles son los obstáculos si cabe el término que se nos enfrenta para poder lograr el objetivo que es identificar al autor de estos ilícitos, es una labor muy complicada en realidad pero hay casos en los que si hay una cierta información por ejemplo el número telefónico, cuenta bancaria, una dirección, el uso de una PC de repente que no sea una cabina, sino un determinado inmueble, estos mecanismos podrían determinar o ubicar al autor de los hechos en estos tipos de delitos. En los delitos de suplantación de identidad, por ejemplo tienes un Facebook o una red social, se crea una página quizás con tu mismo perfil, sin embargo es complicado poder determinar cómo, quien y donde creo esta página falsa o haya suplantado la identidad, la dificultad que existe es que la información de la creación de una página en Facebook esta requiere un acto de cooperación internacional, solicitarlo directamente en concreto a la página oficial de Facebook en el cual al hacer una citación judicial para EE.UU es una complejidad porque en principio elaborar una sentencia judicial implica

recorrer un camino interno de estado a estado, existe el Ministerio Público y existe una unidad de cooperación internacional de extradiciones, el cual se encarga de las operaciones judiciales y el fiscal que se encarga de ello, solicita a EE.UU nos puedan dar información respecto a quien habría creado, donde habría creado un perfil falso por así decirlo, la unidad de cooperación tiene que traducir esa solicitud al idioma del que estamos requiriendo luego mandarlo a cancillería y luego lo mandan a la embajada de Perú en EE.UU o la unidad central de EE.UU para que canalicen esta solicitud y te estoy hablando de tiempo transcurrido de un año, y a veces el juez de EE.UU y el juez mayormente te dice que eso es información reservada, logrando pasar un año y medio para lo cual contamos con plazo de 120 días, por más que lo declares complejo no vas a llegar a buen puerto, hay una realidad una serie de dificultades que imposibilitan que este tipo de delitos podamos identificar quien habría suplantado la identidad, finalmente vamos a llegar a saber dónde de que PC tal vez, pero ya cuando necesitamos hacer un allanamiento o verificar una computadora, todo está completamente borrado o ha sido indispuesto, es complicado en estos tipos de delitos determinar quién ha sido o seria la persona que habría suplantado la identidad a través del uso de tecnología de la información, es lo que te podría decir que es lo más complicado.

5. **A su experticia ¿Cuándo podemos hablar que se ha configurado el delito de Fraude informático?**

   Podemos hablar de fraude informático, todo delito tiene una estructura básica que es la tipicidad, antijuricidad y el injusto penal que es la culpabilidad pero se va a configurar en la medida que el agente concrete las acciones o los verbos rectores que establecen en concreto el artículo 8 de la Ley 30096, el cual prescribe el que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de un tercero, mediante el diseño e introducción, borrado, supresión, de datos informáticos o cualquier interferencia o manipulación en el sistema informático, esta es la estructura del tipo penal, lógicamente estos delitos que yo considero que son delitos de resultado en el cual necesariamente tiene que producirse un perjuicio

patrimonial, esto es, por ejemplo el agente únicamente altera, borra o suprime o clona un dato informático, pero, no obtiene un provecho ilícito, estaríamos ante un delito en grado de tentativa, si la pregunta concreta es cuando se configura, se configura cuando se logra un beneficio ilícito y en tanto para dicho propósito se vean empleados como medios lo que es alteración borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación de manejos de sistemas informáticos, estos son los mecanismos o medios no, es un poco lo que se distingue lo que es un fraude informático propiamente hablando de por ejemplo de que podría existir una sustracción de dinero, por ejemplo no, Joseph te entrega tu tarjeta Multired te da la clave y tú vas al cajero retiras el dinero, entonces hay por ejemplo aparentemente podría decirse que ha habido un tema de fraude informático sin embargo lo dado es un acto de sustracción porque tu no has alterado borrado o suprimido, ni clonado un dato informático, simplemente has usado un cajero electrónico, pero has sustraído un dinero entonces es lo que se distingue por ejemplo de lo que es un hurto de lo que es un fraude informático propiamente dicho, esto es lo que distingue la acción o el tipo penal es el empleo de medios tecnológicos de los cuales mediante alteración, supresión o alteración se logran estos delitos informáticos.

6. **Para usted, ¿a qué se debe el incremento de los delitos informáticos en Pandemia?**

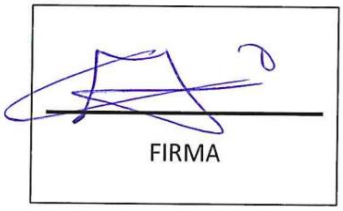
Bueno la pandemia nos ha servido para muchas cosas, entre ellos el empleo de medios tecnológicos o informáticos, para todo, podemos estar encerrados y no podíamos salir a comprar, no podíamos pedir un delivery o incluso los programas sociales que se crearon a través de los bonos que dio el gobierno, requerían no de una si cabe el termino, una cierta tecnología o cierto conocimiento informático en el que los beneficiarios tenían que registrar un número telefónico y acudir a un agente que se le enviaba una clave al celular y ellos podrían hacer retiro del dinero, entonces, toda esta digitalización de los procesos de consumo, de las compras, e incluso de la obtención de beneficios, implica el empleo de sistemas informáticos, entonces si por así decirlo es como que tienes en la nube dinero que está volando, sea a través

de una compra a través de un pago o una transferencia o tal vez de la obtención de un bono, así es donde entran ellos porque ven como que se dice una abundancia de dinero en las redes que les permite a ellos a través del empleo de estos medios fraudulentos informáticos, lograr mayores beneficios, entonces, hay denuncias de compras falsas, de llamadas falsas, de retiro de bonos, una serie de hechos que obviamente tienen como explicación el hecho de que durante la pandemia se haiga usado en demasía los sistemas informáticos, entonces yo considero que esa es una de las explicaciones en la que de alguna manera nos dan o nos revelan que porque se ha incrementado estos tipos de delitos durante la inmovilización obligatoria.

Nombre del participante: Moisés Fernández Benites (Contrastado)

DNI: 40085263

CARGO: Fiscal Provincial



ANEXO C

FICHA DE ENTREVISTA 3

Dirigido a especialistas, abogados titulados, colegiados que ejercen la profesión y son expertos en relación a derecho penal, civil, constitucional, especialista Psicólogos y efectivo policial.

Título: Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19

Nombre del entrevistado: Rogers Vicentico Arbulu Valdez
Código de la entrevista: RVAV3
Sexo: Masculino
Ocupación: Fiscal Adjunto de la Sexta Fiscalia Cooperativa Penal de Cercado de Lima - Breña – Rimac – Jesus Maria – Tercer Despacho
Fecha de entrevista: 17 de mayo del 2022
Entrevistadores: Joseph Alexander Martel Melgarejo y Diana Dolores Quispe Vara

Cuestionario

1. **¿Cuáles son las entidades persecutoras encargadas de hacerle frente a los delitos informáticos en el Perú?**
   En el País tenemos un grupo interinstitucional el cual está a cargo de la lucha contra estos delitos, como el Ministerio Público, Poder judicial y la Policía Nacional y Organismos Privados, en este caso la policía cuenta con una división o unidad especializada, denominada división de investigación de delitos de alta tecnología la cual es el responsable de prevenir, combatir, investigar y denunciar bajo la dirección jurídica del fiscal cometidos por delincuentes comunes u organizaciones criminales en todo el país.

2. **En su opinión, ¿considera usted que el sistema de administración de justicia actual ha evolucionado a fin de frenar los delitos informáticos?**
   Totalmente, hasta hace dos años no contábamos con lo que ahora se llama la fiscalía especializada en ciberdelincuencia o delitos informáticos, el Ministerio Público pues como entidad titular de la acción penal, a fin de crear

condiciones o climas para una adecuada lucha contra la ciberdelincuencia a través de las resoluciones de la Fiscalía de la Nación 1503-2020-MP-FN del 30 de diciembre del 2020, creo la unidad fiscal especializada en ciberdelincuencia del ministerio público, con competencia nacional, la cual se encarga justamente de la lucha contra todos los delitos de ciberdelincuencia que existen actualmente, de la mano con las unidades especializadas de la policía nacional, del poder judicial y otros organismos nacionales privados.

3. **¿Conoce los cuerpos normativos vigentes que regulan los delitos informáticos en el Perú?**

   Para hablar del país tenemos que hablar en principio de la legislación internacional, el país se encuentra adherido al convenio de ciberdelincuencia del convenio de Budapest del 2001, para la cooperación de los estados miembros en cuanto a la lucha contra la ciberdelincuencia, dentro de nuestra legislación nacional, tenemos la ley 30096, Ley de delitos informáticos se promulgo el 21 de octubre del 2013 y que fue modificada por la 30171 del 17 de febrero del 2014 donde se enumeran y detallan los diferentes tipos penales dependiendo también del bien jurídico que protege, contra la ciberdelincuencia.

4. **¿Cómo es el procedimiento de la individualización del sujeto activo en los delitos informáticos?**

   Como bien saben dentro del Ministerio Publico, cuando tenemos conocimiento de la noticia criminal o la denuncia de parte dependiendo de cómo obtengamos, como llegan esta denuncia al Ministerio Público, se abre pues una investigación preliminar con la apertura de investigación preliminar el donde se revisan todos los actos de investigación urgente, en etapa preliminar y en etapa preparatoria, dependiendo si logramos individualizar a los presuntos procesados o presuntos responsables, con el fin de determinar su participación dentro del delito que se le está imputando, esto con colaboración como bien habíamos dicho de las instituciones como en este caso la policía Nacional, la cual definitivamente a través de la división de alta

tecnología, nos brinda todas las herramientas para poder hacer la ubicación respectiva, dependiendo en este caso dependiendo del tipo del delito, dependiendo también la ubicación, del software y todo ese tema de tecnología, así que en buena cuenta contamos pues con peritos técnicos estratégicos dentro de nuestro trabajo o del trabajo del área fiscal, en este caso del área especializada, porque yo vengo de delitos comunes, para que así se pueda lograr, obtener las evidencias necesarias para dar con los hechos denunciados y con la responsabilidad de los que estarían inmersos dentro de estos delitos.

5. **A su experticia ¿Cuándo podemos hablar que se ha configurado el delito de Fraude informático?**

   Bueno, el delito de fraude informático está prescrito y sancionado en la Ley de delitos informáticos en la ley 30096, modificada con la ley 30171 donde dice, bueno y justo lo tengo a la mano, textualmente: El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad, me parece no menor de 3 a 8 años, no lo tengo ese dato exactamente pero los verbos rectores son el que procura delibera e ilegítimamente para si un provecho ilícito mediante el diseño, introducción borrado, todo en referencia a lo que es de datos informáticos o interferencia o manipulación en el sistema informático, lo que normalmente podemos observarlo por ejemplo por las compras que se realizan a través de internet, a través de las páginas web o muchas veces los avisos que sacan a través de las redes sociales en donde indican que tipo por ejemplo, préstamos o venta de determinado producto mediante el cual uno utiliza tarjetas de crédito, cuentas claves donde efectivamente pueden manipular o alterar esos datos informáticos para poder hacer provecho ilícito del patrimonio en este caso del agraviado.

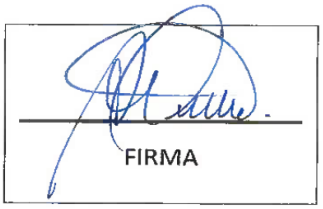
6. **Para usted, ¿a qué se debe el incremento de los delitos informáticos en Pandemia?**

Las redes sociales, bueno las redes sociales y la necesidad de nosotros, del público, de utilizar el internet, efectivamente con la coyuntura sanitaria, en la que nos encontramos aún, pero que provino a raíz del covid-19 en donde tuvimos que quedarnos en casa y en donde surgió una necesidad extrema donde la comunicación se llevara a través del sistema informático, a través del internet, efectivamente estos se normalizo a nivel mundial y volcamos nuestra vida a que todo lo hagamos a través de internet y eso pues desde las reuniones de trabajo o el trabajo mismo como el trabajo remoto hasta también las compras, inscripciones, matriculas en colegios, compras de bienes, etc. Por lo tanto, son mecanismos que han servido también en este caso para los delincuentes no, de vías de acceso para que puedan obtener ellos un fin ilícito en este caso vulnerar el patrimonio de los cibernautas, haciéndolo a través del fraude informático, vulnerando efectivamente datos, alterando nombres, alterando identidades, para que puedan obtener en este caso grandes cantidades de dinero y eso lo podemos ver como algo normal actualmente, vemos denuncias muy comunes en los noticieros, ahora en la mañana justamente estaba viendo en las noticias donde a un jovencito que los ahorros de toda una que será pues cinco años, maso menos sesenta mil soles, a él prácticamente se lo quitaron en cuestión de horas, le robaron el celular y en el celular tenía las aplicaciones de acceso para sus cuentas bancarias, ingresaron a esas cuentas bancarias con el robo del celular y alteraron todos los datos e hicieron transferencias bancarias de las cuentas de este muchacho a la cuenta de los delincuentes y le quitaron prácticamente sesenta mil o setenta mil soles en cuestión de horas, es algo que ni siquiera el propio banco podría o a podido manejar.

Nombre del participante: Rogers Vicentico Arbulú Valdez

DNI: 40443599

Cargo: Fiscal adjunto provincial



ANEXO C

FICHA DE ENTREVISTA 4

Dirigido a especialistas, abogados titulados, colegiados que ejercen la profesión y son expertos en relación a derecho penal, civil, constitucional, especialista Psicólogos y efectivo policial.

Título: Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19

Nombre del entrevistado: Jorge Venegas Rivera
Código de la entrevista: JVR4
Sexo: Masculino
Ocupación: Fiscal Adjunto de la Primera Fiscalía de Ciberdelincuencia de Lima Centro - Primer Despacho
Fecha de entrevista: 18 de mayo del 2022
Entrevistadores: Joseph Alexander Martel Melgarejo y Diana Dolores Quispe Vara

Cuestionario

1. **¿Cuáles son las entidades persecutoras encargadas de hacerle frente a los delitos informáticos en el Perú?**

   El delito informático es un delito que ha tenido un incremento sustancial en la esencial delictiva sobre todo en el distrito fiscal de lima y en realidad en todos los distritos de la ciudad de lima, que actualmente se viene empezando a través de las fiscalías de ciberdelincuencia de lima centro por parte del Ministerio Público esta fiscalía recién se a creado mediante resolución 843-2020 Fiscalía de la Nación por lo cual se inicia funciones a partir del 15 de Junio, sin perjuicio de ello actualmente se viene realizando trabajo en conjunto con la división de investigación de los delitos de alta tecnología de la policía nacional del Perú que es la DIVINDAT por la cual venimos ejecutando diversas acciones para investigar los delitos informáticos y hacer todo un esfuerzo posible para poder judicializar esos casos ante el poder judicial y establecer la responsabilidad penal a los sujetos autores de esa tipicidad delictiva.

2. **En su opinión, ¿considera usted que el sistema de administración de justicia actual ha evolucionado a fin de frenar los delitos informáticos?**
   Los delitos informáticos actualmente se encuentran vistos y regulados en la ley 30096 y su modificatoria de la ley 30171 donde se han previsto hasta diez tipos de delitos encontrándose previos a estos ilícitos, tráfico ilegal de datos, el fraude informático, suplantación de identidad, en el aspecto sustantivo del delito se ha ido recogiendo diversas actuaciones delictivas que se han ido realizando en el extranjero sin embargo en cuanto al ámbito adjetivo esto es en el manejo procesal de estos delitos aún nos falta establecer diversas estrategias toda vez que estos delitos son una modalidad compleja lo que implica el uso de software especializados con los cuales los delincuentes realizan la manipulación de los sistemas informáticos normalmente con las entidades bancarias, las entidades financieras así como las entidades públicas, así como vemos la ONPE, el Jurado nacional de elecciones, hasta el momento que refiere establecer nuevos modelos procesales a efectos de conducir de forma satisfactoria una investigación fiscal, con la cual se pueda establecer la responsabilidad penal de los delincuentes, por ejemplo tenemos el proceso inmediato, en el cual aún no regula en forma específica los delitos informáticos sin embargo, sería factible que a través de una modificación de la ley se pueda prever estos delitos a efectos de poder accionar lo más rápido posible toda vez que se cometen esos delitos, se tiene actualmente una carga procesal que dificulta a las entidades poder hacer una adecuada investigación en torno al caso que se presenta, no, en esa medida pues tenemos que accionar.

3. **¿Conoce los cuerpos normativos vigentes que regulan los delitos informáticos en el Perú?**
   Claro, es la ley 30096, la ley de delitos informáticos y su modificatoria establecida en la ley 30171 que sin perjuicio de ello, muchas veces usted sabrá que algunos elementos normativos de los tipos penales sobre todo en agravio de menores donde se prohíbe y sanciona al sujeto que contacta al sujeto con fines sexuales para recabar de ellos material pornográfico, es importante antes de terminar el contenido de este delito por el cual nosotros

tenemos que unir por ejemplo al Derecho de los tratados internacionales sobre la materia, por ejemplo el tratado internacional de las Naciones Unidas contra la pornografía infantil donde se prescribe que es un material pornográfico, lo que es una conducta sexual explicita donde participe una menor de edad, entonces no basta con conocer la acción los tipos penales previstos en esta ley especial, sino también conocer los diversos tratados que regulan esta materia a efectos de poder contar con estos conocimientos mayor para efectos de poder desarrollar una investigación perfecta debidamente del accionar del Ministerio Público.

4. **¿Cómo es el procedimiento de la individualización del sujeto activo en los delitos informáticos?**

   Este delito es un delito bastante interesante bueno si vale el termino, en la medida que exige que una persona, bueno en la legislación Española lo llaman usurpación de nombre y aquí en Perú se denomina suplantación de identidad lo cual su configuración típica exige que esta suplantación se realiza a través de un medio informático o tecnológico, entonces esto presenta diversas dificultades por ejemplo en un caso de una suplantación de mi persona, en la red social de Facebook donde se crea una cuenta de Facebook con mi nombre, con mi foto de perfil y se empieza a solicitar dinero, entonces yo me entero de ello porque varios familiares han caído en este engaño y han procedido a depositar ciertas sumas de dinero entonces yo voy a la policía nacional del Perú o al ministerio público para que investiguen el hecho, entonces ellos lo que tienen que hacer ahí es básicamente requerir una medida limitativa de derechos, esto es un requerimiento levantamiento del secreto de la comunicaciones ante el poder judicial solicitando los datos del suscriptor y esta cuenta falsa de Perú que se habría creado a mi nombre así como los datos contenidos de tráfico a efectos de frenar las conexiones IP y que permitan establecer la localidad geográfica donde se realizó la conexión y así poder recabar mayores elementos de convicción que sirvan para individualizar al sujeto que suplanto la identidad entonces este elemento normativo, medio tecnológico y el medio informático exige que se realice mayores investigaciones y muchas veces son esas medidas

limitativas de derechos e incluso contactarnos de manera procesal con entidades del extranjero como la empresa Google como otras empresas, programas de internet a nivel mundial lo que exige también es realizar cartas de comunicaciones en idioma inglés, también en idioma chino, que son los mayores incidencias, de eso exige todo un trabajo de estrategia y conocer cuáles son los medios informáticos y cuáles son las posibilidades fácticas que nosotros contamos para poder identificar al autor en estos tipos de delitos.

5. **A su experticia ¿Cuándo podemos hablar que se ha configurado el delito de Fraude informático?**

   El delito de fraude informático está en el artículo 8vo de la ley 30096 que básicamente es un delito que exigen la manipulación de una concepción genérica de un sistema informático de un determinado sistema informático que puede ser generalmente la banda por internet de una entidad financiera, puede ser también un Yape, puede ser también un Plin de donde se logre sustraer dinero, fondos económicos por parte del sujeto agraviado, en esa medida muchas veces pasa de que el dinero nunca logro llegar al destino porque el agraviado se dio cuenta del hecho, interpuso la denuncia al banco, congelaron la transacción y se produce el extorno del dinero que habría sido transferido, entonces hay cabe preguntarse si estamos ante un fraude informático consumado o un fraude informático en tentativa, lo que pasa es que el tipo penal exige la perpetración de este perjuicio económico porque se encuentra previsto en el tipo penal, para que podamos hablar de configuración material de este delito, y en esa medida no basta no solo con la manipulación del sistema informático en términos genéricos, para hablar que el delito de fraude informático se encuentre consumado en el sentido estricto sino que exige también el perjuicio económico llegue a consumarse, llegue a materializarse a la luz de las pruebas recabadas, a la luz de los elementos de convicción recabados para poder hablar así la configuración de este delito.

6. **Para usted, ¿a qué se debe el incremento de los delitos informáticos en Pandemia?**

Bueno la pandemia por lógica lo que ha hecho es que las personas no puedan salir de sus casas, y esto a hecho de que los que realizan actividades ilícitas e irregulares, como han tenido los delincuentes que desarrollar nuevas formas de poder seguir cometiendo sus se podría decir sus crímenes y es por eso que han empezado a buscar nuevas formas, entre ellas pues lo que es la manipulación de cuentas bancarias, las suplantaciones de identidad a través de las redes sociales y todas las formas y los modos de como la vida se ha ido desarrollando en este estado de emergencia es que se ha visto infectadas este tipo de actividades, generalmente habíamos estado haciendo comercio presencial sino comercio electrónico y este ha sido un incidente fundamental para que se incremente los delitos informáticos al llegar al primer puesto a nivel de delitos de incidencias en la ciudad de Lima y en otras partes del País, como Trujillo,, Chiclayo, Piura, estamos haciendo todo lo posible pues para poder enfrentar esta nueva modalidad de criminalidad.

JORGE LUIS VENEGAS RIVERA
FISCAL ADJUNTO PROVINCIAL
FISCALIA PROVINCIAL CORPORATIVA ESPECIALIZADA
EN CIBERDELINCUENCIA DE LIMA - PRIMER DESPACHO

FIRMA

ANEXO C

FICHA DE ENTREVISTA 5

Dirigido a especialistas, abogados titulados, colegiados que ejercen la profesión y son expertos en relación a derecho penal, civil, constitucional, especialista Psicólogos y efectivo policial.

Título: Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19

Nombre del entrevistado: Wuilman Zabarburu Vargas
Código de la entrevista: WZV5
Sexo: Masculino
Ocupación: Analista Informático Forense - DIVINDAT
Fecha de entrevista: 12 de mayo del 2022
Entrevistadores: Joseph Alexander Martel Melgarejo y Diana Dolores Quispe Vara

Cuestionario

1. **¿Cuáles son las entidades persecutoras encargadas de hacerle frente a los delitos informáticos en el Perú?**
   Dentro de la Policía Nacional, la unidad encargada de acuerdo a sus funciones es la División de investigación de delitos de alta, que es parte de la estructura de la DIRINCRI PNP, que coordina y asesora además a otras unidades policiales cuando es requerido frente a alguna investigación donde se ha hecho uso de las TICs como medio u objetivo para un ilícito.

2. **En su opinión, ¿considera usted que el sistema de administración de justicia actual ha evolucionado a fin de frenar los delitos informáticos?**
   Evidentemente sí, la DIVINDAT particularmente viene capacitándose constante te en las nuevas formas que utiliza la ciberdelincuencia, además se debe mencionar que desde año pasado contamos con una fiscalía especializada de ciberdelincuencia. Pero aún es el inicio de un largo camino donde además tienes que haber el compromiso tanto de sector privado para realizar una lucha frontal a la ciberdelincuencia.

3. **¿Conoce los cuerpos normativos vigentes que regulan los delitos informáticos en el Perú?**

   Desde el año 2013 contamos con una ley especial de delitos informáticos, Ley 30096 y su modificatoria la Ley 30171, es el marco jurídico donde estable los tipos penales para la lucha contra la ciberdelincuencia. Asimismo, el Perú forma parte del convenio de Budapest o de la Ciberdelincuencia, para la cooperación entre los países miembros.

4. **¿Cómo es el procedimiento de la individualización del sujeto activo en los delitos informáticos?**

   En el curso de la investigación, se busca establecer el grado de participación de los investigados, contando para ello siempre con el apoyo técnico de peritos y personal especializado que puedan brindar evidencia sobre los hechos que se están investigando.

5. **A su experticia ¿Cuándo podemos hablar que se ha configurado el delito de Fraude informático?**

   El fraude informático según lo establecido artículo 8 de la ley 30096 y su modificatoria Ley 30171, donde establece textualmente El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño que son los verbos rectores, diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, está claramente establecido en nuestro artículo lo que es relacionado a la información.

6. **Para usted, ¿a qué se debe el incremento de los delitos informáticos en Pandemia?**

   La pandemia sin duda ha permitido la comisión de los delitos informáticos en sus diversas modalidades, debido a que el ciberdelincuente ha encontrado un nuevo canal para cometer delitos, teniendo en cuenta que los usuarios

desconocían los riesgos a los que están expuestos que ha sido aprovecho, siendo las modalidades más utilizadas el phishing que es una forma de como obtener información confidencial y también otra modalidad que es el simswap en el cual de los operadores es sacar un duplicado básicamente de nuestros datos y utilizarlos para diferentes propósitos, entre otras modalidades, que utiliza la ciberdelincuencia que utiliza para obtener información confidencial aprovechando el desconocimiento de los cibernautas al utilizar o entrar al internet.

Nombre del participante: Wuilman Zabarburu Vargas

DNI: 40072448

CIP: 31298388

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

ACTA DE SUSTENTACION DE TESIS

Siendo las 21:50 horas del 15/07/2022, el jurado evaluador se reunió para presenciar el acto de sustentación de Tesis titulada: "Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19", presentado por los autores MARTEL MELGAREJO JOSEPH ALEXANDER, QUISPE VARA DIANA DOLORES estudiantes de la escuela profesional de DERECHO.

Concluido el acto de exposición y defensa de Tesis, el jurado luego de la deliberación sobre la sustentación, dictaminó:

Autor	**Dictamen**
DIANA DOLORES QUISPE VARA	Mayoría

Firmado electrónicamente por:
DPAULETTH el 04 Sep 2022 10:27:52

DAVID SAUL PAULETT HAUYON
PRESIDENTE

Firmado electrónicamente por:
MMVALDIVIAC el 04 Sep 2022 00:14:42

MANUEL MOISES VALDIVIA COTRINA
SECRETARIO

Firmado electrónicamente por:
LUPALOMINOG el 25 Jul 2022 20:20:46

LUTGARDA PALOMINO GONZALES
VOCAL

Código documento Trilce: TRI - 0313430

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

ACTA DE SUSTENTACION DE TESIS

Siendo las 21:50 horas del 15/07/2022, el jurado evaluador se reunió para presenciar el acto de sustentación de Tesis titulada: "Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19", presentado por los autores MARTEL MELGAREJO JOSEPH ALEXANDER, QUISPE VARA DIANA DOLORES estudiantes de la escuela profesional de DERECHO.

Concluido el acto de exposición y defensa de Tesis, el jurado luego de la deliberación sobre la sustentación, dictaminó:

Autor	Dictamen
JOSEPH ALEXANDER MARTEL MELGAREJO	Mayoría

Firmado electrónicamente por:
DPAULETTH el 04 Sep 2022 10:27:52

DAVID SAUL PAULETT HAUYON
PRESIDENTE

Firmado electrónicamente por:
MMVALDIVIAC el 04 Sep 2022 00:14:42

MANUEL MOISES VALDIVIA COTRINA
SECRETARIO

Firmado electrónicamente por:
LUPALOMINOG el 25 Jul 2022 20:20:46

LUTGARDA PALOMINO GONZALES
VOCAL

Código documento Trilce: TRI - 0313430

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Autorización de Publicación en Repositorio Institucional

Nosotros, MARTEL MELGAREJO JOSEPH ALEXANDER, QUISPE VARA DIANA DOLORES identificados con DNIs N° 75648664, 70844705 (respectivamente), estudiantes de la FACULTAD DE DERECHO Y HUMANIDADES y de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, autorizamos (X), no autorizamos ( ) la divulgación y comunicación pública de nuestra Tesis: "Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19".

En el Repositorio Institucional de la Universidad César Vallejo, según esta estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art. 23 y Art. 33.

Fundamentación en caso de NO autorización:

SAN JUAN DE LURIGANCHO, 16 de Octubre del 2022

Apellidos y Nombres del Autor	**Firma**
MARTEL MELGAREJO JOSEPH ALEXANDER **:** 75648664 **ORCID:** 0000-0002-0365-5729	Firmado electrónicamente por: JMARTELM el 16-10-2022 21:53:46
QUISPE VARA DIANA DOLORES **:** 70844705 **ORCID:** 0000-0002-1371-4032	Firmado electrónicamente por: DQUISPEV6 el 18-10-2022 20:18:17

Código documento Trilce: INV - 0897396

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Autenticidad del Asesor

Yo, PALOMINO GONZALES LUTGARDA, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, asesor de Tesis titulada: "Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19", cuyos autores son MARTEL MELGAREJO JOSEPH ALEXANDER, QUISPE VARA DIANA DOLORES, constato que la investigación tiene un índice de similitud de 14.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 28 de Junio del 2022

Apellidos y Nombres del Asesor:	**Firma**
PALOMINO GONZALES LUTGARDA **DNI:** 22422843 **ORCID:** 0000-0002-5948-341X	Firmado electrónicamente por: LUPALOMINOG el 21-07-2022 22:44:34

Código documento Trilce: TRI - 0313433

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Originalidad de los Autores

Nosotros, MARTEL MELGAREJO JOSEPH ALEXANDER, QUISPE VARA DIANA DOLORES estudiantes de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, declaramos bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Actuación de las entidades persecutoras de los delitos informáticos en pandemia por COVID-19", es de nuestra autoría, por lo tanto, declaramos que la Tesis:

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

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

Nombres y Apellidos	**Firma**
MARTEL MELGAREJO JOSEPH ALEXANDER **:** 75648664 **ORCID:** 0000-0002-0365-5729	Firmado electrónicamente por: JMARTELM el 16-10-2022 21:54:34
QUISPE VARA DIANA DOLORES **:** 70844705 **ORCID:** 0000-0002-1371-4032	Firmado electrónicamente por: DQUISPEV6 el 18-10-2022 20:18:27

Código documento Trilce: INV - 0897395

INVESTIGA UCV