UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Deficiencias Legislativas en el Tratamiento de la Ley N° 30096, Ley de Delitos Informáticos – Fraude Informático, Lima 2019 – 2021

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogada

AUTORAS:

Arellano Casimiro, Gisela Lisset (orcid.org/0000-0002-2099-4589)

Galindo Martinez, Sofia Emilia (orcid.org/0000-0001-8383-3849)

ASESOR:

Mg. Vásquez Torres, Arturo Rafael (orcid.org/0000-0002-8513-4483)

LÍNEA DE INVESTIGACIÓN:

Derecho penal, procesal penal, sistema de penas, causas y formas del fenómeno criminal

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2022

DEDICATORIA

A Dios, quien ha sido mi guía y fortaleza, a la memoria de mi padre el Dr. Julio César Arellano Espinoza, por enseñarme a luchar y levantarme frente a las adversidades de la vida, a mi madre por tanta dedicación, y a mi pequeña hija quien me da ese auge para salir adelante. (Arellano, Gisela)

Dedicado a mi querida madre Doris Martínez Salvatierra, quien no solo me regaló la vida, sino que es el principal cimiento en mi formación como persona y profesional, desde niña, fomentó en mí las bases de la honestidad, responsabilidad y superación, ella es el espejo en el cual me quiero reflejar, pues sus virtudes y amor son infinitos. (Galindo, Sofia)

AGRADECIMIENTO

Queremos agradecer a todas las personas que hicieron posible esta investigación y que de alguna manera estuvieron con nosotras en los momentos difíciles, alegres y tristes. Estas palabras son para ustedes, a nuestros padres por su amor, comprensión y apoyo, a nuestro asesor de tesis el Dr. Arturo Vásquez Torres, quien nos guio académicamente con su experiencia y profesionalismo.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS Y FIGURAS

Resumen

La presente tesis está enfocada en determinar las deficiencias legislativas advertidas en el delito de Fraude Informático en Lima 2019-2021, tipificado y sancionado en el artículo 8º de la Ley Nº 30096 (Ley de Delitos Informáticos), como objetivos específicos tenemos: 1) Establecer los fundamentos, 2) Analizar las propuestas de solución, y 3) Establecer las propuestas de solución, todo ello con el objetivo de reducir las ineficiencias legislativas en la praxis, cuya metodología de análisis es de enfoque cualitativo, tipo básica, con diseño no experimental, para lo cual examinamos revistas indexadas de relevancia jurídica, así como entrevistas a especialistas en la materia, y una encuesta dirigida a la población, ello nos trajo como resultado que efectivamente el delito de fraude informático contaba con deficiencias legislativas. Finalmente, llegamos a la conclusión que el delito de fraude informático es aquella conducta que ejerce un agente activo a través del uso de las TIC, adicionalmente, hemos determinado que la tasa de criminalidad se ha triplicado los últimos cuatro años, frente a ello tenemos una normativa con deficiencias legislativas las cuales versan en la imposibilidad de individualizar al sujeto activo, además de la desprotección y desamparo de la víctima usuario frente al perpetrador del delito.

Palabras clave: Delitos Informáticos, Fraude informático, modalidades.

Abstract

This thesis is focused on determining the legislative deficiencies noted in the crime of Computer Fraud in Lima 2019-2021, typified and sanctioned in article 8 of Law No. 30096 (Computer Crime Law), as specific objectives we have: 1) Establish the fundamentals, 2) Analyze the solution proposals, and 3) Establish the solution proposals, all with the aim of reducing legislative inefficiencies in praxis, whose analysis methodology is of a qualitative approach, basic type, with a non-experimental design , for which we examined indexed journals of legal relevance, as well as interviews with specialists in the field, and a survey aimed at the population, this brought us as a result that the crime of computer fraud indeed had legislative deficiencies. Finally, we come to the conclusion that the crime of computer fraud is that conduct exercised by an active agent through the use of ICT, additionally, we have determined that the crime rate has tripled in the last four years, compared to this we have a regulation with legislative deficiencies which deal with the impossibility of individualizing the active subject, in addition to the lack of protection and helplessness of the user victim against the perpetrator of the crime.

Keywords: Computer Crimes, Computer Fraud, modalities

I. Introducción

Ocón (2018), sostiene que la realidad va siempre por delante del derecho, afirmación que al paso del tiempo se ha vuelto incuestionable. A lo largo de la historia se han proyectado avances tecnológicos, que ya vivimos y solo imaginábamos en películas de ciencia ficción, tal es así, que dichos cambios han incidido directamente en la forma de relacionarnos, verbigracia, la creación del internet, que resultó un medio eficaz en el suministro de múltiples canales de comunicación virtual y acceso a la información, el mismo que también dio paso a las nuevas formas de criminalidad, aislando la sola voluntad de adquisición de conocimiento del común usuario, en esa línea de ideas, sostienen Rodas y Loor (2018) que "la persona que entra en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes" (p. 9). Por lo que, ignorar dichas posibilidades, resulta el cepo perfecto para los ciberdelincuentes, pues el internet, es mucho más grande de lo que puede imaginar nuestra mente, ya que, lo que podemos ver no es sino más que "el pico del iceberg" de una inminente nueva era digital. Y, en ese contexto, dicha herramienta se convirtió en el medio ideal para la comisión de delitos, pues suele tener un modus operandi inmediato y sin rastros de persecución, lo que provoca que la identificación del sujeto activo se torne más dificultosa (Lorena et al., 2017). A juicio de Pons (2017) el surgimiento del internet y los sistemas informáticos, determinaron un antes y un después en la forma que las personas se introducen a los sistemas informáticos, donde su uso construye y evoluciona nuestra forma de vida. Sin embargo, también se evidenciaron comportamientos ilícitos alrededor de estos espacios, tal es así, que los denominados "ciberdelincuentes" proliferaron técnicas y métodos de alteración en los sistemas de seguridad los cuales fueron manipulados para beneficio propio. En cuanto al alcance de los delitos informáticos, estos tienen una incidencia nacional e internacional, en ese contexto, Espinoza (2018) ha precisado que "los delitos informáticos son transnacionales, cuando la acción se ejecuta en un país y el resultado se da en otro país (...), esto eleva la ubicuidad, los riesgos y la complejidad en su investigación" (p. 8). En cuanto a la normativa internacional,

nuestro país suscribió el convenio de Budapest en el año 2004, el cual como norma madre en la materia hizo frente a la lucha contra la cibercriminalidad, dicho acuerdo fue ratificado mediante Resolución Legislativa N° 30912 de fecha 13.02.2019, considerado como precursor en la materia de cibercriminalidad, dicho convenio se constituyó rápidamente como base normativa a nivel internacional con la finalidad de erradicar los delitos asociados al internet, aunado al objetivo de concientizar en los países miembros una "política penal común" y así combatir el cibercrimen incipiente. La normativa en mención fue producto del trabajo de cuatro largos años de ardua investigación, la cual dio como resultado tipos penales base que las naciones miembros, como cuota de responsabilidad, incorporaron dentro de su regulación penal. En nuestro país, primigeniamente se incorporó el artículo 186° en el Código Penal, sin embargo, el principal problema, era su autonomía, pues aquel delito informático contra el patrimonio, se configuró y tipificó en calidad de agravante del tipo penal de hurto, conocido con la denominación de "hurto electrónico", ello se habría modificado el 17 de julio del año 2009, mediante Ley N° 27309, modificando el título V - Libro segundo de la norma sustantiva penal, e insertando el Capítulo X, denominado "delitos informáticos", posteriormente, fue una vez más corregido y ahora calificado como "delitos informáticos patrimoniales", introduciendo el tipo penal: intrusismo y fraude informático (Art. 207° literal A). Posteriormente, se promulgó la Ley N° 30096 denominada "Ley de delitos informáticos", la cual fue modificada mediante Ley N° 30171, regulando el delito de fraude informático entre otros ilícitos de índole informático. (Leyva, 2021) Dichas normas fueron ratificadas ante el notorio incremento de ilícitos cometidos a través de las Tecnologías de la Información y la Comunicación, en adelante TIC. Visto de otro punto, la aplicación de la norma resultó burocrática e ineficaz en su aplicación, ya que en la norma procesal no se adecúa a los delitos digitales que contienen una naturaleza distinta. A la fecha, la única institución especializada en la lucha frontal contra la ciberdelincuencia a nivel nacional es la División de Investigación de Delitos de Alta Tecnología, en adelante DIVINDAT (en adelante DIVINDAT), cuyo respaldo constitucional se avala en el numeral seis del artículo dos, el cual señala que "todo ciudadano peruano tiene derecho a tener acceso a

los servicios informáticos computarizados o no computarizados, de origen público o privado, teniendo presente que no provean información que afecte la privacidad personal y familiar de los sujetos de derecho", dicho artículo hace referencia al derecho constitucional de uso y disfrute de los servicios informáticos sin que ello dañe o afecte la intimidad personal. En suma, la presente investigación estuvo inspirada por las alarmantes cifras de cibercriminalidad en Lima, frente a una desfasada normativa legislativa y bajos índices estadísticos, lo que consideramos colisiona con la realidad material. **A lo** largo de la presente investigación descubrimos que existen diversas maniobras de estafa cibernéticas mediante las cuales logran escabullirse los ciberdelincuentes, ya sea mediante e-mails, SMS de ostentosos premios o sorteos, redes sociales e incluso llamadas telefónicas, las cuales resultaron familiares a más del 90% de nuestros encuestados. Esta situación, se reporta continuamente, lo que debe dejarse claro a nuestros lectores es que todos podemos ser víctimas potenciales de estos métodos de asalto. Finalmente, en el presente trabajo de investigación buscamos dar respuesta al siguiente problema general: ¿Existen deficiencias legislativas en la Ley Nº 30096 - Fraude Informático en Lima 2019-2021?, y como problemas específicos: 1) ¿Por qué se necesita eliminar o erradicar las deficiencias legislativas en el artículo 8°?, 2) ¿Es pertinente plantear mejoras a la estructura normativa del artículo 8°?, y 3) ¿Qué sugerencias planteamos para eliminar o erradicar las deficiencias legislativas en el artículo 8°?, estableciéndose para tal efecto, como objetivo general: Determinar cuáles son las deficiencias legislativas en la Ley N° 30096, y como objetivos específicos: 1) Definir las razones por las que se debe mejorar o erradicar las deficiencias, 2) Analizar las propuestas para mejorar o erradicar las deficiencias, y 3) Establecer propuestas que coadyuven a mejorar o erradicar las deficiencias, todo ello en razón al art. 8°, ante tal disyuntiva nos hemos planteado como hipótesis general: Existen deficiencias legislativas en la Ley Nº 30096, y como hipótesis específicas: 1) Se necesita eliminar las deficiencias legislativas del artículo 8° porque esta se haya desactualizada y es ineficaz, 2) Se recomienda mejorar la estructura normativa del artículo 8°, y 3) Hemos establecido propuestas que mejoran la estructura normativa del artículo 8°.

II. Marco Teórico

A fin de llevar a cabo el desarrollo de la presente investigación, se han recabado los siguientes antecedentes nacionales e internacionales, según Rodas y Loor (2018) definen a los "delitos informáticos", también conocidos como "cibercriminalidad o ciberdelincuencia" como "toda actividad ilícita que tiene por esencia robo de información, contraseñas, fraude a cuentas bancarias, entre otros" (p. 4), asimismo, Mayer (2018) refiere que los delitos informáticos, presentan características distintas al proceso común, presentando mayor dificultad en el recabo de medios probatorios, subraya que la informática es un campo del conocimiento caracterizado por una elevada especificación y complejidad técnica, la misma que se refleja en el uso de terminologías y códigos particulares para fines ilícitos, los cuales constituyen un idioma propio en su área, en lapsos muy breves de tiempo, colige que los legisladores, operadores y doctrinarios en el tema, realizan una lucha frontal contra estos delitos pluriofensivos, pues se trata de entender los rasgos esenciales del que delinque tras una pantalla anónima y aquel que adecúa sus fines a un medio tecnológico. En Venezuela, Acosta et al. (2020) believes that computer crimes are carried out by extracting personal information from cyberspace, thus threatening private and social environments, causing property, business and personal damage, caused by illegal data leakage. Este tipo de delitos por lo general tiene un carácter transfronterizo, y exigen una respuesta instantánea, por lo tanto, se necesita una adaptación de medidas de seguridad y normas para tales fines, a pesar de no encontrarse regulado el delito de fraude informático como tipo penal en algunas normativas de ciertos países, sin embargo, se determinó que el delito informático de mayor recurrencia, viene a ser el espionaje y sabotaje informático, los cuales se realizan mediante programas específicos, de donde se desprende una serie de acciones y técnicas sucesivas, tales como, robo de identidad (a fin de acceder a fondos bancarios), utilización de programas propios de hackers (a fin de incrustar malwares en los procesadores e infectar cualquier archivo, documentación o sistema informático de seguridad). Por otro lado en Nicaragua, Sánchez (2021), ha determinado que las motivaciones para la comisión de delitos informáticos parte de dos aristas que recaen sobre el

agente activo, las cuales son: motivaciones intrínsecas, consideradas como el propio placer o recompensa que obtiene el infractor ante la comisión del ilícito, ya sea por mera curiosidad, autoaprendizaje, reto o aburrimiento, propios de una edad promedio joven o joven adulto y por otro lado, están las motivaciones extrínsecas, las cuales se encuentran relacionadas al resultado del ilícito penal, sea por el lucro personal o por la posición de poder de lograrlo a través de medios digitales. De la misma forma, Díaz (2019) quien aborda un importante trabajo sobre la globalización de los delitos informáticos y la cooperación internacional, enfatiza que si bien esta nueva modalidad de delitos informáticos, es severamente castigada y se han mejorado las técnicas de ciber patrullaje, refiere que quienes delinquen van siempre uno (o varios) pasos por delante de las autoridades, en ese sentido, se remarca que tan solo en el año 2009 se ha registrado en Estados Unidos pérdidas económicas de hasta $560'000,000.00 dólares como resultado de los asaltos informáticos, sin embargo, estos no se agotan sólo en delitos de índole económico, ya que en los últimos años se han perpetrado ilícitos mediante la red, como medio y fin, tales como, robo de identidad, violación del derecho a la intimidad y devastación de software por virus informáticos, de allí su carácter pluriofensivo. Por último, el autor Díaz refiere que las plataformas virtuales también se desarrollan como una red de terrorismo internacional, ya que se realizan actividades como la captación de fondos, planificación de atentados o ataques de hackers al cimiento de un Estado, siendo ocasión potencial y tangible nada alejada de la realidad que ahora vivimos, (por ejemplo, la intervención de personajes polémicos e icónicos como "*anonymous*" quien recientemente hackeó programas televisivos difundiendo imágenes de Ucrania, que viene siendo atacada militarmente por Rusia, en el contexto del conflicto bélico entre dichos países). A nivel nacional, Huamaní et al. (2021) menciona que los delitos informáticos son definidos como el comportamiento ilegal que perjudica los sistemas y datos informáticos, además de diversos bienes tutelados jurídicamente, el cual se ejecuta por intermedio de las TIC's, adicionalmente, sostiene que el Perú no cuenta con estrategias firmes que garanticen seguridad a la población en cuanto a la protección de datos

informáticos. Como lo plantean Mayer y Oliver (2020) el delito de fraude informático se traduce como “la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos '' (p. 2). Antes, también en palabras de Mayer (2017), expresó que el delito de fraude informático versa sobre la vulneración del patrimonio, situación que se asemeja al delito de estafa computacional, pues se realizan maniobras de transgresión de datos registrados digitalmente, a fin de conseguir un provecho económico. Italia, Fusco (2020) sostiene que la tipificación del delito de fraude informático se ha realizado a fin de “sancionar el incremento patrimonial indebido, obtenido a través del uso fraudulento de un sistema informático; es decir (...) la manipulación de un sistema (...) para lograr una ventaja patrimonial” (p. 12). De igual modo en Chile, se ha enfatizado que el bien protegido jurídicamente se vulnera en el delito de fraude informático adquiere una especial relevancia, pues dentro de la gama de modalidades del fraude informático, se utiliza el internet como medio para la ejecución del ilícito penal, así como, por medio de la obtención de datos personales, resquebrajando de esta manera derechos fundamentales en la sociedad. Por otro lado, el delito de fraude informático, en su ejecución, se encuentra íntimamente relacionado al tráfico comercial electrónico, conocido como el *e-commerce*, así como las transferencias de fondos online, especialmente las “transferencias bancarias”, por tanto, catalogan al fraude informático como un delito pluriofensivo, pues afecta en primer lugar a un bien jurídico individual, de carácter patrimonial, y en segundo lugar afecta también a un bien jurídico supraindividual, ya que durante la ejecución del *iter criminis*, el sujeto activo vulnera barreras de sistema automatizado y a su vez, canales que manejan dicha información (Mayer y Oliver, 2020). Asimismo, en Ecuador, Ortiz et al. (2019), sostiene que respecto a la vulnerabilidad de las empresas frente a los delitos informáticos, enfatiza sobre el delito de fraude informático o fraude cibernético, el cual define como aquel que se realiza a través de un medio digital valiéndose del internet, que se suministra de piratería informática a fin de acceder a distancia a una base de datos de contenido confidencial, donde puede desarrollar la intercepción de datos mediante transmisiones, produciendo el robo de claves, números de cuentas de entidades

bancarias e incluso datos personales de la víctima, por lo que este delito, ha desarrollado figuras como falsificación, estafa o sabotaje en cualquier caso que comprometa la informática como vía para la perpetración del ilícito penal. Igualmente, en Argentina, Belén (2021) alludes that the terms fraud and computer fraud have been classified as synonyms, defining as the agent "who will defraud" the normal operation of the connection of personal data and/or computer systems, with said classification it is sought to sanction computer crimes of a patrimonial nature, disappearing the reluctant atypicality in cases of fraud by digital means to a natural or legal person. Respecto al uso de las billeteras digitales, es importante destacar lo manifestado por Vinelli (2021) quien ha establecido que el mundo mantiene una evolución significativa, dando pie al uso de monederos o billeteras digitales de manera cotidiana, lo que determina una transformación en la convivencia socioeconómica de donde se obtiene un sin número de beneficios, empero, adicionalmente, refiere que en el desarrollo de la actividad delictiva mediante medios tecnológicos, dentro de la gama de ciberdelitos existentes, los más frecuentes son la suplantación de identidad y el fraude informático. Asimismo tenemos que para Encalada et al. (2020) el desarrollo de las billeteras digitales en Ecuador, permite realizar transferencias monetarias en tiempo real a través de medios digitales como smartphones y computadoras mediante el internet, que permite ahorrar tiempo en los métodos de pago, fuera o dentro del país, asimismo, refiere que el uso de la billetera electrónica es imprescindible dado sus características de distanciamiento social y seguridad tecnológica, más aún en los tiempos actuales de pandemia, establecen un sistema rápido y útil. Por otro lado, sabemos que la utilización de dichas billeteras digitales son fuente de transición de dinero, dando paso a las modalidades de fraude informático tales como el phishing, definida como aquella acción mediante el cual un cibernauta, crea una infraestructura web con características similares a una original con el fin de obtener y grabar la información introducida en el formulario (Zambrano, 2021). En Colombia, Medina et al. (2021) destaca la tipología desarrollada sobre el *Phishing*, en primer lugar, aborda el *Spear Phishing*, el cual tiene una dirección específica a determinados grupos, mediante el empleo de correos electrónicos a modo de

señuelos, los cuales aparentan ser de una fuente confiable, sin embargo, la víctima termina en un sitio web falso con virus o malwares en ella. En segundo lugar, nos habla de *Whale Phishing* o *Whaling*, según el autor, este tiene como objetivo funcionarios de altos cargos empresariales, tales como gerentes, directores, etcétera; en general a personas adineradas y prominentes. En tercer lugar, nos describe al *Social Fishing*, el cual se enfoca en las clonaciones de las redes sociales o mensajes que se comparten por las redes sociales a través de links fraudulentos, lo que funciona de perfecto cepo para internautas activos. En cuarto lugar, nos habla del *Pharming*, que aprovecha los principios del Internet, para convertir secuencias de letras, y elaborar un URL o dirección de internet de uso cotidiano, como el buscador Google Chrome, de modo que, al introducir dicha secuencia, el hacker logra colocar un virus o troyano en el ordenador de la víctima al *clickear* el sitio web fraudulento. Carhuancho y Núñez (2020) describen las modalidades y métodos para la comisión de los delitos informáticos, reitera al (1) Phishing, el cual viene a ser una modalidad moderna y repetida la cual requiere una preparación previa, su propia denominación deriva del verbo “pescar”, modalidad que se refiere a la remisión de email-s, utilizando el nombre de una entidad bancaria en la cual se coloca un link (similar al de la entidad) o sitio web adulterada (con el logotipo de la entidad), misma que induce al usuario a proporcionar información confidencial referente a su cuentas bancarias, tarjetas de crédito o claves secretas, también conocido como estafa informática. (2) Cartas Nigerianas: Consiste en la súbita comunicación de un remitente anónimo, mediante correos o SMS, donde ofrecen negocios muy provechosos o regalos de sorteos (en los que no se participó), mismo que indica sea respondido en un plazo determinado. (3) Llamada perdida: Actualmente es otra de las modalidades más utilizadas, consta en la recepción de una llamada de un número telefónico extraño, posterior a esta llamada, se deja un mensaje en el buzón de voz, al oírlo, el usuario se suscribe sin saberlo a un servicio de mensajería, mismo que autoriza facturar un monto de dinero determinado. (4) Sim swapping: Es una modalidad que consiste en privar de cobertura de línea a teléfonos móviles para así clonar o anular la tarjeta SIM del mismo. Asimismo, en cuanto a las características de los

perpetradores del delito de fraude informático, a juicio de Crespo (2020), el hacker cuenta con la capacidad de subyugar diversos aspectos simultáneos como: lenguaje de programación, manipulación de software, telecomunicaciones, así como dominar un computador o red informática, por tanto, se dice que posee altos conocimientos en tecnología, adicionalmente, señala que el estímulo de su accionar llega a ser por hobby o actividades sin o con fines de lucro. Asimismo, enfatiza que el cracker, equivale al “intruso o rompedor”, que produce un daño al sistema de software con relación a los ordenadores, computadores personales (PC), con la finalidad de violar un sistema cibernético causándole el mayor de los daños posibles, su instrucción se deriva en desprogramar dispositivos computacionales protegidos (descodifica, contamina, vulnera), programas que se encuentran acorazados por programas de seguridad. En menor envergadura tenemos a los tipos conocidos como lammer quienes visitan sitios web a fin de descargar programas generando ataques con dicho software. Y, por último, tenemos a script kiddie son aquellos que recopilan información de las redes sociales o buscan programas de hacking produciendo el despliegue de virus en la red. En adición, respecto al concepto de hacker, para Ardila et. al. (2021) a second concept of "hacker" is understood as those with knowledge of systems, network and internet security protocols, and instruction in system tools, who implement methodologies in order to carry out a series of tests that allow avoiding all security measures, security that a system of a certain organization has, and that identifies all possible vulnerabilities, and proceeds to implement procedures in order to eliminate the risks and threats warned. También, a fin de dilucidar sobre las definiciones de hacker y cracker, Mayer y Vera (2020) postulan que ambos términos evocan a usuarios con conocimientos adelantados en el dominio de la tecnológica e informática, sin embargo, el hacker se relaciona directamente con el espionaje informático, es decir, el acceder ilícitamente al sistema informático; en tanto, el cracker es aquel que viola un sistema informático, delegado para usar sus conocimientos informáticos provocando un daño a la red ingresada. Igualmente, existe la figura del “ciberdelincuente de cuello blanco”, quien usualmente ocupa áreas estratégicas en su centro de trabajo donde maneja información de índole

delicada y reservada, su motivación se da muchas veces por el “animus delicti” (carácter lucrativo), por otro lado, el usuario agraviado es la persona natural o jurídica (instituciones financieras o crediticias, entidades gubernamentales, aseguradoras) sobre quienes incide la acción del agente utilizando sistemas automatizados de información. Se resalta que muchas veces las víctimas corporativas, omiten denunciar el ilícito por miedo al desprestigio o deterioro de su perfil corporativo, hecho que ocasiona un aumento en la “cifra oculta” o “cifra negra” e impunidad. Frente a ello, se tiene la participación de la Policía Nacional del Perú, adscrita a ella, la DIVINDAT que pertenece a la Dirección de Investigación Criminal de la PNP. El departamento se encuentra constituido por 145 ciberpolicias. Adicionalmente, tenemos a la Fiscalía, cabe resaltar, que en el distrito judicial de Lima se cuentan con 81 fiscalías penales, conforme el más reciente Directorio de Fiscalías Superiores, de la que destacamos 04 despachos, las Fiscalías Corporativas Especializadas en Ciberdelincuencia de Lima Centro (Santiago de Surco), asimismo, resaltamos la única existencia de la Fiscalía Superior de Ciberdelincuencia de Lima Centro. Al mismo tiempo tenemos que el informe gubernamental realizado por el Ministerio de Justicia y Derechos Humanos (MINJUSDH, 2020) indica que respecto a los alcances y funciones de la DIVINDAT, desarrolla entre sus principales funciones la “[...] ejecución de análisis informático forense de equipos de cómputo, telefonía móvil y otros equipos electrónicos con capacidad de almacenamiento de información, inmersos en la comisión de delitos informáticos [...] mediante el uso de hardware y software forense especializado“ (pág. 60). El panorama tampoco parece alentador en cuanto a las cifras oficiales obtenidas de dicho informe, según la DIVINDAT, la cantidad de denuncias efectuadas por delitos informáticos mantienen un aumento progresivo y constante a lo largo de los años, de hecho, este se mantiene desde el año 2015, en el cual se reportaron 1,007 denuncias por delitos informáticos, en el 2016 se realizaron 1,228 denuncias, en el 2017 se realizaron 1,985 denuncias, en el 2018 se realizaron 2,878 denuncias y en el 2019 se realizaron 3,012 denuncias, haciendo un total de 10,110 denuncias por delitos informáticos reportadas en 4 años, las mismas que de forma desagregada, resultaron con mayor notoriedad,

aquellos que inciden sobre el patrimonio de las víctimas, tal es así, que el 62% de denuncias se realizó por el delito de fraude informático. Otro punto álgido abordado en el referido informe, son las características comunes detectadas en los perpetradores y víctimas del delito de fraude informático, existe un factor común respecto al nivel académico y profesional de los ciberdelincuentes, toda vez, que se trataría, en su vasta mayoría, de profesionales en ingeniería de sistemas e ingeniería electrónica, así como personas con alto conocimiento sobre manejo de las Tecnologías de la Información y la Comunicación y personal técnico en computación, también que la edad promedio de las víctimas de fraude informático oscilaría entre 30 a 44 años de edad, tomando en cuenta que en el año 2019 se reportaron la mayor cantidad de denuncias por el delito de fraude informático siendo las principales víctimas aquellas personas que realizan transacciones de pago y adquisición de bienes, a través de canales virtuales, en cambio, no solo se reportaron como víctimas a personas naturales, sino también jurídicas y entidades bancarias, de ello se colige la existencia de niveles intermedios de conocimiento en informática importantes los cuales van a determinar no solo un factor y rasgo común en los perpetradores del delito en materia informática, sino la preexistencia y predisposición de la comisión de delito a través de las TIC. Así pues, respecto a las TIC, Cruz et al. (2019) refiere que estas permiten no solo la comunicación y adquisición de información, sino también el almacenamiento, producción, acceso, acciones a distancia, la cual incide a nivel educativo, laboral e incluso de entretenimiento, recalcando, además, que sirve para una mejor enseñanza y aprendizaje de conocimientos mediante el uso de tecnologías educativas como las plataformas académicas. En esa línea de ideas, Lizcano et al. (2019) expresa que las “TIC favorecen la interacción traducida en el intercambio de saberes y prácticas” (p. 1), esto aplica a las múltiples ventajas desarrolladas del uso de las TIC. Caso contrario es lo que señala Gairín et al. (2017) quien identifica que la problemática está en base al uso indiscriminado de las TIC, en la población joven y adulta, señalando que “[...] la mala utilización de las TIC viene más por desconocimiento que por factores vinculados a la naturaleza de las mismas o a los potenciales riesgos que las pueden acompañar,

esto en cuanto al perjuicio ocasionado a los usuarios víctimas" (p. 4). Por último, el Perú ha ratificado el Convenio de Budapest, en donde la finalidad es la cooperación internacional a fin de realizar un frente a los delitos informáticos, ya que en muchas ocasiones no solo afecta nuestra frontera, sino que traspasan las mismas, y llega a convertirse en organizaciones internacionalmente peligrosas. (Pereyra y Turpo, 2020)

III. Metodología

3.1. Tipo y diseño de investigación

Previo a señalar el enfoque de análisis del presente trabajo de investigación, es preciso mencionar que, sin duda es bien conocido que, la composición cualitativa y cuantitativa de cuadros científicos es el elemento más importante de la capacidad de investigación científica (Concepción et al., 2019, p. 2). Estando a ello, dado que esta investigación estuvo orientado a determinar las deficiencias legislativas en el tratamiento de la Ley N°30096 - Fraude Informático en Lima durante el periodo del 2019-2021, la elaboración del trabajo está orientada a un análisis de enfoque cualitativo, dado que no analizamos datos numéricos, pues se estudió conforme los hechos se fueron desarrollando, además que fue la herramienta que mejor se adaptó a las necesidades y características de nuestra investigación.

Al respecto tenemos que el enfoque cualitativo utiliza el desarrollo de gráficos, palabras, textos, incluso imágenes, este tipo de investigación se dirige a comprender la vida social de los individuos por medio de los conceptos y enfoques desarrollados por este mismo, este enfoque se basa en evidencias dirigidas a la descripción de un fenómeno a fin de analizarlo y explicarlo mediante técnicas epistemológicas, tales como el método inductivo y la hermenéutica (Sánchez, 2019). En otras palabras, el enfoque cualitativo considerado por corrientes de investigación antipositivistas tal como señala Castañeda (2022) “this focuses on human spiritual and social problems, where the theory reflects the observation of the facts”. (pág. 4)

El tipo de diseño de investigación fue no experimental, pues buscó asociarse tanto a nivel empírico como sistemático, con apoyo de nuestras variables independientes, en otras palabras, éstas no sufrieron cambios ni modificaciones, para ello se desarrolló la observación y análisis de resultados que arrojaron las técnicas de investigación. Este tipo de diseño fue apropiado en proyectos de investigación en donde el investigador observa los sucesos y fenómenos de

manera intacta a cómo se desarrolló en su contexto natural, para así, haber sido posteriormente analizados. (Hernández et al., 2014)

Por consiguiente, el desarrollo del presente trabajo de investigación se ha desarrollado bajo el enfoque cualitativo con diseño no experimental, en donde se realizó métodos de recolección y análisis de datos, y con ello, una vez recabados nos hemos enfocado en el desarrollo de las preguntas de investigación habiéndose extrapolado así nuevas interrogantes. En referencia al presente método, se ha realizado la indagación de estudios científicos, previamente realizados, en base a las cuales hemos planteado diversas hipótesis y situaciones posibles como antecedentes al presente trabajo de investigación, a diferencia del enfoque cuantitativo, el cual siguió una línea de investigación con mayor rigurosidad en orden correlativa a recabar, analizar datos y en base a ello haberse formulado hipótesis, dado que el enfoque elegido permitió haber realizado dicha secuencia en un orden facultativo, ya que la acción de investigación y recolección de datos se trasladó de una manera más dinámica, habiendo logrado así perfeccionar el objetivo plasmado. (Hernández et al., 2014)

En cuanto a, el tipo de investigación estuvo orientado a un tipo básico, dado que dicho tipo de investigación logró acrecentar y consolidar información científica previamente indagada, pues han existido doctrinarios y estudiosos del derecho que han desarrollado trabajos previos similares al mismo, a través de mecanismos de investigación científica, tanto en enfoque cualitativos como cuantitativos, en base al estudio de teorías, investigaciones y/o estadísticas realizadas en años anteriores por estudiosos del derecho, del mismo modo fueron analizadas y observadas ampliando así nuestros conocimientos habiéndose logrado la acreditación de nuestras hipótesis. (Carrasco, 2015)

En suma, hemos aplicado este tipo de investigación, ya que a partir de la elección del tema de investigación que fue dirigido a determinar las deficiencias legislativas en la Ley N° 30096, Delitos informáticos - Fraude Informático en Lima, 2019- 2021, ergo, hemos pretendido adquirir información y datos relevantes de personas naturales y personas jurídicas pertinentes, para así haber arribado conclusiones y

recomendaciones óptimas del presente trabajo de investigación, habiendo logrado así desarrollar soluciones que han efectivizado la aplicación de la ley, no solo a nivel doctrinal sino también a nivel práctico, puesto que hemos advertido que el legislador, no tuvo las herramientas ni especializaciones suficientes para haber practicado una efectiva aplicación de la ley de delitos informáticos en específico en el delito de fraude informático, más aún, que hemos advertido el desarrollo de mecanismos de estafa cibernética, tan escasamente investigada en el Perú.

Existe entonces, una finalidad objetiva en base a datos y definiciones científicamente conceptualizados, dado que fueron utilizados métodos y técnicas, por medio del cual abordamos la problemática social de los Delitos Informáticos en el extremo del Fraude Informático, para ello se realizó un estudio minucioso de los aspectos palpables (denuncias, e investigaciones preliminares a nivel fiscal y policial, así como los archivados judicial, y los motivos principales para dicho archivamiento). Al mismo tiempo, hemos obtenido información cuantificable pertinente, dentro de ellas: entrevistas, encuestas, entre otras herramientas de estudio, por lo cual, hemos podido justificar las hipótesis planteadas, para un rápido actuar, y eficacia en la aplicación de la ley materia de investigación, no sin antes haber delimitado que el lugar de aplicación sería los Juzgados Penal de Lima Centro, así como la División de Investigación de Delitos de Alta Tecnología - DIVINDAT, ubicado en la Av. España 323 - Distrito de Cercado de Lima, y la Fiscalía de la Nación, ubicada en el Jr. Carabaya 442 en el Distrito de Cercado de Lima.

3.2. Categorías, Subcategorías y Matriz de categorización

El proceso de categorización permite certificar la información obtenida dependiendo del tipo de investigación aplicada. Estando a ello tenemos que, los diversos tipos de investigación se utilizan con el objetivo de examinar los resultados al final de la investigación. Ergo, se pudo establecer que las categorías son las bases de la investigación, la cual, en el presente trabajo, fue tomada en consideración con la finalidad de haber validado la información por medio del análisis de resultado de la misma, en palabras más sencillas, las categorías

pudieron ser entendidas como baúles conceptuales dentro del cual la información es almacenada. Para lo cual, en primera instancia, hemos debido identificar las unidades de exégesis e interpretaciones, las cuales tuvieron que ser esbozadas a partir de criterios espaciales, temáticos, temporales, gramaticales y sociales. Como resultado, tuvimos que la subcategoría, fue un elemento que brotó a raíz de una categoría, su finalidad fue profundizar, ello en razón a que nos permitió detallar de forma más específica lo que se relacionó directamente con ella. (Bastis Consultores, 2020)

A mayor abundamiento tenemos que, para llegar a la identificación de las categorías para Acosta et al. (2020), in the first instance, we have the phase of collection and analysis of selected data, depending on the case under investigation, since this will allow the delimitation of the categories, and then, the incidents that will make it possible to recognize the subcategories will be chosen, por otro lado, Hamui, L., y Vives, T. (2021) coligen que, al momento que las categorías y las subcategorías se determinan de manera previa al desarrollo del proceso de recojo de datos, se le denominan categorías apriorísticas, pues derivan de los marcos teóricos y conceptuales.

Estando a lo definido, procedemos con el desarrollo de la materia de investigación, en la siguiente tabla que pasamos a detallar a continuación:

Tabla N° 01

Matriz de categorización

MATRIZ DE CATEGORIZACIÓN	
CATEGORÍAS	**SUBCATEGORÍAS**
1. LEY Nº 30096	DELITOS INFORMÁTICOS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN - TIC

2. FRAUDE INFORMÁTICO MODALIDADES

DIVINDAT

Fuente: Elaboración propia

Información cuya procedencia de data o información son: las revistas indexadas, doctrina, jurisprudencia, estudio de normas nacionales e internacionales, entrevistas y encuestas. (Tabla de Matriz de Categorización Apriorística se haya en el anexo 01)

3.3. Escenario de estudio

En cuanto al escenario de estudio, como lo hace notar García et al. (2020) el problema de investigación científica opera como aquella situación que brota de un compilado dificultoso de factores (hecho materia de investigación) que se articulan provocando un escenario de estudio delimitado y preciso que merece ser interceptado desde la aplicabilidad la utilización del conocimiento científico. En atención a ello, el presente estudio se desarrolló en un ámbito geográfico delimitado dentro del distrito de Lima Centro, provincia Lima, país Perú. Es así que, el instrumento de recolección de datos, entrevista, se desarrolló dentro de las instalaciones de los siguientes despachos judiciales: Juzgado Unipersonal Supraprovincial Administrativo, Tributario, Propiedad Intelectual y Ambiental Liquidador de la Corte Superior de Justicia de Lima (en adelante CSJL), Sala Penal Liquidadora de la CSJL - Sede Barreto y el Gabinete de Asesores de la Fiscalía de la Nación de Lima, ubicado en el espacio geográfico de Lima Centro; así también, se tomó como escenario de estudio el recinto de la División de Investigación de Delitos de Alta Tecnología (en adelante DIVINDAT) ubicado en la Av. España Nº 323 en el distrito de Cercado de Lima, subrayamos que a la fecha es la única división de ejecución especializada en la investigación de delitos informáticos. En lo respecta a la encuesta, se realizó dentro del espacio geográfico de Lima Centro, vía Google Forms, remitida por enlace a los números de celular de los participantes a fin que puedan llenar la encuesta, el nivel de edad de los participantes oscila de 20 a 45 años de edad, el grado académico mínimo

educación secundaria culminada y máximo superior completa, con ocupaciones diversas y con conocimientos básicos sobre el derecho y la informática.

3.4. Participantes

Con relación a los participantes de la investigación, conceptualizamos el término bajo lo expresado por Guzmán (2021), quien refiere que el enfoque cualitativo se apoya en el método de recolección de datos no estandarizados ni predeterminados en su totalidad, dicha recolección comprende, el obtener la posición de los participantes, vale decir, sus sentimientos, experiencias, sentido y preferencia, basándose en eso, el investigador se focaliza en las experiencias de los participantes tal cual fueron (o son en el presente) sentidas y experimentadas, sobre ello el investigador advertida que convergen diversas realidades, en ella se engloba la de los participantes, el investigador y la que produce la interacción de todos los actores parte de la investigación.

Aclarado ese punto, tenemos que los participantes del presente trabajo de tesis, se ciñeron a los lineamientos del enfoque cualitativo, de manera concisa y objetiva, pues se realizaron técnicas de investigación permitidas por el mismo. Para el desarrollo de este acápite, fue menester la obtención de información fidedigna brindada directamente por la entidad policial abocada en realizar en primera instancia, ello en lo que respecta las entrevistas realizada, el carácter indagatorio de las denuncias por delitos informáticos, por ello acudimos a la DIVINDAT adscrita a la PNP de quienes hemos recabado en primera instancia, los índices de denuncias realizadas por delitos informáticos, así como las herramientas tecnológicas que utilizan para consolidar sus labores, y finalmente, el índice de porcentaje de víctimas afectadas que hayan logrado recuperar el patrimonio afectado, así como a la individualización del presunto autor de la comisión del delito realizada por medio de este delitos informáticos de fraude informático. Por otro lado, acudimos a magistrados, especialistas judiciales y relatora de Sala que aportaron información jurídica a la presente investigación. En adición, contamos con la participación de un miembro del Gabinete de Asesores de la Fiscalía de la Nación especializado en delitos informáticos a fin que nos

explique a mayor abundamiento lo que se realiza como labor fiscal, en referencia a los delitos informáticos. Aunado a ello, se recabaron opiniones de ciudadanos en la ciudad Lima centro a fin que brinden información que coadyuve al desarrollo de la investigación. Por otro lado, las encuestas contaron con 46 participantes quienes cuentan con conocimientos básicos del derecho y la informática, ello con la finalidad de acreditar que el delito de fraude informático es un delito que afecta a cualquier estrato de la sociedad.

3.5. Técnicas e instrumentos de recolección de datos

En este acápite corresponde definir las técnicas e instrumentos de recolección de datos utilizadas, para ello tenemos que la recolección de datos es considerada como el cálculo o prerrequisito para alcanzar el conocimiento científico, por tanto, el instrumento de recolección de datos se encuentra destinada a generar los presupuestos para la medición, en tanto tenemos que los datos son definiciones que expresan una conceptualización de lo que es el mundo real de lo sensorial, capaz de ser distinguido por los sentidos de forma directa o indirecta, donde todo lo práctico es medible, conceptos que ayudan a colegir que las técnicas de recolección de datos engloban procedimientos y actividades que facultan al investigador o investigadores a obtener información suficiente con la finalidad de dar respuesta a la problemática planteada en la investigación, para lo cual se determina que existen múltiples y diversos instrumentos provechosos para la recolección de datos, y para todo tipo de investigación ya sean cuantitativas, cualitativas o mixtas. (Duana et al., 2020)

A lo largo del desarrollo de la presente investigación, se utilizaron herramientas establecidas para la obtención de información, en cuanto a las técnicas utilizamos las siguientes: la observación del escenario en cuanto a las noticias masivas por reporte de fraude informático, la entrevista semiestructurada a los participantes señalados en el punto anterior y análisis de artículos en revistas indexadas; en cuanto a los instrumentos de recolección de datos, se utilizaron los siguientes: guía de entrevista y grabaciones al momento de realizar las entrevistas a los participantes antes mencionados. (técnicas e instrumentos permitidos por el

enfoque cualitativo). A continuación, describiremos a fondo los instrumentos de recolección de datos que más aportaron a la presente investigación.

3.5.1. Entrevista

La entrevista cualitativa se desarrolla de una manera más extensa en relación al entrevistado y entrevistador, ya que en ella es posible que el entrevistado se explaye respecto a sus comentarios de una manera reservada, dado que se respeta la total confidencialidad y participación bilateral entre entrevistado y entrevistador, por otro lado, también se caracteriza por tener una mayor adaptabilidad en el desarrollo de la misma en comparación con la cuantitativa, se infiere entonces que la entrevista se realiza con diálogo dirigido al intercambio de información, cuya apertura resulta beneficiosa para el entrevistador, y la cual se encuentra dirigida a aportar información para un objetivo, dirigido al tema de investigación. Ocasionalmente, en el desarrollo de la entrevista, el entrevistador puede realizar preguntas de tipo “piloto” y así realizar posteriormente las preguntas estructuras que aportaron al objetivo final y motivo principal del campo de investigación, y cuya información se busca extraer y analizar. (Hernández et al., 2014)

A lo precitado tenemos que, dentro de la gama de tipologías de entrevistas utilizadas en trabajos de investigación, tenemos las siguientes: estructurada, semi estructurada y no estructurada. En el presente trabajo se utilizó la entrevista semi estructura, Ríos (2019) la define como aquella técnica comúnmente utilizada en las investigaciones sociales y de comportamiento, es inclusive el medio de generación de datos más empleada en distintas tipologías de metodologías investigativas, destaca que la entrevista semiestructurada se haya entre la entrevista libre, que se orienta naturalmente por lo que va ocurriendo en ella, y donde no sigue reglas rígidas ni preguntas anticipadamente redactadas, a diferencia de la entrevistas estructurada donde si hay preguntas preestablecidas que deben ser contestadas, a la mitad, se hallaría la entrevista semiestructurada, en la que no figuran dichas preguntas, empero, sí una línea concreta además de

una serie de cuestiones a esclarecer que serán utilizadas como guía, en resumen, no existen interrogantes a responder, sino, dilemas a tratar.

Aunado a ello, se recalca que aplicamos técnicas de entrevista como herramienta principal para nuestra investigación, permitida en el enfoque cualitativo, se utilizó el cuestionario, como instrumento primordial, dirigido a un panel de expertos de aproximadamente cuatro profesionales en Derecho y el coronel representante de la DIVINDAT - DIRINCRI; resultado con los cuales hemos proyectado dar respuestas a nuestras interrogantes en relación con nuestros objetivos establecidos.

Guía de entrevista: Para el diseño de la guía de temas que hemos abordado en las entrevistas a desarrolladas, fue necesario el planteamiento de los siguientes enfoques: teóricos, prácticos y éticos. Práctico, ya que la entrevista se desarrolló de manera activa e interesante al entrevistado habiendo captado así la atención y el interés necesario para la obtención de aportes favorables al trabajo de investigación. Ético, pues se realizó con la finalidad de provocar en el entrevistado una reflexión en cuanto al problema que se planteó, y que adolece la sociedad, así pues, se ha advertido las falencias de la misma. Finalmente, teórico, ya que la guía de entrevista fue el instrumento idóneo cuya finalidad fue obtener el mayor beneficio en cuanto a información necesaria. (Hernández et al., 2014)

En ese sentido, hemos acudido a Especialistas en el Área del Derecho como: Jueces Penales de Lima Centro, Asistente de Relatoría de Sala Penal de Lima, Asesor de la Fiscalía de la Nación y coronel de la DIVINDAT.

Tabla N° 02

Cuadro de entrevistados

ENTREVISTADOS	CARGO	GRADO ACADÉMICO
María del Rosario Carrillo Espichán	Jueza de Juzgado Penal de Lima – CSJL	ABOGADA

Luis Edgardo Huamán Santamaría	Coronel PNP – DIVINDAT	MAGISTER
María Alejandra Ramos Ramos	Asistente de relatoría Sala Penal – CSJL	ABOGADA
Roberto Carlos Vílchez Limay	Asesor de Gabinete de Fiscalía de la Nación	ABOGADO

Nota: Participaron en el llenado de la Guía de Entrevista, validada por los especialistas, jueces, asistentes, fiscales y representantes de la DIVINDAT.

Fuente: Propia

Como resultado de las entrevistas realizadas, hemos obtenido conceptos relevantes para el presente trabajo de tesis, producido en el ejercicio de sus funciones tanto judiciales como policiales; los cuales nos permitieron abordar el tema con mayor claridad, todo ello con la finalidad de evidenciar el nivel de conocimiento de profesionales relacionados a nuestro tema de investigación.

3.5.2. Encuesta

Las encuestas son consideradas como investigaciones no experimentales, puesto que, su desarrollo conlleva a fines prácticos, sucintos, y atractivos, debiendo evitarse introducir preguntas incómodas, o muy abiertas, que se caracterizan por su facilidad de contestar e involucrar menos tiempo en su respuesta, así pues, es recomendable que estas deban comprender la razón del estudio a realizarse, por otro lado, el encuestado debe sentir la importancia de su participación, se recomienda, asimismo, que en el desarrollo de esta herramienta se debe introducir los agradecimientos y la plena identificación de quienes lo realizan, para así brindar seguridad y motivación a los voluntarios, quienes lo desarrollan. (Hernández et al., 2014)

Ya que, el progreso de esta investigación es enfocada en la recolección fidedigna de datos humanos y científicos, hemos desarrollado además de la entrevista, otra técnica de investigación previamente conceptualizada, la cual fue la encuesta, misma que estuvo dirigida a un público en específico, y a fin de haber concretado

la misma, hemos utilizado como instrumento un cuestionario de quince preguntas, que si bien es cierto, no fue fraccionado por el carácter académico, ni profesional de los encuestados, sin embargo, sí fue desarrollado a un panel de personas que tuvieron conocimiento del uso de las tecnologías tales como: el uso de computadoras, laptops, notebooks, celulares inteligentes o smartphones, el empleo de las redes sociales tales como Facebook, Instagram, WhatsApp, twitter, la lectura de mensajes de texto SMS, y/o redes sociales ya mencionadas, y por último, el atender llamadas telefónicas.

Análisis de fuentes documentales, en los procesos de investigación la verificación documental admite el recabo de datos tales como: documentos de acceso público, informes, cartas, diarios, registros, revistas, folletos, actas, enciclopedias, cintas magnetofónicas u otras bandejas de información, además, con la información recabada se hace sencillo el análisis de los datos extraídos relacionados con el tema materia de investigación. (Díaz et al., 2018)

Guía de análisis de fuente documental, es aquella que contiene información de los documentos a analizar con la finalidad de autenticar y corroborar la información contribuida en la presente investigación. La guía de análisis de fuente documental fue validada por los siguientes expertos en la materia:

Tabla N° 03

Cuadro de Validadores de Instrumento de recolección de datos – Guía de entrevistas

VALIDACIÓN DE INSTRUMENTOS

DATOS GENERALES	CARGO	PROMEDIO
Luis Edgardo Huamán Santamaría	Coronel PNP – DIVINDAT	99
Joselyn Gabriela Padilla Romero	Especialista judicial de Juzgado Penal de Lima – CSJL	95

Pola Milagros Benites Huertas	Abogada litigante – Estudio Jurídico “Milagros”	95
Mickael Andrés Escudero Villacorta	Abogado litigante independente	95

Nota: Especialistas que validaron los instrumentos de recolección (Entrevistas), entre ellos: jueces, representante de la DIVINDAT, especialista judicial y abogados.

Fuente: Propia

3.6. Procedimiento

La triangulación de datos y los diversos métodos de recolección, fueron las bases del presente proceso de investigación de enfoque cualitativo a través de los métodos para la recolección y análisis de datos tanto a nivel teórico como práctico. A ello tenemos que Díaz et al. (2021) revela que la triangulación es denominada también como “convergencia metodológica”, “método múltiple” y “validación convergente”, empero, en todas las terminologías se esconde el supuesto que los métodos cualitativos y cuantitativos deben ser apreciados no como áreas rivales, sino como complementarias, en razón a que en los diversos modelos de triangulación se encuentra sobreentendida la asunción básica que su eficiencia se apoya en lo estipulado por sus flaquezas de cada método de triangulación, pues van a ser compensadas por las virtudes contra balanceadora del otro.

Así, mientras hemos abarcado importantes cantidades de fuentes de datos, y de recursos, nos hemos permitido analizar una variedad de resultados, en otras palabras, a mayor cantidad de datos, mayor cantidad de fuentes de análisis, lo cual resultó ventajoso desde una perspectiva teórico y práctico, ya que generó resultados de mayor profundidad de análisis y aproximación a la realidad problemática en el presente tema abordado, pues si las fuentes se consideraron

diversas, existe un mayor aporte objetivo como resultado del mismo, este hecho es conocido como triangulación de datos (Hernández et al., 2014).

En base a ello, en primer término, el modo de recolección de información se desarrolló, desde fuentes nacionales hasta internacionales, seguidamente, hemos definido las categorías y subcategorías en fuentes bibliográficas reconocidas y prestigiosas, que han sido desarrolladas por autores abocados a la investigación del derecho, a través de revistas internacionales y nacionales, que han desarrollado una ardua investigación referido a los delitos informáticos, así como en el extremo de fraude informático. En segundo término, se realizó la discusión de resultados obtenidos tanto de las entrevistas, encuestas y análisis concienzudo del artículo 8º de la Ley Nº 30096 y revistas indexadas referentes al tema de investigación, para finalmente obtener conclusiones y proceder a estructurar recomendaciones.

3.7. Rigor Científico

Por otra parte, el rigor científico es calibrado por cualidades, como la fiabilidad y la validez medida a través de datos que inspiran confianza en la comunidad científica, así pues, la validez se refiere a aquella hermenéutica de resultados, la cual viene a ser aquel sustento fundamental en la investigación cualitativa, ofreciendo al investigador científico rigor y certeza en la cosecha de resultados, por ello, el delimitar el marco sistemático de recolección y exégesis de datos facilita a los demás investigadores ha delimitar si los resultados alcanzados son válidos o no, por último, el criterio de credibilidad o autenticidad permite demostrar la aproximación a los resultados de la investigación realizada (Noreña et al., 2012).

De otra arista, es evidente la distinción que se aborda en el desarrollo de los enfoques cualitativos y cuantitativos en el proceso de la investigación científica, así pues hemos expuesto brevemente que con relación a la recolección de datos esta se torna rigurosa en el enfoque cuantitativo, pues sigue una línea estricta de recolección de datos, análisis y resultados; contraria a la posibilidad de desarrollar una investigación desde el enfoque cualitativo la cual, cumple con los

presupuestos previamente establecidos para las investigaciones bajo el enfoque cualitativo, no obstante a ello, el rendimiento de la misma se pudo haber desarrollado de manera alternativa en el enfoque seleccionado, pues la recolección de datos se realizó durante, e incluso después de la deducción del problema, que evidentemente es dinámico, dado el carácter aleatorio mencionado, habiéndose generado resultados continuamente variables, acorde al avance la investigación.

Cuando se requiere el rigor científico dentro de un trabajo de investigación, esta se vuelve precisamente la principal polémica, pues es, de carácter aleatorio brevemente descrito anteriormente, sin embargo, no solo aborda el rigor científico sino también la sensibilidad ética y la sensible conservación del carácter secuencial metodológico, dado el carácter interpretativo del mismo.

En pocas palabras, los instrumentos de recolección fueron validadas por tres expertos en la materia del Derecho Penal, ello se puede observar en la Tabla N° 03 de la presente investigación, en tal sentido, la presente tesis se formuló en base al rigor científico que requiere la ciencia, cuya sujeción, se basa en los conocimientos teóricos además de los prácticos referente a los participantes, quienes, fueron previamente informados sobre la interrogante (general y específicas), objetivos (general y específicos) e instrumentos de recolección de datos de la investigación, en concordancia con los antecedentes obtenidos, de igual modo la credibilidad se apoyó en la reconocimiento de argumentación fidedigna recabada del producto de indagaciones hacia los especialistas (jueces, fiscales, coronel PNP y especialista judicial), en suma, tenemos que la auditabilidad o confiabilidad (manera en la que un investigador logra hace seguimiento a la pista de lo que realizo otro investigador - validación de instrumentos), la confiabilidad y validez (modo en que un instrumento de recolección produce resultados - validación de instrumentos), la dependencia o consistencia lógica (medida en que diversos investigadores, quienes acopian datos parecidos en el campo y ejecutan los mismo criterios, producen resultados semejantes -se advertido que existen trabajos similares al presente empero

muestra su sello característico al avocarse netamente al artículo 8° en toda su extensión de la palabra), la credibilidad (alude a como el producto de una investigación cualitativa, es fidedigna hacia los participantes quienes fueron estudiados, así como para otras personas quienes han experimentado, o en su defecto han estado en contacto directo con el fenómeno materia de investigación - se le informo a los participantes sobre el problema y objetivo de la presente tesis), y la transferibilidad o aplicabilidad (informar la viabilidad de ampliar los resultados de la investigación a diferentes poblaciones), se sostuvo en todo momento a lo largo de toda la investigación cualitativa.

3.8. Métodos y Análisis de datos

Los métodos de procesamiento que hemos desarrollado se realizaron en base a la exégesis de todo el material recabado, para ello, los métodos que se emplearon son:

Método Sistemático: Se define como aquel de carácter bibliográfico-reflexivo concordante con la visión de la teoría de sistemas y la reflexión holista, que versa sobre relacionar la empírica y los conocimientos superficialmente apartados de la constitución de esta aportación o modelo conceptual, que hace frente a la existencia del enfoque científico y la intencionalidad sistémica en el reconocimiento de los agentes, experiencias y la sagacidad de una situación social (Ortega et al., 2021). Mediante el método sistemático, si bien es cierto, se ha adquirido previos conocimientos e información de autores que sirvieron de base como antecedentes, se siguió un estricto orden en cuanto al análisis y resultado de la información recabada, que, si bien es cierto, pudo ser modificada y mejorada con posterioridad, ello no significó una alteración completa de nuestras ya adquiridas conclusiones.

Método Hermenéutico: Es considerada como aquella práctica interpretativa que procura ser constantemente reelaborada, puesto que se ejecuta ante la aparición constante de nuevos problemas en la sociedad, como resultado del mismo, el legislador unilateralmente no puede darse abasto, en lo que respecta a la constante investigación e interpretación de la normativa, así pues, este factor

genera que las interpretaciones y exégesis sean una tarea central en las ciencias sociales, dado sus constantes y necesarias modificaciones, pues el sujeto al que se dirige es el ser humano, quien es social por naturaleza y por ello dinámico, dando como resultado. (Rodríguez, 2010)

En esa línea de ideas, el presente trabajo de investigación se enfocó en la exégesis de fundamentos extraídos a partir de las entrevistas realizadas, así como del material documental recabado, tanto de manera virtual como física, habiendo realizado una minuciosa interpretación de elementos importantes y articulado hallazgos más significativos.

3.9. Aspectos Éticos

A ello tenemos que, la ética dentro del marco de la investigación es un área que se debe tener en suma atención, por la colaboración de agentes de diversos sectores del conocimiento. Por consiguiente, se pone a la vista una serie de disyuntivas sobre los aspectos éticos en las intervenciones que ejecutan los investigadores, al momento de abordar a ciudadanos de diferentes aristas. De aquí se colige que, la ética debe encontrarse presente en todos los sectores o ámbitos, primordialmente en aquellos que poseen una relación directa con seres humanos, es imprescindible la existencia de ética en cada una de las profesiones. (Paz, 2018)

Esta investigación fue estructurado en base al uso de técnicas e instrumentos científicos con la finalidad de la recolección de datos necesarios y sucintos, mediante técnicas como encuestas y entrevistas realizadas a un público específico, cuya conciencia estuvo enfocada en la lucha frontal contra la ciberdelincuencia, habiéndose creado así mayor empatía para nuestros conciudadanos, también, hemos desarrollado entrevistas que estuvieron dirigidas a un público en particular, como funcionarios públicos del Poder Judicial, funcionarios del Ministerio Público, además de miembros de la DIVINDAT, cuyo compromiso estuvo dirigido en aras de la lucha contra la cibercriminalidad y crimen en general, todo ello bajo previo consentimiento y autorización respectiva, así como, en el marco de la confidencialidad, y de tal manera haber dado estricto

cumplimiento a las exigencias del rigor científico y ético. Se desarrolló el cabal cumplimiento de las directrices de nuestro asesor, además, de los lineamientos universitarios establecidos, así como las estrictas pautas establecidas en el manual APA, respetando los derechos de autor que han sido empleados, así como las citas y referencias bibliográficas realizadas, igualmente, se ha hecho uso de un programa antiplagio “Turniti”, con la finalidad de poder medir el nivel de originalidad del trabajo.

IV. Resultados y Discusión

4.1. Resultados

En cuanto al resultado de un trabajo de investigación, de acuerdo con Escamilla et al. (2018), se tiene que los resultados de una investigación científica son aceptables en el momento que el estudio se halle libre de desaciertos, por tanto, a fin de dejar sentado que un estudio es exacto, se debe verificar la existencia de sesgos (equivocaciones sistemáticas), como mínimo en: el diseño de investigación, criterios de selección y forma de medición (forma de registrar y evaluar las variables de estudio), por tanto, colige que los resultados puede establecerse verídico en el instante que muestra un alto grado de validez (inexistencia de sesgos).

De lo expuesto, el presente trabajo de investigación tuvo dos etapas de trabajo de recolección de datos a través de los instrumentos anteriormente mencionados, los cuales fueron:

4.1.1. Encuesta

La primera de ellas comprendía la recolección de encuesta con el tópico “Delitos Informáticos - Fraude Informático” realizado a través de la plataforma Google Forms, en la que participaron un total de 46 personas, entre hombres y mujeres, con un rango de edad de 20 a 45 años, de las cuales se obtuvo el siguiente resultado:

1. A la pregunta: ¿Si disponen de alguna cuenta bancaria tales como: ¿cuenta de ahorros, cuenta de plazo fijo, cuenta sueldo o cuenta CTS? Respondieron afirmativamente un 93.5% (43) del total de encuestados, mientras que un 6.5% (3) respondió negativamente.
2. A la pregunta: ¿Si cuentan con alguna billetera digital? Respondieron afirmativamente un 60.9% (28) del total de encuestados, mientras que un 39.1% (18) respondió negativamente.
3. Respecto a los que respondieron afirmativamente la pregunta anterior (30 encuestados), se les consulto indique: ¿Con que frecuencia utilizan dicho

aplicativos móviles? Respondiendo una vez por semana el 53.3% (16), tres veces por semana el 16.7% (5) y de cinco a más veces por semana el 30% (9) del total de encuestados.

4. A la pregunta: Si alguna vez ha escuchado el término: “delitos informáticos”, “ciberdelitos”, “delito cibernético” y/o “ciberdelincuencia”, respondieron afirmativamente un 93.5% (43) del total de encuestados, mientras que un 6.5% (3) respondió negativamente.
5. A la pregunta: Si conoce las modalidades del delito de Fraude Informático, respondieron afirmativamente un 56.5% (26) del total de encuestados, mientras que un 10.9% (5) respondió negativamente, y un 32.6% (15) eligió la opción “algunas”.
6. A la pregunta: Si alguna vez ha sido víctima o ha conocido algún caso de delito de Fraude Informático, respondieron afirmativamente un 45.7% del total de encuestados, mientras que un 50% respondió negativamente, y un 4.3% eligió la opción algunas veces.
7. A la pregunta: Si alguna vez ha recibido llamada(s) telefónica(s) de un supuesto operador de empresa telefónica (Movistar, Claro, Entel o Bitel), siendo posterior a ello, víctima del robo del saldo de sus datos móviles o de alguna suma de dinero en su cuenta bancaria, respondieron afirmativamente un 23.9% (11) del total de encuestados, mientras que un 69.6% (32) respondió negativamente, y un 6.5% (3) eligió la opción algunas veces.
8. A la pregunta: Si alguna vez ha recibido un SMS similar al siguiente enunciado: “BANCO X: Tienes una transferencia retenida de S/.895.98 soles activa tu abono de inmediato en tu cuenta aquí: http:// app-abc,0peracion-web. site”, respondieron afirmativamente un 78.3% (36) del total de encuestados, mientras que un 21.7% (10) respondió negativamente.
9. A la pregunta: Si alguna vez ha recibido algún mensaje de texto o llamada telefónica de remitente desconocido, donde le indica que ha ganado un premio de sorteo (automóvil de último modelo o suma de dinero),

respondieron afirmativamente un 84.8% (39) del total de encuestados, mientras que un 10.9 % (5) respondió negativamente, y un 4.3% (2) eligió la opción algunas veces.

10. A la pregunta de si alguna vez ha recibido algún mensaje de texto o llamada telefónica de remitente desconocido, la cual tras ser atendida se escucha “un breve silencio” y/o al colgar dicha llamada advierte su línea móvil como “fuera de servicio”, respondieron afirmativamente un 60.9% (28) del total de encuestados, mientras que un 30.4% (14) respondió negativamente, asimismo un 8.7 % (4) eligieron la opción algunas veces.
11. A la pregunta de si en el hipotético caso de que fuera víctima del delito de Fraude Informático o conociera algún caso similar, estaría dispuesto a denunciarlo, respondieron afirmativamente un 95.7% (44) del total de encuestados, mientras que un 4.3% (2) eligió la opción tal vez.
12. A la pregunta de si cree usted que los delitos de Fraude Informático quedan impunes, respondieron afirmativamente un 50.0% (23) del total de encuestados, mientras que un 8.7% (4) respondió negativamente, asimismo un 41.3% (19) eligió la opción tal vez.
13. A la pregunta: ¿Cuál considera que es la institución pública en la cual radica la principal causa de impunidad del delito de Fraude Informático? Respondieron a la Policía Nacional un 17.4%(8) del total de encuestados, un 28.3% (13) eligieron la opción Ministerio Público, un 15.2% (7) Poder Judicial, y un 39.1% (18) eligió la opción Entidades bancarias.
14. A la pregunta: Si considera adecuadas las medidas de seguridad para la protección de datos que tienen las entidades bancarias, respondieron afirmativamente un 4.3% (2) del total de encuestados, mientras que un 56.5% (26) respondió negativamente, y un 39.1% (18) eligió la opción tal vez.

Finalmente, se realizó una pregunta abierta a los encuestados: ¿Qué medida(s) sugiere(s) para disminuir o erradicar la comisión del delito de Fraude Informático en nuestro país?, de la cual se obtuvieron las siguientes respuestas:

1. Evitar dejar abierta alguna sesión.
2. Mejores estándares de seguridad en plataformas digitales.
3. A la hora de comprar por internet o se use verificación biométrica desde el celular.
4. Mejorar la promoción de la información en delitos informáticos, renovar ciertas normativas penales para que se adecuen a los delitos informáticos.
5. Promocionar la protección ante delitos informáticos.
6. Mayor protección de las bases de datos.
7. Más difusión de información respecto a transacciones digitales económicas.
8. Cheques gerenciales

A mayor abundamiento procedemos a consignar los datos generales de los 46 encuestados y correos electrónicos respectivamente:

Tabla N° 04

Datos de encuestados sobre Delitos Informáticos – fraude informático vía la plataforma Google Forms

DATOS DE ENCUESTADOS (POBLACIÓN 46)		
N°	NOMBRES Y APELLIDOS	CORREO GMAIL
1	Rebeca Yvonne Flores Ramos	rebe25a@gmail.com
2	Pedro Flores Casimiro	pedroxflores@gmail.com
3	Claudia Susana Clemente Julca	claudia.clementej@gmail.com
4	Melina Ramos Cárdenas	melinamargaritar@gmail.com
5	Giancarlo Jhony Espinoza Gomez	giancarloespinozagomez@gmail.com
6	Christian Enmanuel Flores Ramos	christianfr632@gmail.com
7	Ybet Galindo	ybetgalindo@gmail.com
8	Mateo Dilan Flores Huarez	mateo30f@gmail.com

9	Joseph Mitchell Calixto Ccora	joseph.calixto.ccora@gmail.com
10	Nilton Saravia Yataco	niltonsaravia08@gmail.com
11	Jan Reyes	plocunn1@gmail.com
12	Patricia Carolina Gomero Gomero	carolina_gomero@hotmail.com
13	Fernando Siesquen Vasquez	esiesquen@pj.gob.pe
14	Erika Espinoza Gomez	erikaespinozag@gmail.com
15	Percy Fredy Ríos Luna	prios@colegioparroquialmontserrat.edu.pe
16	Miguel Antonio Ingunza Mendoza	mkct_03@hotmail.com
17	Jean Ñique	ezdeta2603@gmail.com
18	Leonel Quispe Curi	leytokpb@gmail.com
19	Sandy Espinoza Gomez	srocioespinoza@gmail.com
20	Javier Riofrio Ortiz	javier.jro79@gmail.com
21	Geremias André Daryl Carrillo Peña	gerry.daryl@gmail.com
22	Georghette Sutta Morales	georghette20@gmail.com
23	Angello Ferrari Cordero	angelloferraricordero@gmail.com
24	Nekson Pimentel Sanchez	nekson.pimentel@unmsm.edu.pe
25	Alexis Matos	lu220795@gmail.com
26	Roger Jorge Saravia Avilés	rogersaravia18@gmail.com
27	Melissa Rodriguez Olivera	rodriguezmelissa941@gmail.com
28	Maria Victoria Inca Perez	marivicky90@hotmail.com
29	Luis Castillo	betoct99@gmail.com
30	Jean Carlos Sanchez Zegarra	jean161718s@gmail.com

31	Joselyn Gabriela Padilla Romero	pjoselyn1511@gmail.com
32	Maria Alejandra Ramos Ramos	ramos.ramos.maria96@gmail.com
33	José Manuel Mitchell Córdova Lucana	mitchellcr35@gmail.com
34	Mirian Flores Gonzalez	mirian.franari.26@icloud.com
35	Sheyla Gomez Espinoza	gesheyla30@gmail.com
36	Carlos Eduardo Hidalgo Vega	perucehv@outlook.com
37	Paola Medalit Gonzalez Asenjo	pmga-04-27-96@hotmail.com
38	Ibeth Xiomara Torres Quinto	ibeth.xiomi.torres.q@gmail.com
39	José Vargas Galindo	joseph.vargas.g@gmail.com
40	Wilber Luis Ríos Apaza	wluisrios@gmail.com
41	Raquel Nuñez Colquehuanca	rachel.125.17.aqp@gmail.com
42	Miguel Ángel Cortez Vilela	mglcv.mc@gmail.com
43	Aldana Marcela Gutierrez Arellan	Aldana.gutierrez.arellan01@gmail.com
44	Isabel del Carmen Neyra Cerpa	ineyracerpa@gmail.com
45	Lizet Ayzanoa Parra	aparralizet@gmail.com
46	Patricia Ysabel Peñalva Arellano	paty.penalva@gmail.com

Nota: Cuadro de datos de encuestados – población 46 personas

Fuente: Propia

Ante el instrumento recolectado procedemos a realizar la tabulación correspondiente de las respuestas obtenidas graficadas de la siguiente manera:

TABLA 05

Distribución de frecuencias de la Pregunta 01

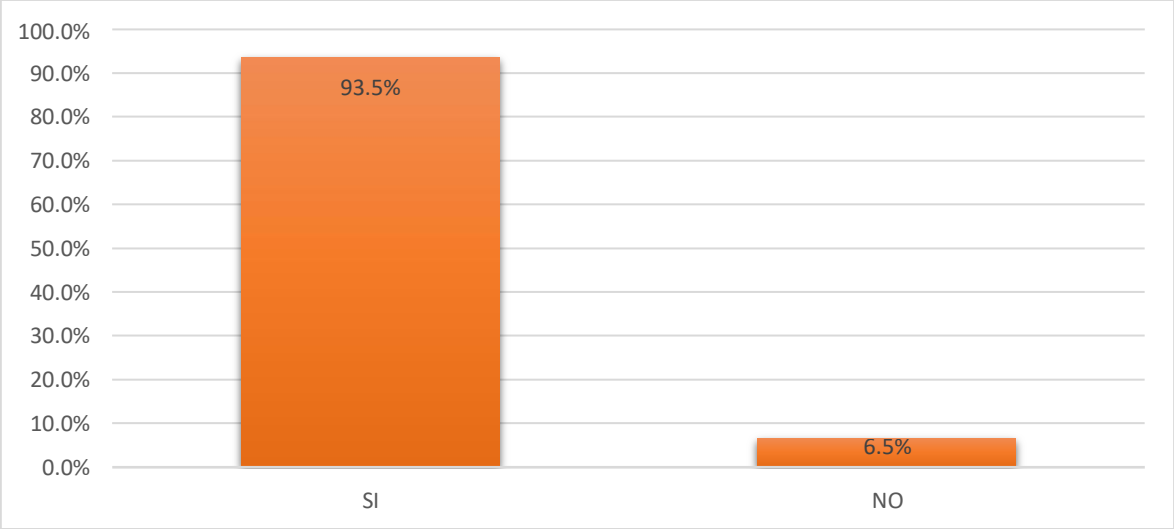
RESPUESTAS	Frecuencia	%
SI	43	93.5%
NO	3	6.5%
TOTAL	46	100%

Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: En la actualidad ¿Dispone de alguna cuenta bancaria? (Cuenta de ahorros, cuenta de plazo fijo, cuenta sueldo o cuenta CTS)

Fuente: Propia

Figura 01

Gráfico de barras de la Pregunta 01



Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: En la actualidad ¿Dispone de alguna cuenta bancaria? (Cuenta de ahorros, cuenta de plazo fijo, cuenta sueldo o cuenta CTS)

Fuente: Propia

Tabla 06:

Distribución de frecuencia de la Pregunta 02

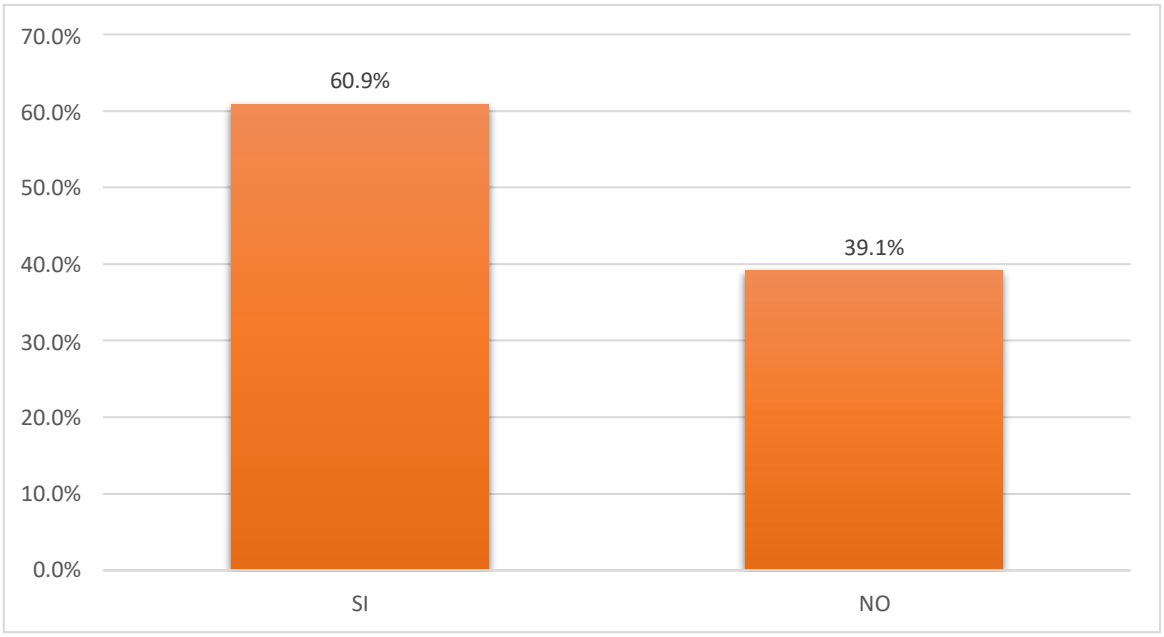
RESPUESTAS	Frecuencia	%
SI	28	60.9%
NO	18	39.1%
TOTAL	46	100%

Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: En la actualidad ¿Cuenta usted con alguna billetera digital?

Fuente: Propia

Figura 02

Gráfico de barras de la Pregunta 02



Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: En la actualidad ¿Cuenta usted con alguna billetera digital?

Fuente: Propia

Tabla 07:

Distribución de frecuencia de la Pregunta 03

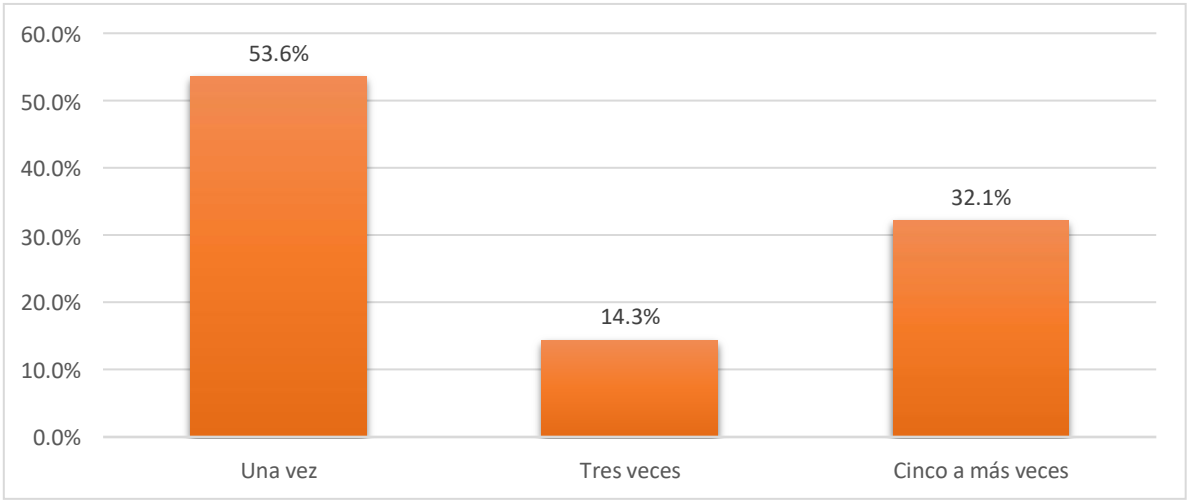
RESPUESTAS	Frecuencia	%
Una vez	15	53.6%
Tres veces	4	14.3%
Cinco a más veces	9	32.1%
TOTAL	28	68%

Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: Si respondió afirmativamente a la pregunta anterior, indique usted ¿con qué frecuencia utiliza dichos aplicativos móviles?

Fuente: Propia

Figura 03

Gráfico de barras de la Pregunta 03



Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: Si respondió afirmativamente a la pregunta anterior, indique usted ¿con qué frecuencia utiliza dichos aplicativos móviles?

Fuente: Propia

Tabla 08:

Distribución de frecuencia de la Pregunta 04

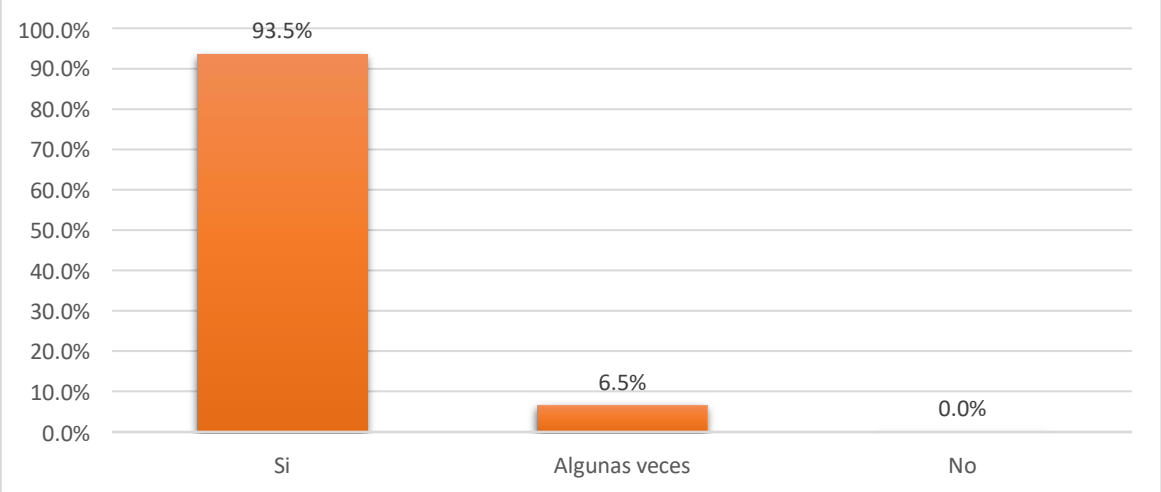
RESPUESTAS	Frecuencia	%
Si	43	93.5%
Algunas veces	3	6.5%
No	0	0.0%
TOTAL	46	100%

Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Alguna vez ha escuchado los siguientes términos: “delitos informáticos”, “ciberdelitos”, “delito cibernético” y/o “ciberdelincuencia”?

Fuente: Propia

Figura 04

Gráfico de barras de la Pregunta 04



Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Alguna vez ha escuchado los siguientes términos: “delitos informáticos”, “ciberdelitos”, “delito cibernético” y/o “ciberdelincuencia”?

Fuente: Propia

Tabla 09:

Distribución de frecuencia de la Pregunta 05

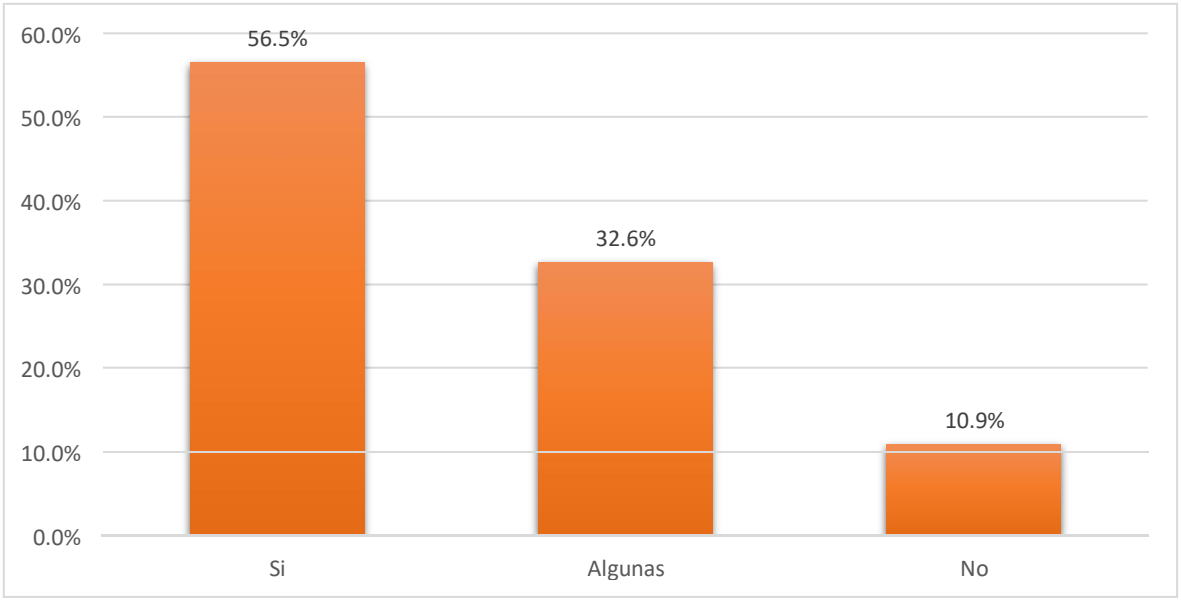
RESPUESTAS	Frecuencia	%
Si	26	56.5%
Algunas	15	32.6%
No	5	10.9%
TOTAL	46	100%

Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Conoces las modalidades del delito de Fraude Informático?

Fuente: Propia

Figura 05

Gráfico de barras de la Pregunta 05



Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Conoces las modalidades del delito de Fraude Informático?

Fuente: Propia

Tabla 10:

Distribución de frecuencia de la Pregunta 06

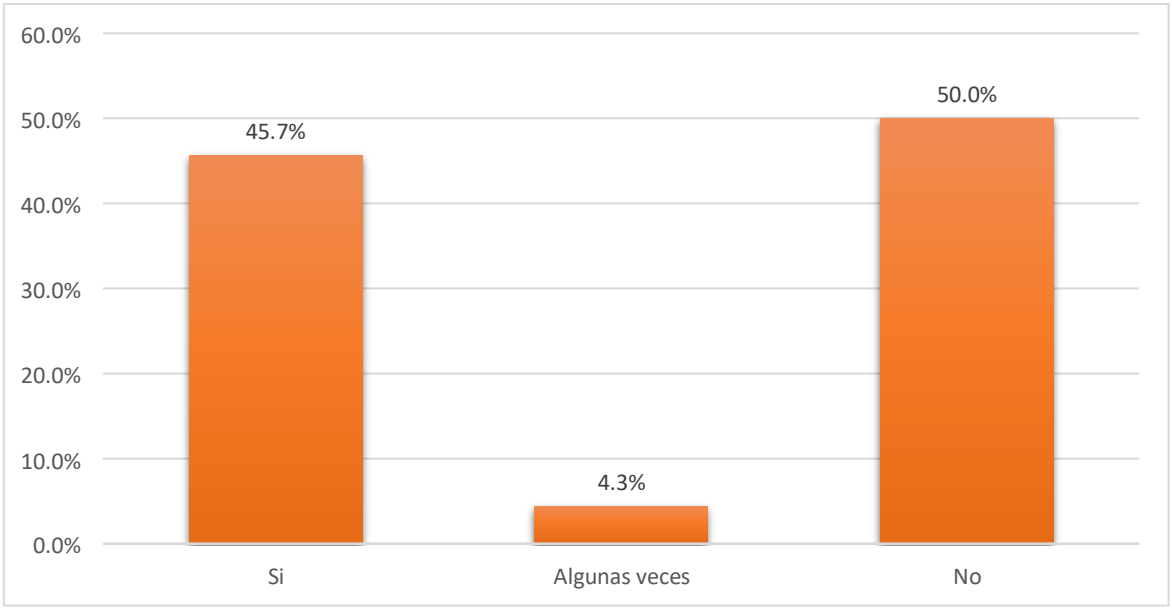
RESPUESTAS	Frecuencia	%
Si	21	45.7%
Algunas veces	2	4.3%
No	23	50.0%
TOTAL	46	100%

Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Alguna vez ha sido víctima o conoce algún caso de delito de Fraude Informático?

Fuente: Propia

Figura 06

Gráfico de barras de la Pregunta 06



Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Alguna vez ha sido víctima o conoce algún caso de delito de Fraude Informático?

Fuente: Propia

Tabla 11:

Distribución de frecuencia de la Pregunta 07

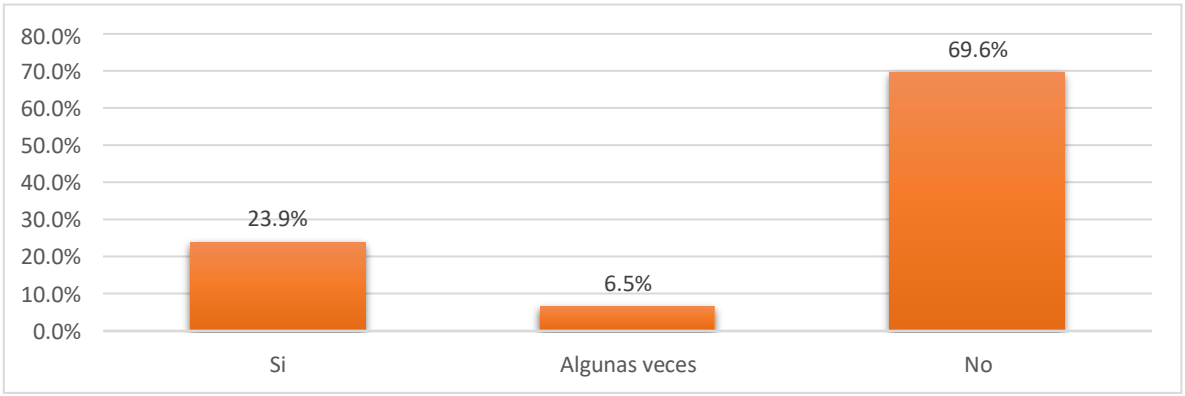
RESPUESTAS	Frecuencia	%
Si	11	23.9%
Algunas veces	3	6.5%
No	32	69.6%
TOTAL	46	100%

Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Alguna vez ha recibido llamada(s) telefónica(s) de un supuesto operador de empresa telefónica (Movistar, Claro, Entel o Bitel), siendo posterior a ello, víctima del robo del saldo de sus datos móviles o de alguna suma de dinero en su cuenta bancaria?

Fuente: Propia

Figura 07

Gráfico de barras de la Pregunta 07



Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Alguna vez ha recibido llamada(s) telefónica(s) de un supuesto operador de empresa telefónica (Movistar, Claro, Entel o Bitel), siendo posterior a ello, víctima del robo

del saldo de sus datos móviles o de alguna suma de dinero en su cuenta bancaria?

Fuente: Propia

Tabla 12:

Distribución de frecuencia de la Pregunta 08

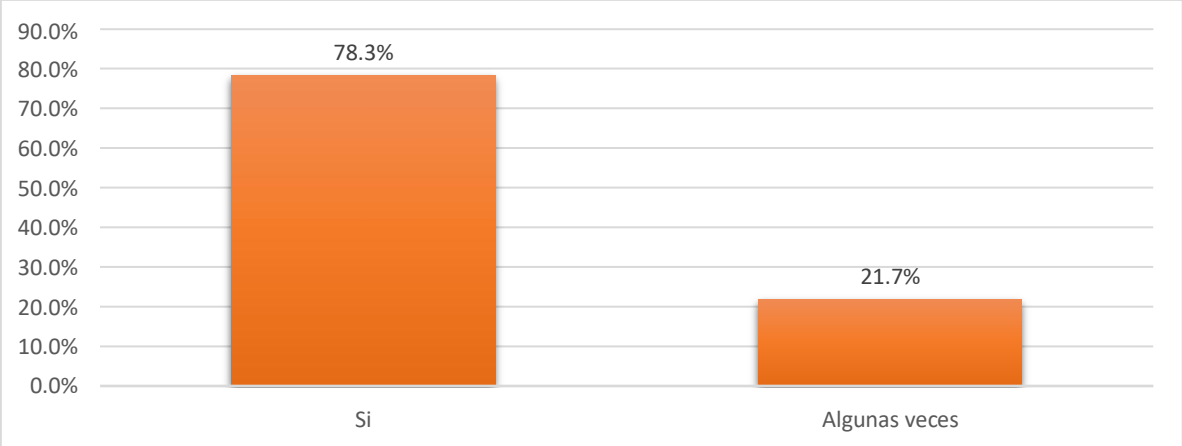
RESPUESTAS	Frecuencia	%
Si	36	78.3%
Algunas veces	10	21.7%
TOTAL	46	100%

Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Alguna vez ha recibido un SMS similar al siguiente enunciado: "BANCO X: Tienes una transferencia retenida de S/.895.98 soles activa tu abono de inmediato en tu cuenta aquí: http:// app-abc,0peracion-web. site"?

Fuente: Propia

Figura 08

Gráfico de barras de la Pregunta 08



Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Alguna vez ha recibido un SMS similar al siguiente enunciado: "BANCO X: Tienes una transferencia retenida de S/.895.98 soles activa tu abono de inmediato en tu cuenta aquí: http:// app-abc,0peracion-web.site"?

Fuente: Propia

Tabla 13:

Distribución de frecuencia de la Pregunta 09

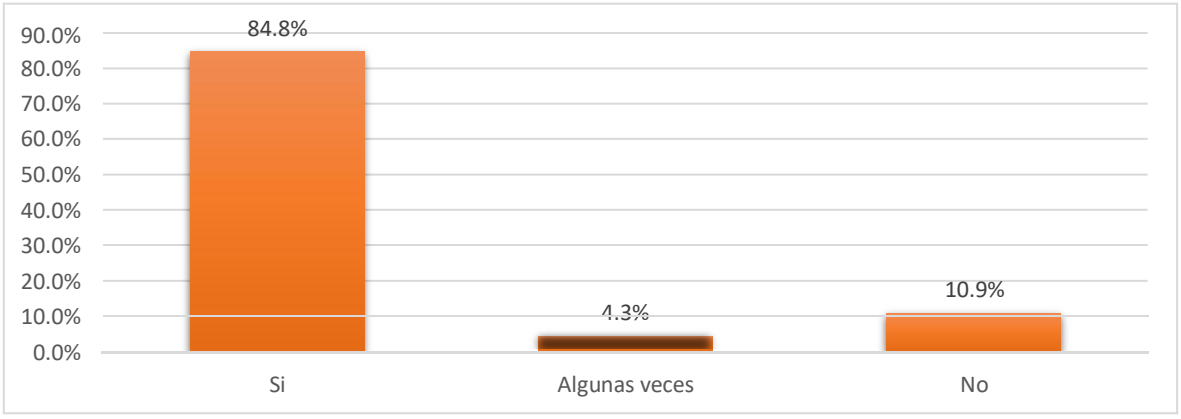
RESPUESTAS	Frecuencia	%
Si	39	84.8%
Algunas veces	2	4.3%
No	5	10.9%
TOTAL	46	100%

Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Ha recibido algún mensaje de texto o llamada telefónica de remitente desconocido, donde le indica que ha ganado un premio de sorteo (automóvil de último modelo o suma de dinero)?

Fuente: Propia

Figura 09

Gráfico de barras de la Pregunta 09



Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Ha recibido algún mensaje de texto o llamada telefónica de remitente desconocido, donde le indica que ha ganado un premio de sorteo (automóvil de último modelo o suma de dinero)?

Fuente: Propia

Tabla 14:

Distribución de frecuencia de la Pregunta 10

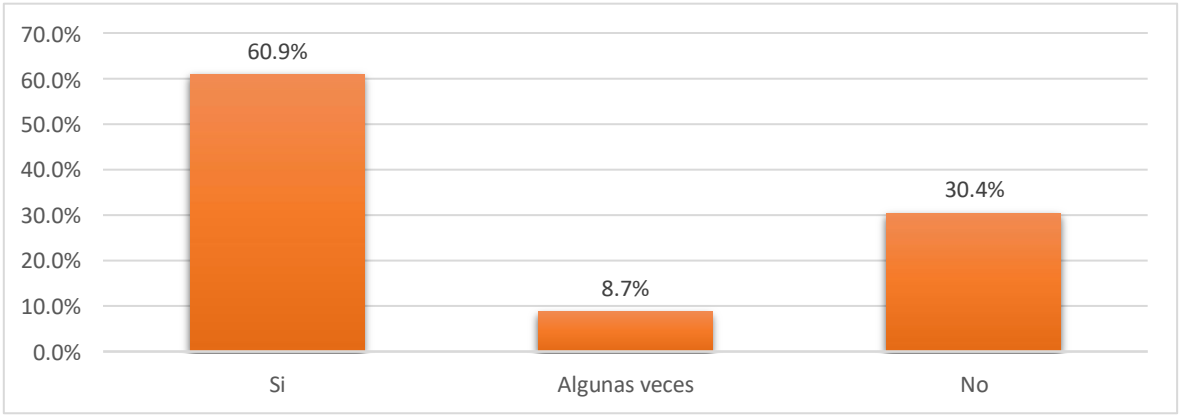
RESPUESTAS	Frecuencia	%
Si	28	60.9%
Algunas veces	4	8.7%
No	14	30.4%
TOTAL	46	100%

Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Ha recibido algún mensaje de texto o llamada telefónica de remitente desconocido, la cual tras ser atendida se escucha “un breve silencio” y/o al colgar dicha llamada advierte su línea móvil como “fuera de servicio”?

Fuente: Propia

Figura 10

Gráfico de barras de la Pregunta 10



Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Ha recibido algún mensaje de texto o llamada telefónica de remitente desconocido, la cual tras ser atendida se escucha “un breve silencio” y/o al colgar dicha llamada advierte su línea móvil como “fuera de servicio”?

Fuente: Propia

Tabla 15:

Distribución de frecuencia de la Pregunta 11

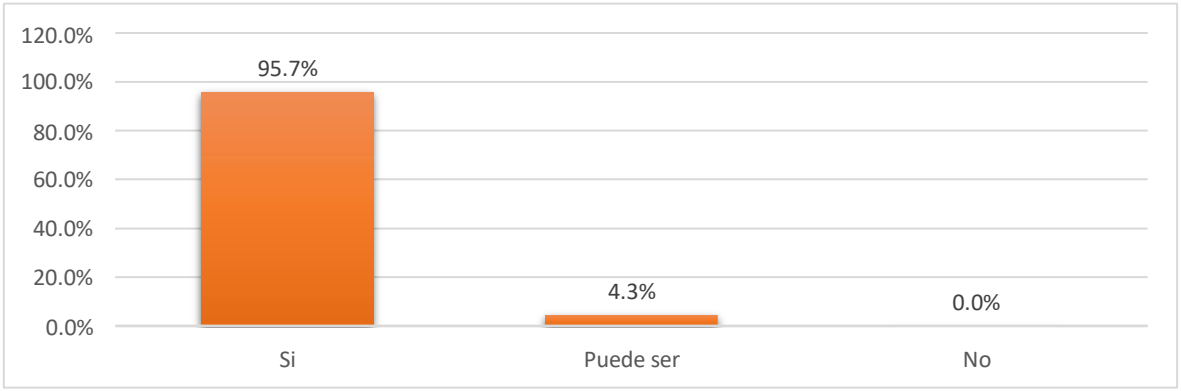
RESPUESTAS	Frecuencia	%
Si	44	95.7%
Puede ser	2	4.3%
No	0	0.0%
TOTAL	46	100%

Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Ha recibido algún mensaje de texto o llamada telefónica de remitente desconocido, la cual tras ser atendida se escucha “un breve silencio” y/o al colgar dicha llamada advierte su línea móvil como “fuera de servicio”?

Fuente: Propia

Figura 11

Gráfico de barras de la Pregunta 11



Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Ha recibido algún mensaje de texto o llamada telefónica de remitente desconocido, la cual tras ser atendida se escucha “un breve silencio” y/o al colgar dicha llamada advierte su línea móvil como “fuera de servicio”?

Fuente: Propia

Tabla 16:

Distribución de frecuencia de la Pregunta 12

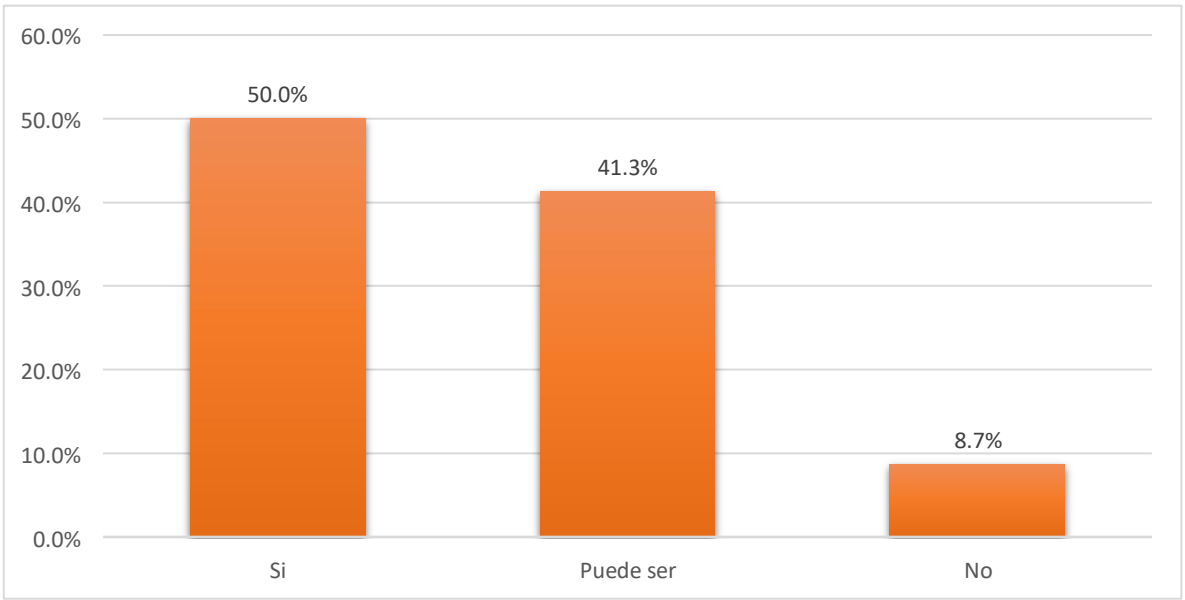
RESPUESTAS	Frecuencia	%
Si	23	50.0%
Puede ser	19	41.3%
No	4	8.7%
TOTAL	46	100%

Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Cree usted que los delitos de Fraude Informático quedan impunes?

Fuente: Propia

Figura 12

Gráfico de barras de la Pregunta 12



Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Cree usted que los delitos de Fraude Informático quedan impunes?

Fuente: Propia

Tabla 17:

Distribución de frecuencia de la Pregunta 13

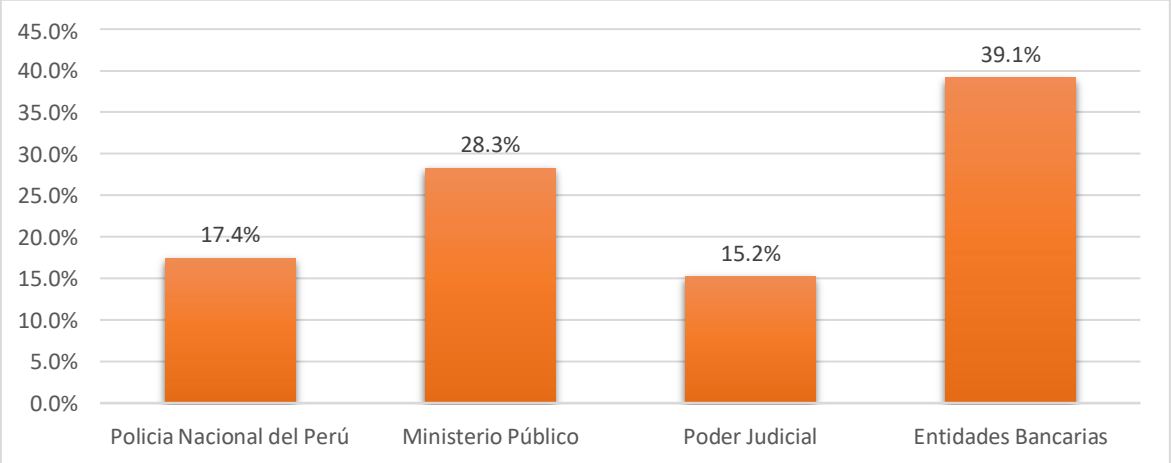
RESPUESTAS	Frecuencia	%
Policía Nacional del Perú	8	17.4%
Ministerio Público	13	28.3%
Poder Judicial	7	15.2%
Entidades Bancarias	18	39.1%
TOTAL	46	100%

Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿En qué institución pública considera que radica la principal causa de impunidad del delito de Fraude Informático?

Fuente: Propia

Figura 13

Gráfico de barras de la Pregunta 13



Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿En qué institución pública considera que radica la principal causa de impunidad del delito de Fraude Informático?

Fuente: Propia

Tabla 18:

RESPUESTAS	Frecuencia	%
Si	23	50.0%
Puede ser	19	41.3%
No	4	8.7%
TOTAL	46	100%

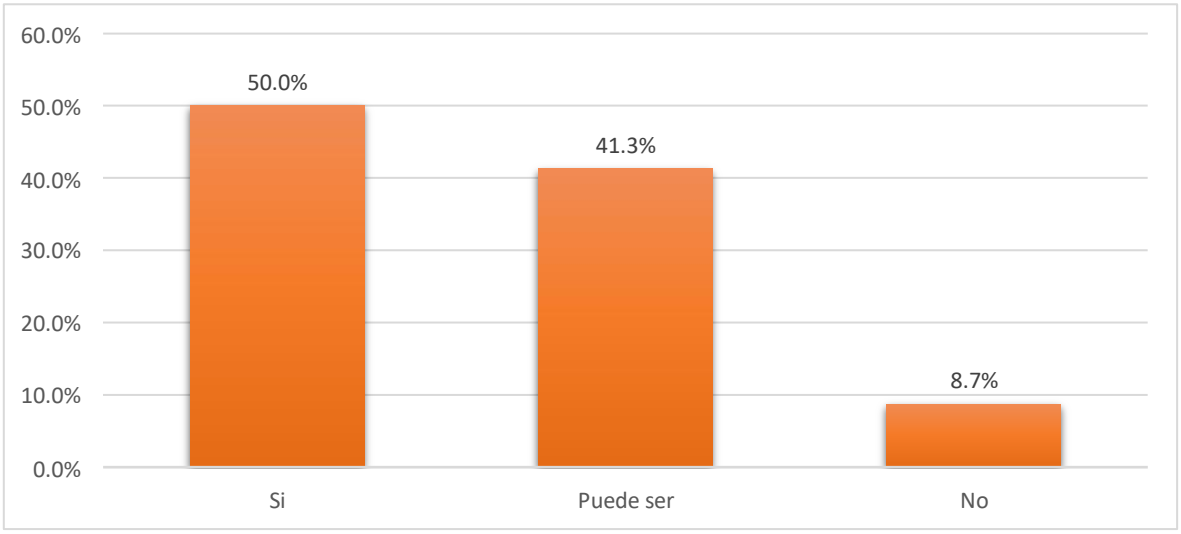
Distribución de frecuencia de la Pregunta 14

Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Cree usted que las medidas de seguridad para la protección de datos que tienen las entidades bancarias, son las adecuadas?

Fuente: Propia

Figura 14

Gráfico de barras de la Pregunta 14



Nota: Porcentaje de las respuestas brindadas por los participantes de la Encuesta sobre Delitos Informáticos – Fraude Informático, sobre la pregunta: ¿Cree usted que las medidas de seguridad para la protección de datos que tienen las entidades bancarias, son las adecuadas?

4.1.1. Entrevista

La segunda etapa constó de aplicar la Guía de entrevista a los especialistas en el ámbito penal, siendo entrevistados 3 jueces penales de Lima, 1 asistente de relatoría de sala penal de Lima, quienes radican en la ciudad de Lima.

Dentro del proceso de ejecución del presente trabajo de tesis, con la finalidad de dar cumplimiento a los objetivos generales y específico, se obtuvieron los siguientes resultados:

OBJETIVO GENERAL Nº 01: Determinar las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático en Lima durante el periodo del 2019-2021.

TABLA N° 19

Respuesta de los especialistas en relación a la pregunta 1 de la entrevista

¿Cómo define usted el concepto de Fraude Informático como institución jurídica, regulada por el Artículo 8° de la Ley Nº 30096?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Juez 1	El incremento en el uso de la tecnología ha generado contrapartida, que con ello se obtenga información de las contraseñas de las tarjetas de créditos, así como de las cuentas a través de medios fraudulentos, sea por llamadas telefónicas, mensajes de texto, correos electrónicos, etc., en forma similar o tan igual las entidades a entidades bancarias generando confusión en los clientes y con ello la pérdida de responsabilidad de estos.	Conciertan refiriendo que el delito de fraude informático es aquel ilícito penal destinado al diseño, introducción de datos, alteración, todo ello a fin de obtener un provecho patrimonial a través del uso de las TIC.	Ninguna
Asistente de Sala	Es aquel ilícito penal que se comete empleando la tecnología de la información o de la comunicación, para obtener un provecho ilícito por parte del sujeto activo, ya sea introduciendo, alterando, clonando, etc. datos informáticos o manipulando un sistema informático.		
Coronel de la	Lo que indica el Código el que diseña, introduce datos, altera, para obtener un provecho patrimonial, sin esa característica no habría		

DIVINDAT	delito, u obtener cualquier otra ventaja, utilizando los medios informáticos, donde el objeto del delito es otra cosa, en los delitos informáticos se utiliza la PC como medio del delito (delito de fraude informático) o como objeto del delito (cuando meten un Ransomware para secuestrar los datos y encripta su disco duro – es un ataque directo al sistema informático).		
Asesor del Gabinete de Asesores de la Fiscalía de la Nación	Es aquella conducta que consiste en diseñar; introducir, alterar, borrar, suprimir, clonar de datos informáticos o interferir o manipular el funcionamiento de un sistema informático, mediante el uso de las TIC's (tecnologías de la información o de la comunicación), con la finalidad de obtener para sí o para otro un provecho ilícito en perjuicio de tercero.		
Resultado	Fraude informático: es aquel ilícito penal destinado al diseño, introducción de datos, alteración, todo ello a fin de obtener un provecho patrimonial a través del uso de las TIC, además colegimos la imputación objetiva del agraviado.		

Fuente: *Propia*

TABLA 20:

Respuesta de los especialistas en relación a la pregunta 2 de la entrevista

De acuerdo a su experiencia, en términos porcentuales, ¿Cuál cree usted que es la incidencia de denuncias relacionadas al delito de Fraude Informático entre los Delitos Informáticos en Lima durante el periodo 2019 - 2021?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Juez 1	No tengo acceso a un número porcentual, pero desde que asumí este despacho, desde noviembre del 2021 hasta la actualidad mayo del 2022, se han tramitado 3 expedientes 2 de ellos con terminación anticipada. Considero que no solo debe establecerse multas a la entidad financiera en el caso que no remita información, sino que en el caso de que los sentenciados sean trabajadores de las entidades financieras, pues a través de ellos son quienes tienen acceso a información privilegiada deben responder como terceros civilmente responsables.	Convergen en que, si existen denuncias tramitadas a nivel fiscal y judicial en Lima Centro.	La Magistrada Carrillo refiere que en su despacho se ha tramitado 3 expedientes, la abogada Ramos señala que existe un 70% y el coronel Huamán señala que al primer trimestre del 2022 existen 2,012 casos, el Fiscal Vílchez indica
Asistente de Sala	Un 70% tomando en cuenta que hoy en día la tecnología es un medio muy recurrido por la mayoría de personas.		

Coronel de la DIVINDAT	No cuento con la data de otros años solo de este año, al primer trimestre del año 2022 se ha reportado un total de 2012 denuncias a nivel Lima Metropolitana, a nivel nacional es visto por otra unidad. Si todas las denuncias llegan a la división como son investigadas, por norma la DIVINDAT debe aceptar todas las denuncias (así no sean de su competencia), la división transfiere al Ministerio Público y como sugerencia indica que: esta investigación debe ser vista por la DIPINCRI invocando el protocolo; cuando no ponemos sugerencias se entiende que será visto por la DIVINDAT, se colige que no todas las denuncias ingresadas son vista por la DIVINDAT, ante ello, hemos coordinado con la séptima región policial de Lima para que sean capacitados la DIPINCRI y las Comisarías, también cuando nos piden hacemos charlas educativas a las mismas comisarias DIPINCRI, como unidad sugiere que se dé estricto cumplimiento al Protocolo.		que la incidencia de denuncias por fraude informático se ubica en el tercer escalafón a nivel de delitos en Lima.
Asesor del Gabinete de Asesores de la Fiscalía de la Nación	Aproximadamente, debe ubicarse en el tercer escalafón de denuncias, después de los delitos contra la libertad e identidad sexual y de los delitos contra el patrimonio.		

Resultado	Se colige que, si existen denuncias tramitadas a nivel fiscal y judicial en Lima Centro, y que existe un alto índice de ella.

Fuente: *Propia*

TABLA 21:

Respuesta de los especialistas en relación de la pregunta 3 de la entrevista

¿Qué deficiencias legislativas puede advertir en el Artículo 8° (Fraude Informático) de la Ley N° 30096 – Ley de Delitos Informáticos?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Juez 1	Considero que no solo debe establecerse multas a la entidad financiera en el caso que no remita información, sino también en el caso de que los sentenciados sean trabajadores de las entidades financieras pues a través de ellos son quienes tienen acceso a información privilegiada deben responden como terceros civilmente responsables.	Concuerdan con el postulado de que existen deficiencias legislativas en el artículo 8° (fraude informático).	La magistrada Carrillo señala multas para las entidades bancarias, la abogada Ramos indica que la norma no regula todas las modalidades del fraude informático, y el coronel Huamán refiere que se debe señalar que los verbos rectores se
Asistente de Sala	Que se encuentran vacíos legales en dicha legislación toda vez que no regula todas las modalidades de delinquir a través de los medios informáticos, siendo que hoy en día existen diversas formas de delinquir mediante el uso de la tecnología.		
Coronel de la DIVINDAT	Los verbos rectores deben ser entendidos de forma copulativa y exclusiva, por ejemplo cuando la norma indica: “el que deliberada e ilegítimamente procura para si u otro un provecho ilícito en perjuicio		

	de un tercero, mediante el diseño", que sucede cuando hace un diseño si no lo utiliza, no ha cometido aún el delito de fraude, puede entenderse que los verbos rectores deben aplicarse de forma dos o más, aclara que para la comisión del delito debe haber un despojo patrimonial de la víctima todo lo demás quedaría en tentativa, el delito es de resultado.		dan copulativa y exclusivamente, y el Fiscal Vílchez indica que el tipo penal no se encontraría bien estructurado.
Asesor del Gabinete de Asesores de la Fiscalía de la Nación	Desde una perspectiva dogmática, el tipo penal prevé, de manera innecesaria, un elemento subjetivo de tendencia interna trascendente el cual consiste en "para obtener un provecho ilícito para sí o para otro"; siendo que, la lesión a la integridad y secreto del sistema informático se encuentre efectivo, indistintamente que pueda generar un beneficio económico o de otra índole en el sujeto activo.		
Resultado	Existen deficiencias legislativas en el artículo 8° a nivel estructura (modificables) y a nivel político penal (agregar penas).		

Fuente: Propia

TABLA 22:

Respuesta de los especialistas en relación a la pregunta 4 de la entrevista.

¿Cuál cree usted que sea el principal motivo por el cual se archivan a nivel preliminar las investigaciones por fraude informático?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Juez 1	Por desconocimiento solo que los afectados desconocen y otros prefieren no invertir tiempo y dinero. Existen dos caminos, depende si la entidad financiera ha enviado la constancia de transacción o no. El primero, si no ha enviado la constancia de transacción, se realiza un reclamo a la entidad financiera quien resuelve rechazar, indicando que es responsabilidad del cliente "la reserva" de la clave; sin embargo, es obligación de esta, enviar el envío del comprobante de la transacción y no ha sido autorizado se procede con la denuncia respectiva, que por obvias razones no pueden ser archivadas. Ambos caminos son exitosos.	Coinciden en que se realiza el archivo a nivel preliminar por mal tratamiento a las denuncias a nivel procedimental, la magistrada Carrillo señala que por no invertir tiempo y dinero, la abogada Ramos indica que por los vacíos legales que provocan la impunidad de los delitos, y el	Disciernen que, la Magistrada Carrillo responsabiliza a la víctima, la abogada Ramos a la norma, y el coronel Huamán al Ministerio Público, y el Fiscal Vílchez refiere que el principal motivo del archivo radicaría en el juicio oral.
Asistente de Sala	Que no se encuentra debidamente regulados, por lo que en muchas ocasiones quedan como atípicos, siendo archivados, en otros casos se da porque el sistema de investigación para este tipo de delitos resulta ineficiente no logrando en muchos casos dar con el		

	responsable.	coronel Huamán refiere que por la postura que adopta el Ministerio Público (teoría funcionalista del Derecho penal).	
Coronel de la DIVINDAT	Muchos fiscales adoptan la teoría funcionalista del derecho penal, apuntan a las ideas de Roxin respecto a la imputación objetiva, teoría de riesgos aquel que cree un riesgo entonces comete delito, se crea el riesgo al poseer bienes de cuidado, uno mismo crea el riesgo, es el criterio de los fiscales, son partidarios de la víctima o dogmática, es decir, se echa la culpa al usuario. Les comento hacer de un tema álgido de la criminalidad, por ejemplo, el famoso cuento de la maleta (delito de estafa agravada) mediante el uso de las TIC también para suplantar la identidad, se da cuando uno está navegando en Facebook y les llega una solicitud de amistad (de un familiar del extranjero) acepta la solicitud y comienzan a conversas, ojo que es el un perfil clonado, entre las conversaciones le indican que su familiar está a punto de viajar a Perú se encuentra en el aeropuerto, pero tiene un problema no puede viajar por no tener la vacuna, pero sus maletas ya están en el avión quiere coordinar con la víctima para que lo reciba, dentro de ellas hay tablets, iPhone, celulares, perfumes, entre otros (cosas caras), el delincuente le dice que dará un teléfono por el favor de recibir la maleta, le solicita su DNI y datos para que la maleta llegue a su domicilio, la		

	comunicación ya se da por el WhatsApp, luego de unas horas llaman a la víctima por el tema de una maleta le comunican que la maleta en el aeropuerto está excediendo de peso que se pondrá a decomiso y que debe pagar una penalidad, solicitando pago S/.17,000.00 Soles para que la maleta sea liberada y pase, indican una cuenta bancaria (cuenta receptora) del servicio de mensajería y transporte, horas después, llaman a la víctima identificándose como la SUNAT refiriendo que el equipaje fue pasado por los rayos X y se ha encontrado dinero en efectivo dentro de las laptops (remiten video de una simulación), la víctima llama al delincuente quien le indica que pague y que del dinero le dará una parte, la víctima solicita le indique cuanto debe pagar y le indican S/.50,000.00, algunas víctimas se dan cuenta y denuncian otros pagan; de todo ello quienes son los actores, en primer lugar el ingeniero social (quien rastrea los datos), diseña la suplantación por Facebook, el inductor el que dialoga, la víctima, supuesto agente de aduanas, todos sin identificarse, quien es el único que se puede identificar, el dueño de la cuenta receptora, ¿se puede producir el delito sin la cuenta receptora? No se puede porque no habría como recibir el dinero, puesto que toda la recepción del dinero es a través de las TIC, ellos no toman en cuenta los fiscales, por tanto, la gran		

	mayoría sale en libertad.		
Asesor del Gabinete de Asesores de la Fiscalía de la Nación	No necesariamente el archivo, a nivel de diligencias preliminares; empero, sí puede generar el sobreseimiento de la causa o la dificultad probatoria para el Ministerio Público, en su estrategia acreditativa en el juicio oral.		
Resultado	Se archivan los casos por mal tratamiento a las denuncias a nivel procedimental y a nivel de aplicación de la norma, por otro lado, también radicaría en la víctima y en la estructura del proceso.		

Fuente: *Propia*

OBJETIVO ESPECÍFICO Nº 01: Definir las razones por las que se debe mejorar o erradicar las deficiencias legislativas en el artículo 8° de la Ley N° 30096.

TABLA 23:

Respuesta de los especialistas en relación a la pregunta 5 de la entrevista.

¿Considera usted que mejorar la estructura normativa del delito de Fraude Informático estipulado en el Artículo 8° de la Ley N° 30096 – Ley de Delitos Informáticos, coadyuvará a la prevención del delito?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Juez 1	Considero que más que mejorar la estructura del delito, son las entidades financieras las que deben mejorar sus medidas de seguridad en el acceso a la base de datos a su sistema. El acceso a estas se está tomando tan común que incluso lo hacen por montos mínimos y a diario que los clientes no se percatan y hace que pasen desapercibidos.	Convienen en que efectivamente el artículo 8° merece mejoras a nivel estructural. La abogada Ramos señala que con ello se permitirá que los delitos no queden impunes, y el coronel Huamán indica que los verbos rectores deben darse copulativa	En oposición expresa la magistrada Carrillo quien indica que las entidades financieras deben mejorar sus medidas de seguridad en el acceso a la base de datos de su
Asistente de Sala	Sí, en definitiva, ya que, con una mejor implementación de la estructura normativa para el fraude informático, hace que estos delitos especiales sean sancionados de una manera adecuada y em definitiva hace que los delincuentes sepan que este tipo de delitos no quedarán impunes y de ser el caso serán sancionados		

	con una pena ejemplar, previniendo de una u otra manera el incremento masivo de este tipo de delitos.	y que el artículo debe apoyarse del Protocolo de trabajo conjunto con el Ministerio Público.	sistema, y el Fiscal Vílchez señala que la normativa no debería ser modificada sino se debería implementar la posibilidad de determinar una política criminal y pública que eduque el respeto a los datos o sistemas informáticos.
Coronel de la DIVINDAT	Si claro, en primer lugar, indicar que los verbos rectores deben darse de forma copulativa y no solamente excluyente, además el artículo 8° debe ser apoyado por el Protocolo de trabajo conjunto con el Ministerio Público, en cuanto a la pena se sugiere prisión preventiva no menos de un año para la cuenta receptora, en cuanto a la aplicación de una medida cautelar, esta debe darse a nivel administrativo o civil.		
Asesor del Gabinete de Asesores de la Fiscalía de la Nación	No, el tópico de la prevención general o especial del delito no responden a las modificaciones dogmáticas en el tipo penal; sino, en la posibilidad de establecer una Política Criminal y Política Pública que enseñen el respeto a la integridad de los datos o sistemáticos informáticos ajenos para motivar una conducta socialmente adecuada.		
Resultado	El artículo 8° (fraude informático) merece mejoras a nivel estructura (verbos rectores), aunado a ello, las entidades bancarias merecen mejora en sus medidas de seguridad, además del aumento de política criminal y pública.		

Fuente: *Propia*

TABLA 24:

Respuesta de los especialistas en relación a la pregunta 6 de la entrevista.

¿Qué opinión merece el aumento progresivo en la comisión del delito de Fraude Informático y el uso de las tecnologías digitales para tal fin?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Juez 1	Como lo acabo de indicar en la respuesta anterior, el uso de esta modalidad de están volviendo tan común, que se torna inseguro el uso de tarjetas de crédito.	Concuerdan en que efectivamente existe un aumento crítico en la comisión del delito de fraude informático, la magistrada Carrillo señala que es una modalidad que se está volviendo muy común para los delincuentes, para la abogada Ramos es una situación aprovechada por los	Ninguna
Asistente de Sala	Pues que es una lástima que hoy en día, algo como lo que es la tecnología sea utilizada por personas inescrupulosas para cometer este tipo de delitos como lo son el fraude informático, tomando en cuenta que en la actualidad la tecnología es un medio muy recurrido por la mayoría de personas.		
Coronel de la DIVINDAT	Todo comenzó con la pandemia y el uso masivo del internet, entonces ha hecho que la gente ya no salga a consumidor donde hasta era de libre acceso, puesto que no había pandemia, las compras por internet también se han masificado, se volvió tendencia, por ello se utilizaron mucho las TIC, no se puede		

	recomendar no usar los móviles, pero si se puede sugerir el control del rubro de las comunicaciones, la seguridad informática, la cultura de cibers, nosotros mismos somos culpables; un sistema informático está compuesto de tres elementos: hardware, Software y el Humanware (el hombre), siendo el más débil el Humanware, es el responsable, por ejemplo: el phishing, uno sabe que no debe hacer click en un link que son de dudosa procedencia, por eso cuando ustedes vean una página de dudosa procedencia deben copiar el dominio (URL) y colocarlo en páginas amigables, como: whois, exsalion o this person does not exist (se colocan en el buscador de Google) se coloca y busca el dominio e informe, por ejemplo: sale una publicación en Facebook que dice: "Vendo casa", copias el URL lo colocas en la página amigable y sale un informe de cuando fue creada, quien lo creo, el administrador, si esta todo privado debes dudar porque puede ser una página creada para estafar, si ha sido creada recientemente puede ser una página creada para estafar, estas son páginas amigables de inteligencia artificial.	inescrupulosos, para el coronel Huamán es producto de la pandemia y la masificación del uso de la internet, además del desconocimiento de las páginas amigables para el público usuario, y para el Fiscal Vílchez aconseja que se debería optar por optimizar la tecnología para desarrollar nuevas técnicas especiales de investigación.	
Asesor del Gabinete de	El avance de las TIC's se encuentra en consonancia con el desarrollo de la ciencia; en consecuencia, son instrumentos		

Asesores de la Fiscalía de la Nación	socialmente aceptados, los que, lamentablemente, pueden ser usados para fines ilícitos, aún delictivos; sin embargo, no se puede limitar su uso porque iría en contra de la misma naturaleza del conocimiento humano. Lo que podría evaluarse, es optimizar la misma tecnología para desarrollar nuevas técnicas especiales de investigación que lucha contra esta clase de criminalidad.		
Resultado	Existe un aumento progresivo y crítico de la cibercriminalidad, ello producto del uso masivo e indiscriminado de la internet, por tanto, es imperativo optimizar la tecnología a fin de desarrollar nuevas técnicas especiales de investigación.		

Fuente: Propia

OBJETIVO ESPECÍFICO Nº 02: Analizar las propuestas que mejoran o erradican las deficiencias legislativas en el artículo 8° de la Ley N° 30096.

TABLA 25:

Respuesta de los especialistas en relación a la pregunta 7 de la entrevista.

¿Qué opinión merece el planteamiento del incremento presupuestal de las siguientes instituciones públicas: DIVINDAT, Fiscalía de Ciberdelincuencia y Juzgados Penales, con la finalidad de reducir y/o erradicar la comisión del delito de Fraude Informático?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Juez 1	Como lo he indicado en mi respuesta 4, la mejor forma de prevenir esta clase de delito, es que las entidades financieras, bancarias, etc., adopten medidas de seguridad al respecto.	El coronel Huamán, el fiscal Vílchez y la abogada Ramos coinciden que efectivamente la DIVINDAT merece un aumento, para fines de mejora en sus herramientas tecnológicas, agrega el	La magistrada Carrillo señala que los que deben mejorar son las entidades financieras sobre sus medidas de seguridad.
Asistente de Sala	Pues me parece un buen planeamiento, tomando en cuenta que, con el uso de mayores implementos tecnológicos, se podría hacer una mejor y adecuada investigación por parte de las instituciones públicas antes mencionadas y por consiguiente realizar una adecuada investigación que permita identificar a los ciberdelincuentes.		
Coronel de la	Si, se necesitan más herramientas, ustedes saben que el delito		

DVINDAT	evoluciona los delincuentes se implementan de herramientas tecnológicas importantes, nosotros también nos estamos quedando atrás y necesitamos renovar nuestros equipos, se necesitan herramientas de última generación, por ejemplo: Inteligencia Artificial (IA) de Oracle Cloud Infrastructure (OCI), inteligencia de fuente abierta.	Fiscal que a la fecha no existen juzgados penales especializados en la materia de ciberdelitos	
Asesor del Gabinete de Asesores de la Fiscalía de la Nación	Resulta correcto, toda vez que permitirá desarrollar nuevas líneas de indagación en la lucha contra la ciberdelincuencia. Conviene anotar que, actualmente, no existen juzgados penales especializados en la materia.		
Resultado	Se establece que la DIVINDAT merece un aumento en su presupuesto anual, para fines de mejorar el equipo tecnológico.		

Fuente: Propia

TABLA 26:

Respuesta de los especialistas en relación a la pregunta 8 de la entrevista.

¿Considera pertinente la aplicación de normas análogas del Derecho Penal, peruano o internacional, ante las deficiencias legislativas del delito de Fraude Informático?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Juez 1	La simplificación en el trámite, así como que no solo incluye la recuperación del patrimonio sustraído porque finalmente dicho monto va para la entidad financiera quien decide devolverle el monto no reconocido. Ello debe incluir los gatos asumidos innecesariamente como repito porque la entidad financiera no adopta las medidas de seguridad en el acceso de la base de datos a sus clientes.	La abogada Ramos, el fiscal Vílchez y el coronel Huamán concuerdan en que, al margen de los convenios sobre la ciberdelincuencia, se debe acudir a ellas ante vacíos o deficiencias, además que resultaría necesaria su aplicación a fin de optar por el mejor modelo legislativo	Discrepa la magistrada Carrillo reitera que las entidades financieras merecen mayor atención.
Asistente de Sala	Claro que sí, sin dejar de lado que también el Perú tiene convenios sobre la ciberdelincuencia con una serie de tratados europeos.		
Coronel de la DIVINDAT	Si se encuentran vacíos o deficiencias en la ley, hay que acudir a normas extra penales o administrativas, o interpretaciones sistemáticas de las normas, pero teniendo en cuenta el Principio		

	de Legalidad.	adaptable.	
Asesor del Gabinete de Asesores de la Fiscalía de la Nación	El análisis Comparado de Derecho, a fin de revisar las legislaciones extranjeras, como, principalmente, el estudio Convencional (Convención de Budapest), resulta necesario para optar por un modelo legislativo que permita la eficiencia y eficacia de la punición del tipo penal de fraude informático.		
Resultado	Se considera pertinente la aplicación de normativa análoga ante vacíos legislativos, y se subraya que el país se encuentra suscrito a convenios europeos referentes a ciberdelincuencia.		

Fuente: Propia

TABLA 27:

Respuesta de los especialistas en relación a la pegunta 9 de la entrevista.

De acuerdo a su experiencia ¿Qué medida o medidas complementarias a la interposición de la denuncia del agraviado por el delito de Fraude Informático, se podrían implementar legislativamente con el objetivo de retrotraer el daño causado al estado anterior de la comisión del delito (Recuperación inmediata del patrimonio sustraído)?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Juez 1	La simplificación en el trámite, así como que no solo incluye la recuperación del patrimonio sustraído porque finalmente dicho monto va para la entidad financiera quien decide devolverle el monto no reconocido. Ello debe incluir los gatos asumidos innecesariamente como repito porque la entidad financiera no adopta las medidas de seguridad en el acceso de la base de datos a sus clientes.	Concilian en que se deben adoptar medidas complementarias tales como: la magistrada Carrillo señala que debe haber simplificación en el trámite, y el coronel Huamán refiere que complementaria el resarcimiento del daño mediante las medidas reales.	Diverge la abogada Ramos quien indica que sería difícil recuperar el bien, que lo más conveniente sería la prevención del usuario, además que el Fiscal Vílchez señala que de igual modo la recuperación del patrimonio hurtado en el delito de fraude informático es difícil de
Asistente de Sala	Creo que en muchos casos la recuperación inmediata del patrimonio sustraído es complicado, creo que la mejor prevención para este tipo de delitos, en definitiva, es tomar conocimiento de los beneficios como problemáticas del uso desmesurado de la tecnología y proteger el uso de nuestros datos, o ante un robo o hurto de pertenencias como DNI, etc., hacer la denuncia		

	correspondiente, ya que en muchos casos el descuido de los ciudadanos permite que personas inescrupulosas, hagan uso de estos descuidos para suplantar identidades, o realizar fraudes informáticos que luego cuando nos damos cuenta estos en algunos casos pueden ser prevenidos.		recuperar pues el delito ya está consumado, y que lo más próximo que se encontraría sería el resarcimiento a nivel de la reparación civil.
Coronel de la DIVINDAT	Resarcir el daño, aplicación de medidas reales, incautación de los medios comisivos, extinción de dominio, aquí algunas veces no hacemos extinción dominio eso deberíamos informar.		
Asesor del Gabinete de Asesores de la Fiscalía de la Nación	La recuperación inmediata de información o patrimonio, sobre la base del fraude informático, resulta difícilmente obtenible. Indistintamente de ello, el delito ya está consumado. La recuperación del patrimonio estaría más orientado al momento de la reparación civil.		
Resultado	Se debe adoptar medidas complementarias a la denuncia interpuesta, simplificación del trámite y aplicación de medidas reales, *empero,* se encuentra difícil que se llegue a realizar la recuperación del patrimonio hurtado.		

Fuente: Propia

OBJETIVO ESPECÍFICO N° 03: Establecer propuestas que coadyuven a mejorar o erradicar las deficiencias legislativas en el artículo 8° de la Ley N° 30096.

TABLA 28:

Respuesta de los especialistas en relación a la pregunta 10 de la entrevista.

¿Qué opina usted de la implementación de un registro de denuncias de delitos de Fraude Informático, bajo el control de la Superintendencia de Banca, Seguros y AFPs?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Juez 1	Es una excelente propuesta a efectos de que los clientes puedan tener reconocimiento en que entidad financiera, banco tiene mayores denuncias y no confiar sus fondos.	Conciertan la magistrada Carrillo, el fiscal Vílchez y la abogada Ramos en que en efecto se debería implementar dicha medida a fin de la SBS cumpla sus funciones.	Difiere el coronel Huamán quien señala que existe el registro de denuncias de delitos de fraude informático, pero es de carácter confidencial entre la PNP y los bancos.
Asistente de Sala	Me parece una buena idea, la implementación de un registro de denuncias bajo el control de la SBS ya que esta institución tiene como fin propiciar una mayor confianza y protección de los intereses del público usuario, ejerciendo control y supervisión de las entidades bancarias, siendo estas entidades en donde más se cometen los fraudes informáticos y en los que los usuarios en muchos casos son los más perjudicados.		
Coronel de la	Tenemos, pero es confidencial, no podemos compartirlo, con que		

DIVINDAT	finalidad podría tener el acceso la SBS, ellos no investigan, esos son datos personales que no pueden ser divulgados, es muy delicada.		
Asesor del Gabinete de Asesores de la Fiscalía de la Nación	Resulta relevante contar con un registro de denuncias por esta clase de delitos, pero que no esté bajo la tutela de la SBS y AFPs, sino, más bien, por la DIVINDAT.		
Resultado	Existe el registro de denuncias entre la PNP y las entidades financieras la cual se mantiene en confidencialidad.		

Fuente: Propia

TABLA 29:

Respuesta de los especialistas en relación a la pregunta 11 de la entrevista.

¿Considera usted necesaria la capacitación de jueces, fiscales y funcionarios del Poder Judicial y el Ministerio Público, así como de miembros de la DIVINDAT - PNP, sobre los alcances de la Ley N° 30096 - Ley de Delitos Informáticos, casuística, aplicación de la Ley, índice de denuncias y modus operandi en la comisión de los mismos?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Juez 1	Considero que este grupo de personas si tienen conocimiento de los alcances de la Ley, siendo en quienes deberían incidirse más, es en la población vulnerable, pues como repito esta modalidad se está volviendo común. Como experiencia personal, ene l mes de febrero 2022, revisé el APP del BCP y tenía consumos diarios de S/ 12, S/13, S/14, cuando hice mi reclamo me devolvieron los montos, porque obviamente no había autorizado dichas transacciones (Adjunto cartas). Por ello le indico, a los que realizan este tipo de delitos les resulta más fácil sustraer montos pequeños y a los Bancos les resulta más económico devolver montos pequeños que realizar medidas de seguridad, mientras el cliente es el más perjudicado porque tiene que bloquear la tarjeta e ir a renovarla, etc.	La abogada Ramos, el fiscal Vílchez y el coronel Huamán concuerdan en que debería capacitarse a los jueces y fiscales a fin de realizar una adecuada investigación, El coronel Huamán precisa que las que necesitan capacitación son las fiscalías penales.	En contraparte la magistrada Carrillo indica que se debe capacitar a la población usuaria.

Asistente de Sala	Sí, ya que, al utilizar la tecnología como medio para la comisión de este tipo de delitos, debe haber una capacitación por parte de los operarios de justicia, ya que, de esa manera, los delitos podrán ser investigados de la manera más adecuada y así no queden impunes.		
Coronel de la DIVINDAT	Si se considera necesario, para estar a la par y conversar del mismo tema, es bueno que los fiscales y jueces se capaciten, había cursos Online donde ha participado el Ministerio Público y Poder Judicial, de hace dos años de forma presencial, la idea es que se masifique o fomente más, tenemos una fiscalía de ciberdelincuencia que solamente abarca Lima Metropolitana, y también se tiene una Sala de Fiscalía Superior que se encuentra en Surco, quienes se encuentran aptas, las que necesitarían capacitarlas serían las fiscalías penales.		
Asesor del Gabinete de Asesores de la Fiscalía de la Nación	La capacitación académico-profesional resulta siempre relevante. Las capacitaciones deben estar orientadas a recepcionar información de experiencias en otros países donde el fenómeno criminal de la ciberdelincuencia ha sido tratado con anterioridad a nuestro caso (por ejemplo, España, Colombia, Argentina y Chile).		

Resultado	Colegimos que se necesita capacitar a los magistrados, a los fiscales e inclusiva a los usuarios, a fin de estar a la par y superior a la delincuencia cibernética.

Fuente: Propia

TABLA 30:

Respuesta de los especialistas en relación a la pregunta 12 de la entrevista.

¿Tiene usted alguna propuesta, comentario o solución alternativa que aportar al presente tema de investigación?			
Entrevistado	**Respuesta**	**Convergencia**	**Divergencia**
Juez 1	La Superintendencia de Banca y Seguros debe establecer un sistema de control auditor en los Bancos y entidades financieras a efectos de determinar qué medidas de seguridad están realizando, de lo contrario sancionar con el cierre definitivo.	Ninguna	Difieren en sus recomendaciones: la magistrada Carrillo aconseja que la SBS establezca un sistema de control auditor en las entidades financieras, la abogada Ramos sugiere que debe realizar una debida adecuación a la norma, y el coronel Huamán propone incentivar una cultura de ciberseguridad con la
Asistente de Sala	A modo de recomendación, creo que se debe diferenciar el fraude informático con la estafa tradicional, pues en muchos casos la administración de justicia ante el desconocimiento de las nuevas modalidades de fraude informático, las califica como delito de estafa y al final terminan siendo casos archivados.		
Coronel de la DIVINDAT	Como les dije el ser más indefenso del sistema informático es el ser humano, se debe crear una cultura de cibercriminalidad en la ciudadanía, los medios de prensa deben participar, los colegios enseñarles a los niños, la ciberseguridad, por ejemplo: que pasaría si encuentras un USB en la mesa, te aseguro que lo pones en tu		

	computadora, pero ahí te meten el virus.		participación de todos sectores, el Fiscal Vílchez señala que los mayores estriban de los vacíos del artículo 8°-
Asesor del Gabinete de Asesores de la Fiscalía de la Nación	Considero que, los mayores problemas en el tópico de la ciberdelincuencia estriban en los vacíos normativos que ostenta nuestra actual legislación (delito contra la propiedad intelectual mediante las TIC´s y el ciberterrorismo) y los temas procesales (agente encubierto cibernético y la prueba digital), donde debería concentrarse el debate y propuestas de aplicación.		
Resultado	Concluimos que las entidades financieras requieren mayor control, la norma un cambio y la promoción de la cultura de ciberseguridad, desde niños hasta adultos.		

Fuente: Propia

Análisis documental: Jurisprudencia.- En cuanto al análisis documental, el material es escaso en cuanto a los acuerdos plenarios, acuerdos plenarios extraordinarios ni plenos casatorios en materia penal referentes a los delitos informáticos de Fraude Informático, pues de la investigación hemos determinado que en los Juzgados Penales de Lima la gran mayoría de casos se encuentra en Etapa de Instrucción (con el Antiguo Código de Procedimientos Penales) o Etapa de Investigación Preparatoria (con el Nuevo Código Procesal Penal en adelante CPC) y la otra parte en Etapa de Juicio Oral (con el Antiguo CPC) o Etapa de Juzgamiento (con el Nuevo CPC), no obstante, los casos concluidos se encuentran o archivados, con sentencia en primera instancia o concluido por alguna medida alternativa de simplificación procesal, hecho que denota un gran vacío a nivel jurisprudencial más aún con la modificación de la norma mediante Ley N° 30171 emitido del año 2014, pues los órganos jurisdiccionales no encuentran una base sólida donde apoyar sus argumentos o una guía donde puedan orientar su fundamentación, aunado a ello, debe tenerse presente que de la totalidad de casos a nivel judicial un gran porcentaje no llega a una tutela efectiva de derechos, pues su bien jurídico vulnerado (patrimonio) no llega a devolverse a su esfera jurídica patrimonial. Por otro lado, en lo que, respecto al trabajo de investigación más relevante para la presente tesis, tenemos la investigación realizada por Utreras (2017) quien concluyó, en su memoria de prueba para optar el grado de licenciado en Ciencias Jurídicas y Sociales, que:

> El fraude informático está compuesto por los siguientes presupuestos típicos: manipulación informática (u otro artificio semejante); disposición patrimonial; y perjuicio. Los elementos engaño y disposición patrimonial tienen un parecido únicamente conceptual respecto a los de la estafa, pues la estructura de estos injustos reclama matices diferenciadores que impiden equipararlos en cuanto a presupuestos típicos. Es decir, la estafa y el fraude informático presentan una estructura similar, pero las peculiaridades de ambos injustos los apartan diametralmente (p. 62).

Por otro lado, en cuanto al delito de fraude informático regulado mediante la Ley N° 30096 en su tipo penal primigenio publicada el 23 de octubre del año 2013, se recabó como precedente judicial, la sentencia del proceso signado con el Expediente N° 09405-2014, visto por la señora Juez del Décimo Juzgado Penal de Lima Norte, quien con fecha 16 de junio del año 2017, dispuso condenar a MARCOS MORALES VARGAS como autor del Delito Informático de Fraude Informático y otros, en agravio de la Empresa Financiera "Caja Municipal de Ahorro y Crédito de Trujillo S.A." condenándolo a ocho años de pena privativa de libertad, misma que fue apelada en dicho extremo, y consecuentemente revocada en la pena de ocho años a seis años de pena privativa de libertad por la Primera Sala Penal de Reos en Cárcel de la Corte Superior de Justicia de Lima Norte, misma que se declaró consentida y ejecutoriada por el Juzgado Penal de primera instancia con fecha 23 de mayo del 2018.

Análisis de casos: Respecto al expediente citado en la presente tesis tenemos que, se demostró que el condenado en su condición de auxiliar de operaciones y controlador en la entidad financiera, realizó un uso indebido de sus facultades, pues mediante del uso de las tecnologías informáticas valiéndose de su propia condición de auxiliar utilizó las claves de usuarios que contaban con cuentas a plazo fijo en la entidad financiera agraviada, logrando así sustraer el monto ascendiente a S/. 194.834.69 Soles a favor del condenado, delito que logró ejecutar de manera continuada y aprovechándose de su cargo funcional, a través de certificados de retiro fraguados, lo que simultáneamente ejecutaba utilizando comandos y claves alteradas, de entre las víctimas usuario, una declaró que se le entregaba los Boucher correspondientes a los supuestos movimientos, y de la revisión de las videocámaras de seguridad se advirtió que el sentenciado revisaba las fichas RENIEC de los usuarios agraviados, y posteriormente firmaba una hoja, acreditándose la comisión del delito de fraude informático, pues las pruebas grafotécnica arrojaron que dichas firmas fueron falsificadas.

4.2. Discusión

En el presente acápite, se procederá a realizar la discusión de resultados obtenidos, para lo cual, en principio cabe aclarar qué entendemos por discusión de resultado dentro del marco de un trabajo de investigación, para ello, empleando las palabras de Aliaga et al. (2018), the word "discussion" comes from the latin "discutere" which means "dispel or resolve", within the research sector this involves examining a certain matter in a conscientious and concentrated manner, the result shows an argumentative nature that tries to persuade the reader about the veracity of the findings obtained, in short lines, infers that the result of the discussion is that place where most analyst readers go after reading the summary; however, it becomes the deepest and most complicated section to structure and write, since it tests the scientific rigor of an investigation.

Estando a lo antes expuesto, procederemos a desarrollar la discusión de los resultados obtenidos, en base a la utilización de instrumentos habilitados por el enfoque cualitativo, tales como la entrevista, la hermenéutica en base la información indexada recabada a nivel nacional e internacional desglosando las categorías y subcategorías respectivas. Aunado a ello, en el presente acápite discutiremos los resultados de campo recabados a través de las encuestas realizadas a un grupo de personas que promedian desde los 20 a 45 años de edad, en base a nuestros objetivos generales y específicos.

A continuación analizaremos los resultados obtenidos a partir de las guías de entrevistas realizadas a los nuestros participantes, los cuales fueron (1) El Juez Penal María del Rosario Carrillo Espichán; (2) miembro de la DIVINDAT, Abogado y Magíster en Derecho Penal el Coronel Luis Edgardo Huamán Santamaría y finalmente a la (3) Abogada y Asistente de Relatoría María Alejandra Ramos Ramos, (4) Asesor del Gabinete de Asesores de la Fiscalía de la Nación, Abogado por la UNMSM, Fiscal Roberto Carlos Vílchez Limay, en relación al objetivo general: Determinar las deficiencias legislativas en el tratamiento del artículo 8° de la Ley N° 30096, en Lima durante el periodo del 2019-2021, formulando las siguientes preguntas:

1. ¿Cómo define usted el concepto de Fraude Informático como institución jurídica, regulada por el Artículo 8° de la Ley Nº 30096?
2. De acuerdo a su experiencia, en términos porcentuales, ¿Cuál cree usted que es la incidencia de denuncias relacionadas al delito de Fraude Informático entre los Delitos Informáticos en Lima durante el periodo 2019 - 2021?
3. ¿Qué deficiencias legislativas puede advertir en el Artículo 8° (Fraude Informático) de la Ley N° 30096?
4. ¿Cuál cree usted que sea el principal motivo por el cual se archivan a nivel preliminar las investigaciones por fraude informático?

En ese sentido, los participantes Carrillo, Huamán, Vílchez y Ramos (2022), coinciden en relación a la primera interrogante, refiriendo que el delito de fraude informático es aquel ilícito penal destinado al diseño, introducción de datos y alteración, todo ello a fin de obtener un provecho patrimonial, a través de los medios informáticos como las TIC´s, en ese sentido el coronel Huamán (2022) sostiene que en el caso de las computadoras, estas pueden ser utilizadas como medio para la ejecución del delito, pero también como objeto del delito, a través de la inserción de virus como el “Ransomware” que secuestra los datos y encripta el disco duro convirtiéndose en un ataque directo al sistema informático. Por otro lado, la Juez Penal Carrillo (2022) ha indicado que durante la comisión de este delito se obtiene información personal de las víctimas a través de medios fraudulentos, tales como mensajes de texto, llamadas telefónicas, correos electrónicos generando confusión en los usuarios y con ello la pérdida de responsabilidad de estos (quienes delinquen), en este extremo hacemos hincapié, pues se desprende la imputación objetiva del agraviado, institución que también ha referido el Coronel Huamán (2022) como factor principal para el archivo de la investigación preparatoria a nivel fiscal.

En cuanto a la segunda interrogante, la Juez Penal Carrillo (2022) refiere que en el tiempo que lleva desempeñando el cargo de Juez Penal, esto es, de noviembre del 2021 a la fecha mayo del 2022 se han tramitado solo 3 expedientes, 2 de ellos

con terminación anticipada, por otro lado, Ramos (2022) señala que existe un alto índice de denuncias tomando en cuenta, que el uso de las tecnologías es un medio muy recurrido por las personas. El Fiscal Vílchez (2022) refiere que la incidencia de denuncias por fraude informático se ubica en el tercer escalafón después de los delitos contra la libertad e identidad sexual y de los delitos contra el patrimonio. El coronel Huamán (2022) señala que, si bien no cuenta con cifras de los años anteriores, en lo que va del año 2022 se han reportado, durante su gestión, más de 2,012 denuncias solo en Lima Metropolitana, no contando con data detallada de años anteriores. Respecto a este punto, hemos de precisar, que habiendo realizado la búsqueda de registros de denuncias efectuadas por delitos informáticos durante los años 2019-2021 en el portal web del Ministerio Público, esto es, el Observatorio de Criminalidad del Ministerio Público, este no detalla un reporte de denuncias por delitos informáticos, asimismo, el portal de transparencia persiste en su inaccesibilidad de datos por errores desconocidos (Anexo 13), lo cual evidencia una obstaculización en el acceso a la información, ya que siendo este un portal oficial de información de índice penal, se hace imprescindible su funcionamiento las veinticuatro horas del día y siete días a la semana, a mérito de incentivar un constante investigación en la materia a futuro y un acceso a información constante por el público en general. Por otro lado, se ha desarrollado la búsqueda boletines estadísticos de delitos informáticos, ubicando solamente la expedición del Boletín Estadístico del año 2019 (Anexo 4), siendo este un Informe Gubernamental, que detalla: "(...) the type of crime with the highest incidence occurs in computer crimes against property with 33.77%", con ello, hemos de precisar que pese a no contar con cifras oficiales del periodo de años 2019-2021, el coronel Huamán, quien desarrolla el ejercicio de funciones como Coronel en la DIVINDAT en lo que va del año 2022 (enero a mayo) refiere que se han reportado más de 2,012 denuncias solo en Lima Metropolitana, esto, obviando la cifra negra respecto a las denuncias no efectuadas, o las efectuadas a nivel nacional en las jurisdicciones policiales no especializadas.

Respecto a la tercera interrogante, la Juez Penal Carrillo (2022) examina la estructura de la norma, donde sugiere que no sólo se debe establecer multas a la

entidad financiera, en caso de que no remita información, sino que también en el hipotético caso de que los sentenciados sean trabajadores de las entidades financieras (pues a través de ellos tienen acceso a información privilegiada) deberán responder como terceros civilmente responsables. El Fiscal Vílchez (2022) refiere que, desde una perspectiva dogmática, el tipo penal prevé, de manera innecesaria, un elemento subjetivo de tendencia interna trascendente el cual consiste en “para obtener un provecho ilícito para sí o para otro”, siendo que, la lesión a la integridad y secreto del sistema informático se encuentra efectivo, indistintamente que pueda generar un beneficio económico o de otra índole en el sujeto activo. Por otro lado, la Abogada Ramos (2022) señala que se encuentran vacíos legales, ya que no regula todas las modalidades de delinquir a través de los medios informáticos, ya que hoy en día existen diversas formas de delinquir mediante la utilización de la tecnología. Finalmente, el Coronel Huamán (2022) refiere que los verbos rectores del tipo penal en cuestión, deben ser entendidos de forma copulativa, por ejemplo cuando la norma indica: “el que deliberada e ilegítimamente procura para sí u otro un provecho ilícito en perjuicio de un tercero, mediante el diseño”, sobre ello refiere que cuando se realiza un diseño fraudulento este por sí solo, no se configura como delito de fraude, ya que es necesaria la introducción de los datos personales del propio agraviado o sea este hackeado a través de las modalidades del tipo, refiere también que se disgrega de la norma que los verbos rectores se aplican de manera disyuntiva, debiendo aplicarse de forma copulativa, esto dado que, el delito de fraude informático no admite tentativas, debiendo realizarse el despojo patrimonial por ser un delito de resultado.

A partir a la cuarta interrogante, la participante Carrillo (2022) señala que el principal motivo por el cual se archivan a nivel preliminar es por desconocimiento y por la decisión de no invertir tiempo y dinero, refiere también que existen dos caminos si la entidad ha enviado la constancia de transacción o no, en este caso si no se envía la constancia de transacción se realiza un reclamo ante la entidad, quien resuelve rechazar la misma, indicando que es responsabilidad del cliente “la reserva” de la clave, sin embargo, también es obligación de esta remitir el

comprobante de la transacción, en caso no lo realice, se realiza la reclamación ante INDECOPI, ahora bien, si la entidad financiera ha remitido la constancia de transacción y no ha sido autorizada por el titular se procede con la denuncia respectiva. En ese sentido, el coronel Huamán (2022) ha referido que muchos fiscales adoptan la teoría funcionalista del Derecho Penal, pues apuntan a las ideas de Roxin sobre la imputación objetiva, en base a la teoría de riesgos, quien es aquel que crea un riesgo al poseer bienes de cuidado, pues colige que uno mismo crea el riesgo, aquel señala es el criterio de los fiscales, pues son partidarios de la víctima o dogmática, es decir, se le echa la culpa al usuario. En contraparte, el Fiscal Vílchez (2022) refiere que no necesariamente el archivo se realiza a nivel de diligencias preliminares, empero, se puede disponer el sobreseimiento de la causa o la dificultad probatoria para el Ministerio Público, en su estrategia acreditativa en el juicio oral. Finalmente, la Abogada Ramos (2022) precisa que la norma no se encuentra debidamente regulada, resultando en muchas ocasiones como atípicas las conductas ilícitas realizadas, en consecuencia, disponiendo su archivo, en otros casos, el mismo sistema de investigación resulta ineficiente no logrando dar con el responsable resultando su archivo por falta de individualización del presunto autor, siendo este un requisito para la formalización de la investigación preparatoria.

Ahora bien, los resultados obtenidos en la guía de entrevista en relación al primer objetivo específico de nuestro trabajo de investigación: Definir las razones por las que se debe mejorar o erradicar las deficiencias legislativas en el art. 8° de la Ley N° 30096, formulando las siguientes preguntas:

5. ¿Considera usted que mejorar la estructura normativa del delito de Fraude Informático estipulado en el Artículo 8° de la Ley N° 30096 – Ley de Delitos Informáticos, coadyuvará a la prevención del delito? (Fundamente su respuesta)
6. ¿Qué opinión merece el aumento progresivo en la comisión del delito de Fraude Informático y el uso de las tecnologías digitales para tal fin?

En ese sentido, en cuanto a la quinta interrogante, la participante Carrillo (2022) indica que más que mejorar la estructura del delito, son las entidades financieras las que deben mejorar sus medidas de seguridad en el acceso a la base de datos a su sistema, ya que se está tornando común, tanto que incluso lo hacen por montos mínimos a diarios y los clientes no se percatan de ello, pasando desapercibidas dichas acciones. Por otro lado, el coronel Huamán (2022) manifiesta que, en primer lugar, los verbos rectores deben darse de forma copulativa y no solamente excluyente, además el artículo 8° debe ser apoyado por el Protocolo de trabajo conjunto con el Ministerio Público, en cuanto a la pena se sugiere prisión preventiva no menos de un año para la cuenta receptora, en cuanto a la aplicación de una medida cautelar, esta debe darse a nivel administrativo o civil como una medida real. En oposición a lo esgrimido por los participantes Carrillo (2022) y Human (2022), el Fiscal Vílchez (2022) sostienen que el tópico de la prevención general o especial del delito no responden a las modificaciones dogmática en el tipo penal, sino, en la posibilidad de establecer una Política Criminal y Política Pública que enseñen el respeto a la integridad de los datos o sistemáticos informáticos ajenos para motivar una conducta socialmente adecuada. Finalmente, Ramos (2022) concluye que, con una mejor implementación en la estructura normativa del tipo, permitirá que estos delitos especiales sean sancionados de una manera más adecuada y hacer que los delincuentes sepan que este tipo de delitos no quedarán impunes.

Asimismo, respecto a la sexta interrogante, la participante Carrillo (2022) señala que el uso de esta modalidad de delinquir se está volviendo muy común, tal es así, que se torna inseguro el uso de tarjetas de crédito, en ese sentido, el coronel Huamán (2022) refiere que todo comenzó con la pandemia y el uso masivo del internet, además las compras por internet también se han masificado pues se volvieron tendencia, por ello, se utilizaron mucho más las TIC´s, a ello agrega que no se puede recomendar no usar los móviles, pero si se puede sugerir el control del rubro de las comunicaciones, la seguridad informática y la cultura de ciber, señala que un sistema informático está compuesto de tres elementos: hardware, Software y el Humanware (el hombre), siendo el más débil el Humanware, pues es

el responsable, por ejemplo: en el phishing, las personas saben que no debe hacer click en un link de dudosa procedencia, por eso cuando se advierte una página de dudosa procedencia se deben copiar el dominio (URL) y colocarlo en páginas amigables, como: whois.com, exsalion o thispersondoesnotexist.com por ejemplo: sale una publicación en Facebook que dice: “Vendo casa”, se debe copiar el URL colocar en la página amigable, ante ello sale un informe de cuándo fue creada, quién lo creó, el administrador (es), alertando que si está todo privado se debe sospechar que trata de una página creada para fines de estafa, aunado a ello, si ha sido creada recientemente puede ser una página creada de igual modo para estafar, señala que estas son páginas amigables de inteligencia artificial. En ese mismo sentido la abogada Ramos (2022) y el Fiscal Vílchez (2022) agrega que pese a que las TIC´s son utilizadas en consonancia con el desarrollo de la ciencia, no se puede limitar su uso porque iría en contra de la misma naturaleza del conocimiento humano, sin embargo, apuesta por una optimización en la tecnología para desarrollar nuevas técnicas especiales de investigación de lucha contra esta clase de criminalidad.

Por otro lado, los resultados obtenidos en la guía de entrevista en relación al segundo objetivo específico de nuestro trabajo de investigación: Analizar las propuestas de mejorar o erradicar las deficiencias legislativas en el art. 8° de la Ley N° 30096, formulando las siguientes preguntas:

7. ¿Qué opinión merece el planteamiento del incremento presupuestal de las siguientes instituciones públicas: DIVINDAT, Fiscalía de Ciberdelincuencia y Juzgados Penales, con la finalidad de reducir y/o erradicar la comisión del delito de Fraude Informático?
8. ¿Considera pertinente la aplicación de normas análogas del Derecho Penal, peruano o internacional, ante las deficiencias legislativas del delito de Fraude Informático?, Explique.
9. De acuerdo a su experiencia ¿Qué medida o medidas complementarias a la interposición de la denuncia del agraviado por el delito de Fraude Informático, se podrían implementar legislativamente con el objetivo de

retrotraer el daño causado al estado anterior de la comisión del delito (Recuperación inmediata del patrimonio sustraído)?

En cuanto a la séptima interrogante la Juez Carrillo (2022) ha manifestado que la forma de prevenir esta clase de delitos es que las entidades financieras adopten medidas de seguridad al respecto. En ese sentido Huamán (2022), Vílchez (2022) y Ramos (2022) coinciden en que efectivamente se necesitan más herramientas, dado que el derecho evoluciona, y quienes delinquen utilizan herramientas tecnológicas, además refieren que se necesitan renovar los equipos, pues se necesitan herramientas de última generación, por ejemplo: Inteligencia Artificial (IA) de Oracle Cloud Infrastructure (OCI), inteligencia de fuente abierta, todo ello a fin de utilizar mayores implementos tecnológicos que permitan realizar una mejor y adecuada investigación que permita la identificación de los ciberdelincuentes. Agrega Vílchez (2022) que actualmente, no existen juzgados penales especializados en la materia.

Por otro lado, en cuanto a la octava interrogante la participante Carrillo (2022) precisa que, dado que las entidades financieras son en su mayoría internacionales, deben implementarse sanciones pecuniarias y administrativas a nivel internacional tanto a las entidades financieras como a sus representantes legales. En esa línea de ideas Huamán (2022), Vílchez (2022) y Ramos (2022) coinciden en que el Perú también es parte de convenios sobre la ciberdelincuencia con una serie de tratados europeos a las cuales hay que acudir siempre que se encuentre vacíos o deficiencias en la Ley, agrega Huamán (2022) que siempre se debe tomarse en cuenta el principio de legalidad.

En relación a la novena interrogante, la participante Carrillo (2022) señala que una de las medidas complementarias a la interposición de la denuncia del agraviado debe ser la simplificación en el trámite. Aunado a ello, el Coronel Huamán (2022) manifiesta que se debe resarcir el daño, mediante la aplicación de medidas reales, incautación de medios comisivos, extinción de dominio, sostienen que algunas veces no se realiza extinción de dominio, haciendo un mea culpa su institución, sostiene que deberían informar. Por otro lado, Ramos (2022) se sincera

manifestando que en la realidad problemática es complicado hablar de una recuperación inmediata del patrimonio sustraído, indicando que lo más efectivo sería la prevención del propio usuario en el uso desmesurado de las tecnologías y protección de uso de datos, agrega un punto álgido, en cuanto a la responsabilidad de las víctimas hurtos o robos de pertenencias como DNI, las cuales no suele ser denunciada, permitiendo así que muchos inescrupulosos, hagan uso de dicha data realizando suplantaciones de identidad o fraudes informáticos. En ese mismo sentido, Vílchez (2022) señala que la recuperación inmediata de información o patrimonio, sobre la base del fraude informático, resulta difícilmente obtenible, indistintamente de ello, se tiene que el delito ya está consumado, y que la recuperación del patrimonio estaría más orientado al momento de la reparación civil.

Finalmente, los resultados obtenidos en la guía de entrevista en relación al tercer objetivo específico de nuestro trabajo de tesis: Establecer propuestas que coadyuven a mejorar o erradicar las deficiencias legislativas en el artículo 8° de la Ley N° 30096, formulando las siguientes preguntas:

10. ¿Qué opina usted de la implementación de un registro de denuncias de delitos de Fraude Informático, bajo el control de la Superintendencia de Banca, Seguros y AFP?
11. ¿Considera usted necesaria la capacitación de jueces, fiscales y funcionarios del Poder Judicial y el Ministerio Público, así como de miembros de la DIVINDAT - PNP, sobre los alcances de la Ley N° 30096, casuística, aplicación de la Ley, índice de denuncias y modus operandi en la comisión de los mismos? Explique.
12. Finalmente ¿Tiene usted alguna propuesta, comentario o solución alternativa que aportar al presente tema de investigación?

Respecto a la décima interrogante, Carrillo (2022) ha manifestado que en efecto, sería conveniente implementar un registro de denuncias bajo el control de la SBS, la abogada Ramos (2022) coincide, ya que la SBS tiene como fin propiciar una mayor confianza y protección de los intereses del público usuario, ejerciendo un

control y supervisión de las entidades bancarias, ya que son estas últimas donde más se cometen los fraudes informáticos y en los que los usuarios en muchos casos son los más perjudicados. En contraparte el coronel Huamán (2022) y Vílchez (2022) coinciden que debe existir un registro de denuncias de delitos de fraude informático, sin embargo, precisa Huamán (2022) que este existe y es confidencial, indicando que no sería pertinente ya que son ellos (DIVINDAT) quienes investigan, y no la SBS, no pudiendo ser divulgados, criterio concordante entre estos dos participantes.

En relación a la décimo primer interrogante, Ramos (2022), Vílchez (2022) y Huamán (2022) condicen de que efectivamente es necesaria, la capacitación a jueces y fiscales a fin de realizar una adecuada investigación, agrega Huamán (2022) que se han realizado cursos online donde han participado tanto el Ministerio Público como el Poder Judicial, sin embargo, ello fue hace dos años de forma presencial, la idea es que se masifique o fomente más y constantes capacitaciones, ya que aunado a ello solo se cuenta con una sola fiscalía de ciberdelincuencia que abarca solo Lima Metropolitana, y también se tiene una Sala de Fiscalía Superior que se encuentra en Surco, quienes se encuentran aptas, por otro lado, las que necesitan capacitar son las fiscalías penales. En contraparte sostiene Carrillo (2022) que los justiciables tienen conocimientos de los alcances de la Ley, por el contrario, a quien debe capacitarse es a la población vulnerable ya que estas modalidades se están volviendo comunes.

Finalmente, en cuanto a la décimo segunda interrogante, los entrevistados difieren en sus recomendaciones, donde Carrillo (2022) ha recomendado que la SBS establezca un sistema de control auditor en las entidades financieras a efectos de determinar qué medidas de seguridad están realizando, de lo contrario aconseja imponer una sanción más drástica que disponga de cierre definitivo. Asimismo, Ramos (2022) recomienda que se debe realizar una debida adecuación de la norma a fin de evitar la disposición de archivos de las investigaciones preparatorias, donde se suele confundir el tipo penal de estafa tradicional con la del fraude informático, tipos penales totalmente diferentes. El Fiscal Vílchez (2022)

considera que, los mayores problemas en el tópico de la ciberdelincuencia estriban en los vacíos normativos que ostenta nuestra actual legislación (delito contra la propiedad intelectual mediante las TIC´s y el ciberterrorismo) y los temas procesales (agente encubierto cibernético y la prueba digital), donde debería concentrarse el debate y propuestas de aplicación. Por último, el coronel Huamán, quien ampliamente ha aportado al presente a la presente investigación, ha incidido en promover una cultura de ciberseguridad, para lo cual deben participar desde los medios de prensa hasta los colegios.

Ahora bien, habiendo desglosado los aportes de nuestras entrevistados, acerca de la estructura normativa del artículo N° 08 de la Ley N° 30096, en el presente acápitedesarrollaremos la discusión en base a la efectividad de la aplicación de la norma, acto seguido desarrollaremos un análisis en cuanto al material documental, encuestas y entrevistas realizadas.

Si bien se advierte que la norma materia de discusión delimita la conducta del sujeto activo como aquel que “deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero” realiza la conducta ilícita, es decir, establece el dolo premeditado en el accionar ilícito, lo cual se condice con lo manifestado por Acosta et al. (2020) quien sostiene que los delitos informáticos se ejecutan a través de la extracción de información personal del usuario víctima, efectuándose dolosamente el delito, por medio de la filtración de datos, sin embargo, hay que delimitar también, que por otro lado, el delito de fraude informático prevé entre sus verbos rectores, de manera disyuntiva, los siguientes supuestos, el que “mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático”, entendiendo que para la comisión del delito se configure con la ejecución de uno o más de los verbos rectores detallados dependiendo de la modalidad empleada para la comisión del delito de fraude informático, mediante las diversas modalidades del mismo, cabe señalar, que estas modalidades mantendrán una evolución constante a la par del uso de las tecnologías.

Ahora bien, seguramente se plantearán la siguiente interrogante ¿Dónde comienza el problema?, para ello, en primer lugar, abordemos las estadísticas, y en ese sentido hablemos de las cifras oficiales, las cuales hablan por sí mismas. Para el presente trabajo de investigación, se recabó la data consignada en el Boletín Estadístico del Ministerio Público (MP, 2019) un trabajo bastante importante, el cual se venía realizando de manera anual con cifras a nivel nacional, arrojando (Anexo 4) para el mes de enero del año 2019, 208 casos de delitos informáticos contra el patrimonio, para el mes de febrero del año 2019 arroja 353 casos de delitos informáticos contra el patrimonio, y para el mes de marzo del año 2019 señala 554 casos de delitos informáticos contra el patrimonio, esto es, en cuanto a la información pública recabada del propio portal web del Ministerio Público, es en ese sentido, que nos cuestionamos cuáles podrían ser las razones para la disposición de archivo a nivel fiscal respecto de los delitos informáticos, a fin de entender las cifras reportadas (tomando en cuenta que estas se realizan sobre la base de más de 32 millones de peruanos, que residen actualmente en el Perú en base a las estadísticas recabadas del INEI - 2020), empero, dicho informe no detalla la cantidad de disposiciones de archivo preliminar, tampoco cuáles son las regiones más afectadas a nivel nacional por los delitos informáticos, ni los tipos penales de la Ley N° 30096 que más se comentan en agravio de los peruanos, lo que sí tiene a bien, precisar una cifra genérica de delitos informáticos los cuales, como es de verse mantienen un aumento constante en el tiempo siendo el de mayor comisión los delitos informáticos de índole patrimonial. Por otro lado, dicho informe coteja y hace una comparativa entre el índice delincuencial del año 2019 y el año 2018, reflejando su incremento, por ello es de la opinión de las investigadoras, que mantener una actualización constante y detallada de dicha información, fomenta al conocimiento de una cifra real para los interesados en el tema, no solo para efectos de conocimiento, sino también de investigación, la transparencia en el detalle de los delitos que contienen modalidades nuevas para las personas, y que utilizan herramientas diariamente a través de las cuales se exponen, ya que todos contamos con algún aparato digital hoy en día, y estadísticamente hablamos de cifras muy por debajo

de lo real que se estarían denunciando, y es menester descubrir el porqué de dicha situación. En ese contexto, lamentamos advertir que dicho -importantísimo- boletín informativo se ha estancado en la data obtenida en el año 2019, el cual además, cabe recordar, se realizó antes del inicio de la pandemia del Sars Covid-19, y en base a lo señalado por nuestros entrevistados Ramos (2022) y Huamán (2022) este se habría agudizado de manera dramática a la fecha, recordemos, que nuestro participante Huamán (2022) es Coronel de la DIVINDAT, quien nos ha referido haber recibido 2,012 denuncias por delito de fraude informático en lo que va del año 2022 (primer trimestre del 2022).

En segundo lugar, a fin de examinar la problemática desde la posición de un ciudadano promedio -y así cotejar, de cierta manera, qué tan ciertas son nuestras dudas- realizamos una encuesta dirigida a personas que oscilan entre los 20 a 45 años de edad, en un universo de 46 personas, con la finalidad de obtener información sobre el uso de las herramientas digitales, la forma, frecuencia de usos de medios digitales, así como la confiabilidad en nuestras instituciones públicas y entidades financieras, entre otras cuestiones de carácter general, obtuvimos algunos resultados muy importantes, por ejemplo, 28 de ellas manifestaron utilizar activamente billeteras digitales tales como Plin, Yape y medios análogos para las transferencias digitales de los cuales 30 de ellas las utilizan de 1 hasta 5 veces por semana, asimismo, 21 de los encuestados conoce o ha sido víctima de los delitos de fraude informático, 36 de ellas refirieron haber recibido mensajes o llamadas donde les ofrecen regalos o premios de sorteos que nunca participaron donde se consignan enlaces que deben seleccionar a fin de recabar el premio. Por su parte, lo que sabemos de estos ejemplos prácticos planteados, son modalidades de intento de fraude informáticos, todo ello con la finalidad de realizar un timo virtual, que necesariamente en su gran mayoría de casos, termina siendo de carácter patrimonial, ahora bien, lo que se ha verificado es que este tipo penal de incidencia digital se realiza sobre una población activa en la utilización de las TIC's, las herramientas y medios tecnológicos, tales como celulares, computadoras, tablets y análogos, sin embargo, en muchas ocasiones dicho descuido es trasladado a la víctima, y a nuestros leyentes cabe realizarles la

siguiente pregunta cerrada ¿Resulta justo trasladar la responsabilidad a la víctima en base a que este ingresó a un enlace digital fraudulento, o contestar una llamada telefónica fraudulenta, sin la intención ni conocimiento de estar siendo víctima del delito de fraude informático? ¿Hasta qué grado la responsabilidad se traslada al agraviado que recibe una llamada telefónica de una supuesta empresa telefónica quien mediante dicha llamada intercepta datos personales de la víctima para hurtar su dinero? Hoy en día, las personas realizamos llamadas, enviamos mensajes de texto, realizamos transacciones mediante la utilización de nuestros smartphones, ello no puede de ninguna manera ser catalogado como una exposición voluntaria al riesgo de ser víctimas de un delito informático contra el patrimonio, es así, que necesitamos ver las reales estadísticas y detectar el problema sin vendas sobre los ojos; no olvidemos que el Derecho es una ciencia social, y desarrollamos nuestras investigaciones y estudios con la finalidad de aportar a la sociedad, para una mejor calidad de vida, en seguridad y armonía con nuestra tecnología que tantos beneficios nos provee.

Finalmente, cuando hablamos de la naturaleza del delito de fraude informático per se, el tipo penal está referido al perjuicio económico, en su propia estructura lo detalla; “el que (...) procura para sí o para otro un provecho ilícito (...) mediante el diseño, (...) de datos informáticos”, en ese sentido, pongamos un ejemplo práctico; si una persona con conocimiento en informática, realiza una interfaz fraudulenta de una entidad financiera en la web, la cual evidentemente se encuentra a la espera de una futura víctima, ergo, cuando una -desafortunada- persona ingrese al referido link y consigne sus datos personales (claves, password) y es hurtado automáticamente de sus fondos monetarios, se habrá ejecutado el delito de fraude informático, en este caso, se entiende que quien ingresa lo hace de manera involuntaria, ya que preguntamos a nuestros lectores si existiría alguna persona que, a sabiendas que ha ingresado a una página web falsa ¿Consignaría sus datos personales a fin de realizar una transacción financiera y ser defraudado con sus fondos? Eventualmente, presumimos que la respuesta se basará en la protección de la propiedad (el patrimonio) establecida en el artículo 2° numeral de 16 de la Carta Magna, pero ¿Cuál es el motivo por el

que nos realizamos dicha cuestión? -que a muchos puede parecer irrelevante u obvia-, sin embargo, en el Derecho Penal, no existe lo irrelevante u obvio, y nos llama la atención una famosa figura que, en ciertas situaciones, traslada la responsabilidad a la víctima, nos referimos a la Teoría de la Imputación Objetiva, dicha figura, ampliamente explicada por Claus Roxin, así como por Rojas y Mojica (2014) quienes concluyen que la imputación objetiva tiene como finalidad "establecer si determinados hechos deben ser considerados relevantes, (...) para formular la imputación de sus consecuencias a una determinada persona. La teoría de la causalidad adecuada es, en esencia, una teoría de la imputación objetiva, que permite (...) que un resultado pueda ser atribuido a un comportamiento" (pág. 27), en ese sentido desde el propio riesgo asumido por una persona, la fiscalía puede disponer el archivo preliminar en base a la imputación objetiva de la víctima, pues, realiza una pregunta inicial ¿Quién fue el responsable de digitar sus propios datos en una página web fraudulenta? o ¿Quién fue el responsable de brindar datos personales a una operadora, de una supuesta entidad telefónica, que en realidad era un estafador que buscaba defraudar patrimonialmente a su víctima?, y este criterio se comparte con las entidades financieras, quienes trasladan la absoluta responsabilidad de cautelar por el cuidado de sus datos, código de usuario, números de cuenta, contraseñas de sus tarjetas de crédito a sus clientes -y nosotros sus clientes- a sufrir las negativas a querer investigar ¿A qué destinatarios se dirigieron nuestros fondos -que reclamamos a gritos- no haber autorizado? recibiendo un rotundo no, por parte de las entidades financieras. El coronel de la DIVINDAT Huamán (2022), refiere en ese sentido, que el gran dilema de los archivos por delitos informáticos, como el fraude informático, se realiza en base al criterio adoptado, en su mayoría, por el Ministerio Público, quienes al advertir que el propio agraviado es quien consigna sus datos, se expone al riesgo y al fraude, mismo criterio que comparten, como ya hemos mencionado, las entidades financieras al realizar denuncias de sus usuarios de haber sufrido un asalto cibernético al haber clickeado o consignado sus datos personales en páginas web fraudulentas, en esa línea de ideas, nos preguntamos cuáles son las razones para la disposición de archivo a nivel

preliminar, considerando las posibilidades a nivel policial y fiscal, los cuales constituyen el primer filtro del incremento delincuencial en materia penal, y en ese aspecto, cabe recalcar que las disposiciones de archivo a nivel fiscal se realizan al no poder cumplir con los requisitos establecidos en el artículo 336° del CPC, del cual queremos recalcar “la individualización del presunto autor del hecho delictivo”, como primera barrera procesal en los estos delitos especiales, más aún en estos tipos digitales, donde el agente se oculta cómodamente tras una pantalla de celular o computadora.

Por otro lado, en cuanto al delito de fraude informático, sostiene el Coronel Huamán (2022) ser un delito de resultado, el cual no admite la tentativa, esto se traduce en que ante la posibilidad de que el agente diseñe una página web fraudulenta no sea pasible de sanción, sino que del propio perjuicio patrimonial se realice la finalidad del tipo, asimismo el Coronel de la DIVINDAT, agrega a lo expuesto que para la comisión de delitos de fraude informático debe existir un perjuicio patrimonial, tal como lo precisa la norma, sin embargo, consideramos que la sola puesta en peligro del bien jurídico patrimonial en base a una potencial página web fraudulenta, a la espera de su potencial víctima deberá investigarse y sancionarse, pues ya se expuso a la sociedad en general a una afectación patrimonial, aunado a ello se realizó la afectación pluriofensiva de derechos, que si bien Díaz (2019) en su interesantísimo trabajo sobre la globalización de los delitos informáticos y cooperación internacional, sostuvo que no solo se afecta el derecho patrimonial, sino que también, se presta de cepo para la adquisición ilegal de datos personales y destrucción o alteración del software de la víctima, permitiendo que del error de la víctima, sirva de pretexto para que el encargado de realizar las investigaciones preliminares (e incluso la propia entidad financiera) disponga su archivo en base a la imputación objetiva, concordante a la aportaciones realizadas por los conocedores en la materia tales como la Juez Penal Carrillo (2022) quien traslada el deber de las entidades financieras a comunicar sobre las transferencias y/o retiros económicos al correo, SMS del titular y el Coronel de la DIVINDAT Huamán (2022), quien refiere que so pretexto de muchos fiscales para la disposición de archivo, es la imputación objetiva realizada sobre la propia víctima,

lo cual se traduce en la responsabilidad del usuario de tener mayor rigurosidad en brindar o hacer click en datos o links sospechosos.

Finalmente, la obtención de los datos personales recabados (número de DNI, datos de la ficha RENIEC, número de las tarjetas de crédito, nombres y apellidos, contraseñas, correos electrónicos de la potencial víctima) se traducen en una vulneración múltiple, que se condice con lo abordado por los autores Mayer (2018) y Díaz (2019), en ese sentido queda establecido la calidad de pluriofensivo del delito de fraude informático. En esa línea de ideas, si bien el artículo 46 numeral 2), literal h) e i) del Código Penal ha establecido circunstancias agravantes y el artículo 46-A - circunstancias agravantes por condición del agente activo -, estas no realizan una diferenciación ante la gravedad del ocultamiento de la afectación patrimonial del sujeto pasivo de la acción por parte del representante legal de la entidad bancaria, verbigracia, en los casos que las propias víctimas realizan la denuncia ante el operario de la entidad bancaria, a gritos silencios, toda vez que el usuario ya se habría visto despojado de su dinero, hacia un destinatario desconocido, y que el referido operario de la entidad bancaria, se niegue en brindar mayores detalles del trayecto final del mismo, sólo conlleva a la resignada interposición de una denuncia o queja que, valgan verdades, más allá de las investigaciones que se puedan efectuar, resulta siendo materialmente imposible recuperar el patrimonio ilícitamente sustraído, más aún, que en los casos de delitos informáticos, que consisten en la comisión de delitos especiales por su condición de ocultamiento del sujeto activo tras aquella pantalla digital protectora, concluye en un par de meses de investigación -como se ha detallado- en un archivo posiblemente, por falta de individualización del sujeto activo (artículo 336° del NCPP) o falta de medios probatorios que ofrecer en juicio oral, todo ello suma al aumento de la peligrosa cifra negra o real de casos denunciados o fraudes realizados, toda vez que, si bien las personas ajenas al derecho no conocen el proceso penal per se por el cual acaecen las denuncias que efectúan, sí existe una poca fiabilidad en cuanto a los resultados de las mismas, lo que se colige con nuestra encuesta efectuada en la cual un 50.0% (23) de los encuestados respondieron considerar que los delitos de fraude informático quedarán impunes,

lo que permite inferir, que existe poca fiabilidad en la aplicación de una efectiva Justicia penal.

V. Conclusiones

i. El fraude informático es aquella conducta típica y antijurídica ejercida por un agente con conocimientos en informática y/o utilización de las TIC, valiéndose de instrumentos informáticos mediante el uso del internet como medio de ejecución, así como por medio de la obtención de datos personales, a fin de fracturar el derecho a la intimidad y privacidad, a través de la obtención de los datos personales mediante las diferentes modalidades de fraude informático, con la finalidad de causar un perjuicio patrimonial a una persona natural o jurídica a través de la trasgresión de cuentas bancarias, billeteras digitales o análogos.

ii. Se ha determinado deficiencias legislativas en la Ley Nº 30096 respecto al delito de Fraude Informático, el cual si bien ha delimitado la tipicidad y antijuridicidad del mismo, existe una desprotección en cuanto a las víctimas del delito de fraude informático en el citado artículo, toda vez que no establece medidas preventivas o protectoras que puede realizar el agraviado una vez detectado el ataque, así como barreras burocracias en el trámite de identificación del destinatario a quien se realiza las transferencias bancarias no autorizadas por el titular de la cuenta bancaria, todo ello con la finalidad de establecer una denuncia formal contra un presunto autor del delito, evitando así la disposición de archivo de la investigación preparatoria por la falta de individualización del presunto autor, lo cual deviene en una de las causales de archivo, quedando impunes en su investigación.

iii. A fin de hacer frente a las cifras negras, e imputación objetiva como disposición de archivo en agravio del afectado, se propone la siguiente modificación al artículo 8° de la Ley N° 30096, a fin de establecer sanción penal al grado de tentativa en los delitos de fraude informático, debiendo incorporarse el siguiente párrafo, quedando de la siguiente manera:

(...)

La pena será privativa de libertad no menor de uno ni mayor de tres años y de ochenta a ciento cuarenta días-multa, al agente que efectúe cualquiera de los supuestos antes desglosados, por intermedio de un sistema informático, sin que exista un perjuicio patrimonial resultante, pero que su finalidad está dirigida al mismo.

iv. Respecto al análisis del Informe Gubernamental elaborado por el MINJUSDH (2020), data recabada por la DIVINDAT se evidencia un alarmante aumento de casos por delitos informáticos en los últimos años, que afectan al patrimonio de las personas y a sus estilos de vida, por cuanto, esta afectación se ve reflejada en el uso de aplicativos móviles, lo cual condice con el análisis del Informe Gubernamental elaborado por el MINJUSDH (2020) data recabada por la DIVINDAT que pone en evidencia la cantidad de denuncias efectuadas por delitos informáticos, se subraya que durante el periodo de años 2015 al 2019, la cantidad de denuncias efectuadas ha sido 1,007 y 3,012 denuncias, respectivamente, advirtiéndose que el número de denuncias se ha triplicado en tan solo 4 años, lo que genera preocupación e inseguridad en los usuarios, y en esa línea de ideas, encontramos al Boletín Informativo del Portal Web del Ministerio Público del año 2019, perteneciente a los meses de: enero, febrero y marzo, donde también se evidenció este aumento progresivo en los delitos informáticos de índole patrimonial, enfatizando que dichas estadísticas no son actualizadas hasta la fecha (2022), por lo que resulta imprescindible, actualizar las estadísticas, especificar y difundir las modalidades que se vienen cometiendo a fin de tener un mejor conocimiento de las cifras reales.

VI. Recomendaciones

i. Se recomienda la modificación del artículo 8° de la Ley N° 30096, debiendo incorporarse el siguiente párrafo, quedando de la siguiente manera: *(...) La pena será privativa de libertad no menor de uno ni mayor de tres años y de ochenta a ciento cuarenta días-multa, al agente que efectúe cualquiera de los supuestos antes desglosados, por intermedio de un sistema informático, sin que exista un perjuicio patrimonial resultante, pero que su finalidad está dirigida al mismo.* Dicha modificación se establece como mecanismo de prevención, a fin de hacer frente la cifra negra del tipo penal cuestionado, pues al ser este un tipo penal especial necesita una regulación especial, ergo, se ha determinado del presente trabajo de investigación que los *modus operandi* del delito de fraude informático seguirá aumentando y se ejecutará en sus diversas modalidades, de manera progresiva, como hasta la fecha (2019) ha acontecido, haciéndose urgente establecer una sanción punitiva al agente que elabore, diseñe, altere o suprima datos informáticos a fin de defraudar a una potencial víctima, sin que ello signifique un perjuicio patrimonial que finalmente no podrá ser resarcido, por las dificultades en la investigación en la instancia pertinente, lo cual se busca prevenir, para dicho fin deberá capacitarse a la Policía Nacional del Perú a nivel nacional.

ii. Se recomienda la descentralización de la DIVINDAT, cuya facultad es la de realizar el patrullaje cibernético en nuestro país cuyas investigaciones preliminares arrojen indicios de la participación de una organización criminal en la comisión del delito de fraude informático, para ello se recomienda realizar un incremento presupuestal a dicho órgano adscrito especializado en la PNP, a fin de ampliar la adquisición de computadoras, softwares de última generación y mayor cantidad de personal en el área, dado que a la fecha se cuenta con 120 personas laborando en dicha División, la misma que abarca a nivel nacional, de este modo buscando equiparar las desventajas en la investigación de los delitos informáticos, cuya noticia criminal es analizada por dicho órgano, pues todas las denuncias de Lima Metropolitana respecto a las TIC llegan a su departamento incrementando la carga

procesal en dicha unidad, para tal fin, se recomienda realizar capacitaciones especializadas a los miembros de la PNP en las diversas jurisdicciones a nivel nacional, a fin de realizar un efectivo y constante ciber patrullaje.

iii. Finalmente, se recomienda fomentar una cultura de ciberseguridad, promover capacitaciones sobre el uso de las TIC´s, definición, casos prácticos, conceptos, tipología y modalidades del delito de fraude informático, dirigidas al público en general, escuelas, universidades y miembros de instituciones públicas y privadas, con la finalidad de detectar el manejo, uso y defensa de datos personales, además de la importancia de tener un mayor cuidado al momento de brindar y publicar datos personales mediante el uso de las TIC´s, en esa línea de ideas, difundir la instalación de aplicativos móviles de plataformas como *TrueCaller* cuya finalidad es detectar llamadas de remitentes desconocidos, que hayan sido denunciados como “SPAM” evitando ser víctimas de algún tipo de ilícito penal de carácter informático, especialmente aquellas que conlleven a un perjuicio patrimonial, esto es, delito de fraude informático, el cual se ejecuta a través de alguna de sus modalidades de estafa comunes tales como el *phishing, pharming,* cartas o llamadas nigerianas, etc., desarrolladas en el presente trabajo de investigación, paralelamente a ello fomentar la utilización de aplicaciones amigables cuyo propósito es descubrir la procedencia lícita de las páginas web tales como www.whois.com o www.thispersondoesntexist.com.

Referencias

Acosta, M., Benavides, M., & Garcia, N. (2020). Computer crimes: Organizational impunity and its complexity in the business world. Venezuelan Management Magazine, 25(89), pp. 351-368. https://doi.org/10.37960/revista.v25i89.31534

Acosta, I., Acurero, M., & Peréz, M. (2020). Categories of analysis on sustainability a theoretical and contextualized proposal for the business sector. CUC economics. 41(2), p. 115-136. https://doi.org/10.17981/econcuc.41.2.2020.Org.7

Ardilla, J., Salcedo, E., Pedraza, C., & Saavedra, M. (2021). Review on ethical hacking and its relationship with artificial intelligence. Magazine - CHALLENGE. Volume 8. No. 1. pp. 11 - 21. https://doi.org/10.23850/reto.v8i1.3064

Aliaga, A., Castro, Y., & Mattos, M. (2018). Considerations in scientific writing: discussion, conclusions and references. Sanmarquina dentistry. 21(4). pp. 330–335. https://doi.org/10.15381/os.v21i4.15562

Belen, M. (2021) Computer crimes in the Argentine Penal Code. CHILEAN JOURNAL OF LAW AND SCIENCE 11(2). P.P. 122-144. POLITICS. https://doi.org/10.7770/rchdcp-V11N2-art2289

Public Ministry [MPDN]. (2019) Statistical Bulletin of the Public Ministry - Bulletin No. 1. https://www.mpfn.gob.pe/Docs/0/files/boletin_estadistico_enero_2019.pdf

Carhuancho, B. y Núñez, F. (2020). Ciberdelincuencia en tiempo de Covid-19: ¿La vulneración a derechos constitucionales?. *Lumen - Revista de la Facultad de Derecho - Unifé.* Volumen 16. Nº 1. pp 93-100. https://doi.org/10.33539/lumen.2020.v16n1.2287

Castañeda, M. (2022). The scientificity of quantitative, qualitative and emerging methodologies. Digital Journal of Research in University Teaching, 16(1), e1555. https://doi.org/10.19083/ridu.2022.1555

Concepción, D., González, E, García, R., y Miño, J. (2019). Metodología de la investigación: Origen y construcción de una tesis doctoral. *Revista Científica de la UCSA*, *6* (1), 76-87. https://dx.doi.org/10.18004/ucsa/2409-8752/2019.006(01)076-087

Crespo, L. (2020). La acción nuclear del delito informático en la Novísima Reforma Parcial del Código Integral Penal. *Revista Internacional Tecnológica - Educativa docentes 2.0.* Volumen 9 Nº 1. pp. 17 - 27. https://doi.org/10.37843/rted.v9i1.8

Cruz, M., Pozo, M., Aushay, H. y Arias, A. (2019). Las Tecnologías de la Información y de la Comunicación (TIC) como forma investigativa interdisciplinaria con un enfoque intercultural para el proceso de formación estudiantil. *Revista e-Ciencias de la Informació*n, 9 (1). [ensayo 3] https://doi.org/10.15517/eci.v1i1.33052

Díaz, A., (2019). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. *Revista Electrónica del Departamento de Derecho - Universidad de la Rioja.* Núm. 8, págs. 169-203. https://doi.org/10.18172/redur.4071

Díaz, J., Fernández, M. y Sánchez, M. (2021). Técnicas e instrumentos de recolección de información: análisis y procesamiento realizado por el investigador cualitativo. *Revista Científica UISRAEL*. 8(1). pp. 107–121. https://doi.org/10.35290/rcui.v8n1.2021.400

Encalada, V., Ruiz, S. Encarnación, O. (2020). Billetera electrónica móvil: una alternativa de pago del sistema financiero ecuatoriano. *Revista de*

Contabilidad y Negocios. (15) 30, pp. 24-42 https://doi.org/10.18800/contabilidad.202002.002

Escamilla, A., Márquez, H., Miranda, G., Villasís, M. y Zurita, J. (2018). El protocolo de investigación VII. Validez y confiabilidad de las mediciones. *Revista alergia México*. 65(4). pp. 414-421. https://doi.org/10.29262/ram.v65i4.560

Espinoza M. (2018). El derecho penal informático humano como cautela frente al poder punitivo en la sociedad de control. *Revista de Derecho.* Volumen 3(2), pp. 233 - 245. https://doi.org/10.47712/rd.2018.v3i2.26

Fusco, L. (2020). Los delitos informáticos en el Código Penal Italiano. *Derecho global. Estudios sobre derecho y justicia*, *5* (14), 127-149. https://doi.org/10.32870/dgedj.v5i14.250

Gairín, J., y Mercader, C. (2017). Usos y abusos de las TIC en los adolescentes. *Revista de Investigación Educativa*, *36* (1), pp. 125–140. https://doi.org/10.6018/rie.36.1.284001

García, J., y Sánchez, P. (2020). Diseño teórico de la investigación: instrucciones metodológicas para el desarrollo de propuestas y proyectos de investigación científica. *Información tecnológica*. 31(6). pp. 159-170. https://dx.doi.org/10.4067/S0718-07642020000600159

Guzmán, V. (2021). El método cualitativo y su aporte a la investigación en las ciencias sociales. *Gestionar: Revista de Empresa y Gobierno*. 1(4). pp. 19–31. https://doi.org/10.35622/j.rg.2021.04.002

Hamui, L., y Vives, T. (2021). La codificación y categorización en la teoría fundamentada, un método para el análisis de los datos cualitativos. *Investigación en Educación Médica*. 10(40). pp. 97-104. https://doi.org/10.22201/fm.20075057e.2021.40.21367

Hernández, S., y Duana, D. (2020). Técnicas e instrumentos de recolección de datos. *Boletín Científico De Las Ciencias Económico Administrativas Del ICEA.* 9(17). 51-53. https://doi.org/10.29057/icea.v9i17.6019

Hernández, S. et al. (2014). *Metodología de la investigación.* Recuperado el 20 de febrero del 2022: https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Huamaní, H., Machuca, J. y Riega, Y., (2021). Contratación electrónica y los delitos informáticos. En protección al consumidor en el Perú. *Lex - Revista de la Facultad de Derecho y Ciencias Políticas - Universidad Alas Peruanas*. Volumen 19 N° 28. pp. 197-236. http://dx.doi.org/10.21503/lex.v19i28.2318

Instituto Nacional de Estadística e Informática [INEI]. (2020). Estado de la Población Peruana 2020. https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1743/Libro.pdf

Mayer, L. (2018). Elementos criminológicos para el análisis jurídico - penal de los delitos informáticos. *Ius et Praxis.* Volumen 24. págs. 159-206. http://dx.doi.org/10.4067/S0718-00122018000100159

Mayer, L. (2019). El bien jurídico protegido en los delitos informáticos. *Revist chilena de derecho.* Volumen 44. Nº 1. pp. 235 - 260. https://doi.org/10.4067/S0718-34372017000100011

Mayer, L. y Oliver, G. (2020). *El delito de fraude informático: Concepto y delimitación*. Revista chilena de Derecho y Tecnología. VOL. 9 NÚM. 1. PP. 151-184.https://rchdt.uchile.cl/index.php/RCHDT/article/download/57149/61669/

Mayer, L. y Vera, J. (2020). El delito de espionaje informático: Concepto y delimitación. *Revista Chilena de Derecho y Tecnología - Pontificia Universidad Catolica Valparaíso Chile - Centro de estudios en derecho informático facultad de derecho Universidad de Chile.* Volumen 9. Nº 2. pp. 221 - 256. https://doi.org/10.5354/0719-2584.2020.592 6

Medina, J., Cárdenas, C y Mejía, M. (2021). Análisis del Phishing y la Ley de delitos informáticos en Colombia. *Cuaderno De Investigaciones: Semilleros Andina*, *1*(14). https://doi.org/10.33132/26196301.1948

Ministerio de Justicia y Derechos Humanos [MINJUSDH] (2020) *Diagnóstico situacional multisectorial sobre la ciberdelincuencia en el Perú.* https://indagaweb.minjus.gob.pe/wp-content/uploads/2020/12/01-Diagn%C3%B3stico-Situacional-Multisectorial-sobre-la-Ciberdelincuencia-en-el-Per%C3%BA.pdf

Morales, S. y Daza, S. (2016). *El concepto de Patrimonio y su aplicación en España.* Recuperado el 25 de febrero del 2022: https://repository.ucatolica.edu.co/bitstream/10983/14364/4/El-concepto-de-patrimonio-y-su-aplicacion-en-espana.pdf

Ocón, J. (2018). Derecho a la intimidad y registro de dispositivos informáticos: a propósito del asunto Trabajo Rueda c. España. Revista Española de Derecho Constitucional, 113, 327-343. doi: https://doi.org/10.18042/cepc/redc.113.11

Ortiz, D., Pazmiño, C., Pilay, L. y Ramos, T. (2019). Los delitos informáticos en la vulnerabilidad de las empresas en medios tecnológicos. *Revista Ciencia digital.* 3(2.6) pp. 481-494. https://doi.org/10.33262/cienciadigital.v3i2.6.598

Leyva, C. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. *Revista "Lucerna*

Iuris Et Investigatio". VOL. 01 - 2021, pp. 29 - 48 https://doi.org/10.15381/lucerna.v0i1.18373

Pereyra y Turpo, (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.* Universidad Tecnológica del Perú. Recuperado el 04 de marzo del 2022 de: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/3579/Luz%20Pereyra_Jessy%20Turpo_Trabajo%20de%20Investigacion_Bachiller_2020.pdf?sequence=1&isAllowed=y

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO - Revista Latinoamericana de Estudio de seguridad.* Nº 20. pp. 80-93. http://dx.doi.org/10.17141/urvio.20.2017.2563

Noreña, A. et. al (2012). *Aplicabilidad de los criterios de rigor y éticos en la investigación cualitativa*. Recuperado el 22 de febrero del 2022: http://jbposgrado.org/icuali/Criterios%20de%20rigor%20en%20la%20Inv%20cualitativa.pdf

Paz, E. (2018). La Ética en la Investigación Educativa. *Revista Ciencias Pedagógicas e Innovación*. 6(1). pp. 45-51. https://doi.org/10.26423/rcpi.v6i1.219

Ríos, K. (2019). La entrevista semi-estructurada y las fallas en la estructura. La revisión del método desde una psicología crítica y como una crítica a la psicología. *Caleidoscopio - Revista Semestral de Ciencias Sociales y Humanidades*. 23(41). pp. 65–91. https://doi.org/10.33064/41crscsh1203

Rodriguez, M. (2010). *Métodos de interpretación, hermenéutica y derecho natural.* Recuperado el 23 de febrero del 2022: http://www.scielo.org.co/pdf/dika/v19n2/v19n2a04.pdf

Rojas, S. y Mojica, J. (2014) *De la causalidad adecuada a la imputación objetiva en la responsabilidad civil colombiana,* 129 Vniversitas, 187-235. http://dx.doi.org/10.11144/Javeriana.VJ129. caio

Sánchez, F. (2019). Fundamentos epistémicos de la investigación cualitativa y cuantitativa: consensos y disensos. *Revista Digital de Investigación en Docencia Universitaria*, *13*(1), 102-122. https://dx.doi.org/10.19083/ridu.2019.644

Sánchez, S. (2021). Perfiles del ciberdelito: Un campo de estudio inexplorado. *Revista De Derecho*, (30), 67–76. https://doi.org/10.5377/derecho.v1i30.12223

Schneider, B. (2004). *Secrets y lies. Digital Security in a networked world (John Wiley y Sons Inc.)* https://www.accord.edu.so/web/content/32538?download=true&access_token=d5a8988c-4ac7-4eed-872f-c206fd8bd147

Schlack, A. (2008). *El concepto de patrimonio y su contenido en el delito de estafa.* Revista Chilena de Derecho, Vol. 35, núm. 2, 2008, pp. 261-292. https://www.redalyc.org/pdf/1770/177014518003.pdf

Sánchez, F. (2019). Fundamentos epistémicos de la investigación cualitativa y cuantitativa: consensos y disensos. *Revista Digital de Investigación en Docencia Universitaria*, *13* (1), pp. 102-122. https://dx.doi.org/10.19083/ridu.2019.644

Lizcano, A., Barbosa, J. y Villamizar, J. (2019). Aprendizaje colaborativo con apoyo en TIC: concepto, metodología y recursos. *Magis, Revista Internacional De Investigación En Educación*, *12* (24), pp. 5–24. https://doi.org/10.11144/Javeriana.m12-24.acat

Orozco, J., y Díaz, A. (2018). ¿Cómo redactar los antecedentes de una investigación cualitativa?. *Revista Electrónica de conocimientos, saberes y prácticas.* 1(2), pp. 66-82. https://doi.org/10.30698/recsp.v1i2.13

Rodas, P., y Loor, E. (2018). Proceso de formación en tipificación en el código orgánico integral penal para los delitos cibernéticos. *Revista Iberoamericana De educación*, *1*(1). https://doi.org/10.31876/ie.v1i1.4

Ortega, W., Gamarra, S., y Yon, M. (2021). Enfoque de investigación sistémica Vs. enfoque de investigación científica: análisis comparativo de su efectividad. *Maestro y Sociedad*. 18(3). pp. 967-983. https://maestroysociedad.uo.edu.cu/index.php/MyS/article/view/5388

Utreras, P. (2017). *La necesidad de tipificar el fraude informático en Chile.* [Tesis de Licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile]. Archivo digital. https://repositorio.uchile.cl/bitstream/handle/2250/151758/La-necesidad-de-tipificar-el-delito-de-fraude-inform%c3%a1tico-en-Chile-an%c3%a1lisis-jurisprudencial-doctrinario-y-normativo.pdf?sequence=1&isAllowed=y

Vinelli R. (2021). *Los delitos informáticos y su relación con la criminalidad económica. Ius et Praxis, Revista de la Facultad de Derecho N° 53-2021, pp. 95-110*: https://doi.org/10.26439/iusetpraxis2021.n053.4995

Zambrano, A. (2021). El uso de banca móvil en los delitos informáticos contra el patrimonio en la ciudad de Arequipa, 2020. Universidad César Vallejo. Recuperado el 04 de marzo del 2022 de: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/62306/Zambrano_GAA-SD.pdf?sequence=1&isAllowed=y

Zevallos, O. (2020). *Delitos informáticos: ¿Cuáles son los principales fraudes informáticos que se pueden cometer a través del E-Commerce?* Recuperado el 15 de febrero del 2022: https://ius360.com/delitos-

informaticos-cuales-son-los-principales-fraudes-informaticos-que-se-pueden-cometer-a-traves-del-e-commerce-oscar-zevallos-prado/#:~:text=Los%20principales%20fraudes%20informaticos%20que,%2C%20ransomware%2C%20smishing%20y%20 phishing

VII. ANEXOS: ANEXO N° 01: MATRIZ DE CATEGORIZACIÓN APRIORÍSTICA

VARIABLES DE ESTUDIO	DIMENSIÓN	DEFINICIÓN CONCEPTUAL	DEFINICION OPERACIONAL	INDICADORES	ESCALA DE DIMENSIÓN
Ley N° 30096	Delitos Informáticos	Rodas y Loor (2018), es toda actividad ilícita que tiene por esencia robo de información, contraseñas, y consecuente fraude a cuentas bancarias u otros.	Los procedimientos que se emplearan para medir la variable son: revistas indexadas, tesis y doctrina.	Convenio de Budapest (2004) Código Penal – Art. 186° Ley N° 30171	Nominal
	Tecnología de información y Comunicación – TIC	Permite la comunicación y adquisición de información, almacenamiento, producción, acceso, acciones a distancia (educativo, laboral y entretenimiento). (Cruz et al. 2019)		Entidades bancarias Billetera digital	
Fraude Informático	Modalidades	Phishing (email), Cartas nigerianas (email o sms), Llamada perdida (mensaje de voz), Sim swapping (cobertura), Hacker (protege-acceso ilícito), Cracker (viola y daña sistema), Lammer (descarga) y Script kiddie (virus). (Crespo, 2020)	Los procedimientos que se emplearan para medir la variable son: encuesta y entrevistas.	Hacker Cracker Phishing Spear Phishing Whale Phishing Social Phishing Pharming Sim Swapping Lammer Script kiddie	Nominal
	División de Investigación de Delitos de Alta Tecnología - DIVINDAT	Función de ejecución de análisis informático forense de equipos electrónicos con capacidad de almacenamiento de información, inmersos en la comisión del delito. (MINJUSDH, 2020)		Policía Nacional del Perú División de Investigación Criminal (DIRINCRI)	

Fuente: Propia

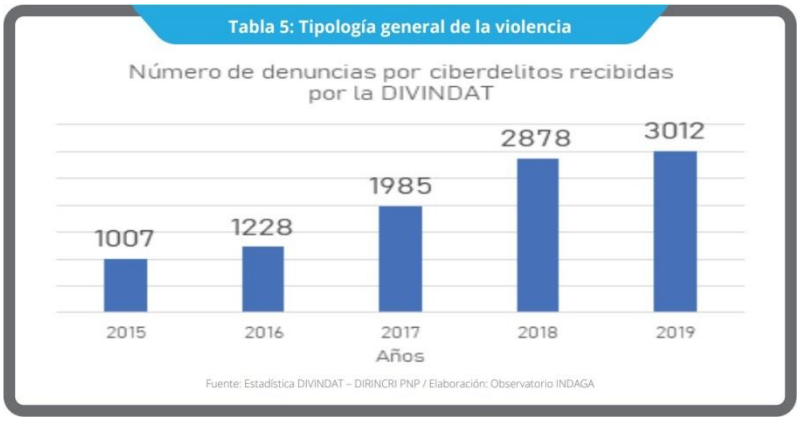
ÁMBITO TEMÁTICO	PROBLEMA DE INVESTIGACIÓN	OBJETIVOS GENERALES	PREGUNTAS DE INVESTIGACIÓN	CATEGORÍAS	SUBCATEGORÍAS
Deficiencias Legislativas en el Tratamiento de la Ley N° 30096, Ley de Delitos Informáticos – Fraude Informático	¿Existen deficiencias legislativas en la Ley Nº 30096 - Fraude Informático en Lima durante el periodo del 2019-2021?	Determinar cuáles son las deficiencias legislativas en la Ley N° 30096 - Fraude Informático en Lima durante el periodo del 2019-2021	1. ¿Cómo define usted el concepto de Fraude Informático como institución jurídica, regulada por el Artículo 8°? 2. De acuerdo a su experiencia, en términos porcentuales, ¿Cuál cree usted que es la incidencia de denuncias relacionadas al delito de Fraude Informático entre los Delitos Informáticos en Lima durante el periodo 2019 - 2021? 3. ¿Qué deficiencias legislativas puede advertir en el Artículo 8°? 4. ¿Cuál cree usted que sea el principal motivo por el cual se archivan a nivel preliminar las investigaciones por fraude informático?	Ley N° 30096	Delitos Informáticos
	PROBLEMA ESPECÍFICO	**OBJETIVOS ESPECÍFICOS**			Tecnología de información y Comunicación – TIC
	¿Por qué se necesita eliminar o erradicar las deficiencias legislativas en el artículo 8°?	Definir las razones por las que se debe mejorar o erradicar las deficiencias del artículo 8° de la Ley N° 30096.	5. ¿Considera que mejorar la estructura normativa del delito de Fraude Informático estipulado en el Artículo 8°? 6. ¿Qué opinión merece el aumento progresivo en la comisión del delito de Fraude Informático y el uso de las tecnologías digitales para tal fin?	Fraude Informático	Modalidades
	¿Es pertinente plantear mejoras a la estructura normativa del artículo 8°?	Analizar las propuestas para mejorar o erradicar las deficiencias del artículo 8° de la Ley N° 30096.	7. ¿Qué opinión merece el planteamiento del incremento presupuestal de las siguientes instituciones públicas: DIVINDAT, Fiscalía de Ciberdelincuencia y Juzgados Penales, con la finalidad de reducir y/o erradicar la comisión del delito de Fraude Informático? 8. ¿Considera pertinente la aplicación de normas análogas del Derecho Penal, peruano o internacional, ante las deficiencias legislativas del delito de Fraude Informático? 9. ¿Qué medida o medidas complementarias a la interposición de la denuncia del agraviado por el delito de Fraude Informático?		

	¿Qué sugerencias planteamos para eliminar o erradicar las deficiencias legislativas en el artículo 8°?	Establecer propuestas que coadyuven a mejorar o erradicar las deficiencias del artículo 8° de la Ley N° 30096.	10. ¿Qué opina usted de la implementación de un registro de denuncias de delitos de Fraude Informático, bajo el control de la Superintendencia de Banca, Seguros y AFPs? 11. ¿Considera usted necesaria la capacitación de jueces, fiscales y funcionarios del Poder Judicial y el Ministerio Público, así como de miembros de la DIVINDAT - PNP, sobre los alcances de la Ley N° 30096 - Ley de Delitos Informáticos, casuística, aplicación de la Ley, índice de denuncias y modus operandi en la comisión de los mismos? ¿Tiene usted alguna propuesta, comentario o solución alternativa que aportar al presente tema de investigación?		División de Investigación de Delitos de Alta Tecnología - DIVINDAT

Fuente: Propia

ANEXO N° 02: RESULTADO PORCENTUAL DE DENUNCIAS EFECTUADAS POR DELITOS INFORMÁTICOS RECABADOS EN LA DIVINDAT.

Respecto a la evolución de cantidad de denuncias realizadas en la DIVINDAT, efectuada durante los años 2015 al 2019, en el informe gubernamental realizado por el MINJUSDH, realizada por el CONAPOC, se tiene la siguiente gráfica.



Fuente: MINJUSDH - CONAPOC

Respecto a las características académicas o profesionales de los perpetradores de delitos informáticos, así como el perfil de la víctima, según denuncias recabadas por la DIVINDAT.

Tabla 10:

Tipo de ciberdelito	Actoresidentificados	
	Perfiles del ciberdelincuente	Perfiles de las víctimas
Abuso de mecanismos y dispositivos informáticos	▪ Profesionales en ingeniería de sistemas e ingeniería electrónica. ▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Personas jurídicas.
Contra datos y sistemas informáticos	▪ Profesionales en ingeniería de sistemas e ingeniería electrónica. ▪ Personal técnico en computación. ▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Entidades financieras.
Contra la fe pública	▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Empresas.
Contra la indemnidad y libertad sexual	▪ Profesionales de la educación. ▪ Personas con diagnóstico clínico de malestar psicológico. ▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Niños, niñas y adolescentes vulnerables.
Contra el patrimonio y fraude informático	▪ Profesionales en ingeniería de sistemas e ingeniería electrónica. ▪ Personal técnico en computación. ▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Entidades financieras.
Otros cometidos mediante el uso de TIC	▪ Profesionales en ingeniería de sistemas e ingeniería electrónica. ▪ Personal técnico en computación. ▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Entidades financieras.

Fuente: DIVINDAT – DIRINCRI PNP / Elaboración: DIVINDAT – DIRINCRI PNP

Fuente: MINJUSDH - CONAPOC

ANEXO N° 03: RESULTADOS RECABADOS DEL PORTAL DEL MINISTERIO PÚBLICO SOBRE LOS DELITOS INFORMÁTICOS

ENERO: 2019

DELITOS EN FISCALÍAS PROVINCIALES PENALES Y MIXTAS A NIVEL NACIONAL

LEY Nº 30096, LEY DE DELITOS INFORMÁTICOS

Durante el mes de enero del año 2019, se registró un total de 616 delitos informáticos, cifra mayor en un 124.00% a los delitos registrados en el mismo período del año 2018 que fueron de 275 delitos; asimismo, al mes de enero del 2019 se puede observar que el tipo de delito con mayor incidencia se presenta en los delitos informáticos contra el patrimonio con un 33.77%.

Cuadro N°47

Delitos registrados en fiscalías provinciales penales y mixtas según tipo de delito sub genérico a nivel nacional - ley nº 30096, ley de delitos informáticos enero 2018 y enero 2019.

DELITOS SUB GENÉRICOS	2018 ENERO		2019 ENERO	
	N° DELITOS	%	N° DELITOS	%
LEY Nº 30096, LEY DE DELITOS INFORMÁTICOS				
DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO	116	42.18	208	33.77
DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA	9	3.27	22	3.57
DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS	11	4.00	21	3.41
DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	6	2.18	10	1.62
DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	6	2.18	3	0.49
DISPOSICIONES COMUNES	4	1.45	2	0.32
SIN ESPECIFICAR DELITO SUB GENÉRICO	123	44.74	350	56.82
TOTAL	275	100.00	616	100.00

FUENTE: Boletín N° 1 - Boletín Estadístico del Ministerio Público - enero (2019), emitido en marzo del 2019.

FEBRERO: 2019

Cuadro N°47

Delitos registrados en fiscalías provinciales penales y mixtas según tipo de delito sub genérico a nivel nacional - ley nº 30096, ley de delitos informáticos febrero 2018 y febrero 2019.

DELITOS SUB GENÉRICOS	2018 FEBRERO		2019 FEBRERO	
	N° DELITOS	%	N° DELITOS	%
LEY Nº 30096, LEY DE DELITOS INFORMÁTICOS				
DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO	216	40.07	353	34.14
DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA	16	2.97	43	4.16
DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS	14	2.60	36	3.48
DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	20	3.71	16	1.55
DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	9	1.67	5	0.48
DISPOSICIONES COMUNES	6	1.11	5	0.48
SIN ESPECIFICAR DELITO SUB GENÉRICO	258	47.87	576	55.71
TOTAL	539	100.00	1,034	100.00

FUENTE: Boletín N° 1 - Boletín Estadístico del Ministerio Público - enero (2019), emitido en marzo del 2019.

MARZO: 2019

Cuadro N°47

Delitos registrados en fiscalías provinciales penales y mixtas según tipo de delito sub genérico a nivel nacional - ley nº 30096, ley de delitos informáticos marzo 2018 y marzo 2019.

DELITOS SUB GENÉRICOS	2018 MARZO		2019 MARZO	
	N° DELITOS	%	N° DELITOS	%
LEY Nº 30096, LEY DE DELITOS INFORMÁTICOS				
DELITOS INFORMATICOS CONTRA EL PATRIMONIO	299	38.88	554	36.07
DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	20	2.60	62	4.04
DELITOS INFORMATICOS CONTRA LA FE PUBLICA	21	2.73	59	3.84
DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	29	3.77	20	1.30
DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	11	1.43	12	0.78
DISPOSICIONES COMUNES	9	1.17	5	0.33
SIN ESPECIFICAR DELITO SUB GENÉRICO	380	49.42	824	53.64
TOTAL	769	100.00	1,536	100.00

FUENTE: Boletín N° 1 - Boletín Estadístico del Ministerio Público - enero (2019), emitido en marzo del 2019.

ANEXO N° 04: GUIA DE ENTREVISTA EFECTUADA A LA JUEZ MARIA DEL ROSARIO CARRILLO ESPICHAN

UNIVERSIDAD CÉSAR VALLEJO

GUÍA DE ENTREVISTA

Título: "Deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático, Lima 2019-2021"

INDICACIONES: *El presente instrumento tiene por finalidad recabar opinión de miembros especializados en la materia, tanto a nivel judicial como fiscal en materia penal, así como de miembros de la PNP - DIVINDAT.*

Respecto a las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático, Lima 2019-2021, agradeceré responda a las siguientes preguntas, para lo cual se le pide responder a las siguientes preguntas con mayor sinceridad y precisión las siguientes preguntas:

Entrevistado (a): MARÍA DEL ROSARIO CARRILLO ESPICHÁN

Cargo/Profesión/Grado académico: jueza supernumeraria en Juzgado Penal Unipersonal Supraprovincial en delitos Tributarios, Aduaneros, Propiedad Intelectual y Ambiental de la Corte Superior de Justicia de Lima. Abogada, egresada en doctorado, egresada en maestría en derecho civil y comercial, y egresada en maestría en ciencias penales.

Institución: Poder Judicial

OBJETIVO GENERAL

Determinar las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático en Lima durante el periodo del 2019-2021

1. ¿Cómo define usted el concepto de Fraude Informático como institución jurídica, regulada por el Artículo 8° de la Ley Nº 30096?

   El incremento en el uso de la tecnología ha generado como contrapartida, que con ello se obtenga información de las contraseñas de las tarjetas de créditos, así como de las cuentas a través de medios fraudulentos, sea por llamadas telefónicas, mensajes de texto, correos electrónicos, etc., en forma similar o tan igual las entidades a entidades bancarias generando confusión en los clientes y con ello la pérdida de responsabilidad de éstos.

2. De acuerdo a su experiencia, en términos porcentuales, ¿Cuál cree usted que es la incidencia de denuncias relacionadas al delito de Fraude Informático entre los Delitos Informáticos en Lima durante el periodo 2019 - 2021?

No tengo acceso a un número porcentual, pero desde que asumí este despacho desde noviembre del 2021 hasta la actualidad mayo del 2022, se han tramitado 3 expedientes 2 de ellos con terminación anticipada.

¿Qué deficiencias legislativas puede advertir en el Artículo 8°[1] (Fraude Informático) de la Ley N° 30096 – Ley de Delitos Informáticos?

Considero que no solo debe establecerse multas a la entidad financiera en el caso que no remita información, sino también en el caso de que los sentenciados sean trabajadores de las entidades financieras pues a través de ellos son quienes tienen acceso a información privilegiada deben responder como terceros civilmente responsables.

3. ¿Cuál cree usted que sea el principal motivo por el cual se archivan a nivel preliminar las investigaciones por fraude informático?

Por desconocimiento, solo que los afectados desconocen y otros prefieren no invertir tiempo y dinero. Existen dos caminos, depende si la entidad financiera ha envidado la constancia de transacción o no. El primero, si no ha enviado la constancia de transacción, se realiza un reclamo la entidad financiera quien resuelve rechazar, indicando que es responsabilidad del cliente "la reserva" de la clave; sin embargo, es obligación de esta, enviar el envío del comprobante de la transacción realizar la entidad financiera y si no lo ha realizado se realiza el reclamo ante INDECOPI. Ahora si la entidad financiera envió la constancia de transacción y no ha sido autorizado se procede a la denuncia respectiva, que por obvias razones no puede ser archivadas. Ambos caminos son exitosos.

OBJETIVO ESPECÍFICO N° 01

Definir las razones por la que se debe mejorar o erradicar las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático en Lima durante el periodo del 2019-2021

4. ¿Considera usted que mejorar la estructura normativa del delito de Fraude Informático estipulado en el Artículo 8° de la Ley N° 30096 – ¿Ley de Delitos Informáticos, coadyuvará a la prevención del delito? (Fundamente su respuesta)

Considero que más que mejorar la estructura del delito, son las entidades financieras las que deben mejorar sus medidas de seguridad en el acceso a la base de datos a su sistema. El acceso a estas se esta tornando tan común que incluso lo hacen por montos mínimos y a diario que los clientes no se percatan y hace que pasen desapercibidos.

5. ¿Qué opinión merece el aumento progresivo en la comisión del delito de Fraude Informático y el uso de las tecnologías digitales para tal fin?

Como lo acabo de indicar en la respuesta anterior, el uso de esta modalidad se está volviendo tan común, que torna inseguro el uso de las tarjetas de crédito.

OBJETIVO ESPECÍFICO N°02

[1] **"Artículo 8° Fraude informático:** El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el 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 no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social."

Analizar las propuestas de mejorar o erradicar las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático en Lima durante el periodo del 2019-2021

6. ¿Qué opinión merece el planteamiento del incremento presupuestal de las siguientes instituciones públicas: DIVINDAT[2], Fiscalía de Ciberdelincuencia y Juzgados Penales, con la finalidad de reducir y/o erradicar la comisión del delito de Fraude Informático?

   Como lo he indicado también en mi respuesta 4, la mejor forma de prevenir esta clase de delito, es que las entidades financieras, bancarias, etc., adopten medidas de seguridad al respecto.

7. ¿Considera pertinente la aplicación de normas análogas[3] del Derecho Penal, peruano o internacional, ante las deficiencias legislativas del delito de Fraude Informático?, Explique.

   Las entidades financieras la mayoría al ser internacionales, deben implementarse sanciones pecuniarias y administrativas a nivel internacional tanto a las entidades financieras como a sus representantes legales.

8. De acuerdo a su experiencia ¿Qué medida o medidas complementarias a la interposición de la denuncia del agraviado por el delito de Fraude Informático, se podrían implementar legislativamente con el objetivo de retrotraer el daño causado al estado anterior de la comisión del delito (Recuperación inmediata del patrimonio sustraído)?

   La simplificación en el trámite, así como que no solo incluye la recuperación del patrimonio sustraído porque finalmente dicho monto va para la entidad financiera quien decide devolverte el monto no reconocido. Ello debe incluir los gastos asumidos innecesariamente como repito porque la entidad financiera no adopta las medidas de seguridad en el acceso de la base de datos a sus clientes.

OBJETIVO ESPECÍFICO N° 03

Establecer propuestas que coadyuven a mejorar o erradicar las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático en Lima durante el periodo del 2019-2021

9. ¿Qué opina usted de la implementación de un registro de denuncias de delitos de Fraude Informático, bajo el control de la Superintendencia de Banca, Seguros y Afp?

   Es una excelente propuesta, a efectos de que los clientes puedan tener conocimiento en que entidad financiera, banco tiene mayores denuncias y no confiar sus fondos.

---

[2] **DIVINDAT:** División de Investigación de delitos de alta tecnología de la DIRINCRI – PNP.

[3] **Norma análoga:** Procedimiento lógico de aplicar una norma establecida para una situación determinada a un caso distinto pero semejante.

10. ¿Considera usted necesaria la capacitación de jueces, fiscales y funcionarios del Poder Judicial y el Ministerio Público, así como de miembros de la DIVINDAT - PNP, sobre los alcances de la Ley N° 30096 - Ley de Delitos Informáticos, casuística, aplicación de la Ley, ¿índice de denuncias y modus operandi en la comisión de los mismos? Explique.

Considero que este grupo de personas si tienen conocimiento de los alcances de la Ley, siendo en quienes deberían incidirse más, es en la población vulnerable, pues como repito esta modalidad se está volviendo común. Como experiencia personal, en el mes de febrero 2022, revise el app del BCP y tenía consumos diarios de S/12, S/13, S/14, cuando hice mi reclamo me devolvieron los montos, porque obviamente no había autorizado dichas transacciones. (Adjunto cartas). Por ello, te indico, a los que realizan este tipo de delitos les resulta más fácil sustraer montos pequeños y a los Bancos les resulta más económico devolver montos pequeños que realizar medidas de seguridad, mientras que el cliente es el más perjudicado porque tiene que bloquear la tarjeta ir a renovarla, etc.

11. Finalmente ¿Tiene usted alguna propuesta, comentario o solución alternativa que aportar al presente tema de investigación?

La Superintendencia de Banca y Seguros debe establecer un sistema de control auditor en los Bancos y entidades financieras a efectos de determinar que medidas de seguridad están realizando, de lo contrario sancionar con el cierre definitivo.

PODER JUDICIAL

MARIA DEL ROSARIO ARAUJO ESPICHAN
JUEZ
Juzgado Penal Unipersonal Supraprovincial en Delitos Aduaneros, Tributarios, de Propiedad Intelectual y Ambientales de Lima
CORTE SUPERIOR DE JUSTICIA DE LIMA

Lima, 09 de mayo de 2022.

ANEXO N° 05: GUIA DE ENTREVISTA EFECTUADA A LA ASISTENTE DE RELATORÍA DE LA 2DA. SALA PENAL LIQUIDADORA MARIA ALEJANDRA RAMOS RAMOS

UNIVERSIDAD CÉSAR VALLEJO

GUÍA DE ENTREVISTA

Título: "Deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático, Lima 2019-2021"

INDICACIONES: *El presente instrumento tiene por finalidad recabar opinión de miembros especializados en la materia, tanto a nivel judicial como fiscal en materia penal, así como de miembros de la PNP - DIVINDAT.*

Respecto a las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático, Lima 2019-2021, agradeceré responda a las siguientes preguntas, para lo cual se le pide responder a las siguientes preguntas con mayor sinceridad y precisión las siguientes preguntas:

Entrevistado (a): María Alejandra Ramos Ramos

Cargo/Profesión/Grado académico: Asistente Relatoría – Abogada

Institución: Poder Judicial

OBJETIVO GENERAL

Determinar las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático en Lima durante el periodo del 2019-2021

1. ¿Cómo define usted el concepto de Fraude Informático como institución jurídica, regulada por el Artículo 8° de la Ley Nº 30096?

   Es aquel ilícito penal que se comete empleando la tecnología de la información o de la comunicación, para obtener un provecho ilícito por parte del sujeto activo, ya sea introduciendo, alterando, clonando, etc datos informáticos o manipulando un sistema informático.

2. De acuerdo a su experiencia, en términos porcentuales, ¿Cuál cree usted que es la incidencia de denuncias relacionadas al delito de Fraude Informático entre los Delitos Informáticos en Lima durante el periodo 2019 - 2021?

   Un 70%, tomando en cuenta que hoy en día la tecnología es un medio muy recurrido por la mayoría de personas.

3. ¿Qué deficiencias legislativas puede advertir en el Artículo 8°[1] (Fraude Informático) de la Ley N° 30096 – Ley de Delitos Informáticos?

Que se encuentran vacíos legales en dicha legislación, toda vez que no regula todas las modalidades de delinquir a través de los medios informáticos, siendo que hoy en día existen diversos formar de delinquir mediante el uso de la tecnología.

4. ¿Cuál cree usted que sea el principal motivo por el cual se archivan a nivel preliminar las investigaciones por fraude informático?

Que no se encuentra debidamente regulados, por lo que en muchas ocasiones quedan como atípicos, siendo archivados, en otros casos se da porque el sistema de investigación para este tipo de delitos resulta ineficiente no logrando en muchos casos dar con el responsable.

OBJETIVO ESPECÍFICO N° 01

Definir las razones por la que se debe mejorar o erradicar las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático en Lima durante el periodo del 2019-2021

5. ¿Considera usted que mejorar la estructura normativa del delito de Fraude Informático estipulado en el Artículo 8° de la Ley N° 30096 – Ley de Delitos Informáticos, coadyuvará a la prevención del delito? (Fundamente su respuesta)

Si, en definitiva, ya que, con una mejor implementación de la estructura normativa para el fraude informático, hace que estos delitos especiales sean sancionados de una manera adecuada y en definitiva hace que los delincuentes sepan que este tipo de delitos no quedaran impunes y de ser el caso serán sancionados con una pena ejemplar, previniendo de una u otra manera el incremento masivo de este tipo de delitos.

6. ¿Qué opinión merece el aumento progresivo en la comisión del delito de Fraude Informático y el uso de las tecnologías digitales para tal fin?

Pues que es una lastima que hoy en día, algo como lo es la tecnología sea utilizada por personas inescrupulosas para cometer este tipo de delitos como lo son el fraude informático, tomando en cuenta que en la actualidad la tecnología es un medio muy recurrido por la mayoría de personas.

---

[1] **"Artículo 8° Fraude informático:** El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el 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 no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social."

OBJETIVO ESPECÍFICO N°02

Analizar las propuestas de mejorar o erradicar las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático en Lima durante el periodo del 2019-2021

7. ¿Qué opinión merece el planteamiento del incremento presupuestal de las siguientes instituciones públicas: DIVINDAT[2], Fiscalía de Ciberdelincuencia y Juzgados Penales, con la finalidad de reducir y/o erradicar la comisión del delito de Fraude Informático?

   Pues me parece un buen planteamiento, tomando en cuenta que con el uso de mayores implementos tecnológicos, se podría hacer una mejor y adecuada investigación por parte de las instituciones publicas antes mencionadas y por consiguiente realizar una adecuada investigación que permita identificar a los ciberdelincuentes.

8. ¿Considera pertinente la aplicación de normas análogas[3] del Derecho Penal, peruano o internacional, ante las deficiencias legislativas del delito de Fraude Informático?, Explique.

   Claro que sí, sin dejar de lado también que el Perú tiene convenios sobre la ciberdelincuencia con una serie de tratados europeos.

9. De acuerdo a su experiencia ¿Qué medida o medidas complementarias a la interposición de la denuncia del agraviado por el delito de Fraude Informático, se podrían implementar legislativamente con el objetivo de retrotraer el daño causado al estado anterior de la comisión del delito (Recuperación inmediata del patrimonio sustraído)?

   Creo que en muchos casos la recuperación inmediata del patrimonio sustraído es complicado, creo que la mejor prevención para este tipo de delitos, en definitiva, es tomar conocimiento de los beneficios como problemáticas del uso desmesurado de la tecnología y proteger el uso de nuestros datos, o ante un robo o hurto de pertenencias como dni, etc. hacer la denuncia correspondiente, ya que en muchos casos el descuido de los ciudadanos permite que personas inescrupulosas, hagan uso de esos descuidos para suplantar identidades, o realizar fraudes informáticos que luego cuando nos damos cuenta estos en algunos casos pueden ser prevenidos.

---

[2] **DIVINDAT:** División de Investigación de delitos de alta tecnología de la DIRINCRI – PNP.

[3] **Norma análoga:** Procedimiento lógico de aplicar una norma establecida para una situación determinada a un caso distinto pero semejante.

OBJETIVO ESPECÍFICO N° 03

Establecer propuestas que coadyuven a mejorar o erradicar las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático en Lima durante el periodo del 2019-2021

10. ¿Qué opina usted de la implementación de un registro de denuncias de delitos de Fraude Informático, bajo el control de la Superintendencia de Banca, Seguros y Afp?

Me parece una buena idea, la implementación de un registro de denuncias bajo el control de la SBS ya que esta institución tiene como fin propiciar una mayor confianza y protección de los intereses del público usuario, ejerciendo control y supervisión de las entidades bancarias, siendo estas entidades en donde mas se cometen los fraudes informáticos y en los que los usuarios en muchos casos son los más perjudicados.

11. ¿Considera usted necesaria la capacitación de jueces, fiscales y funcionarios del Poder Judicial y el Ministerio Público, así como de miembros de la DIVINDAT - PNP, sobre los alcances de la Ley N° 30096 - Ley de Delitos Informáticos, casuística, aplicación de la Ley, ¿índice de denuncias y modus operandi en la comisión de los mismos? Explique.

Si, ya que, al utilizar la tecnología como medio para la comisión de este tipo de delitos, debe haber una capacitación por parte de los operarios de justicia, ya que, de esa manera, los delitos podrán ser investigados de la manera mas adecuada y así no queden impunes.

12. Finalmente ¿Tiene usted alguna propuesta, comentario o solución alternativa que aportar al presente tema de investigación?

A modo de recomendación, creo que se debe diferenciar el fraude informático con la estafa tradicional, pues en muchos casos la administración de justicia ante el desconocimiento de las nuevas modalidades de fraude informático, las califica como delito de estafa y al final terminan siendo casos archivados.

CORTE SUPERIOR DE JUSTICIA DE LIMA
2ª Sala Penal Liquidadora
PODER JUDICIAL
REPÚBLICA DEL PERÚ

MARIA ALEJANDRA
RAMOS RAMOS
ABOGADA
Reg. 82602

FIRMA Y SELLO

Lima, 16 de Mayo del 2022.

ANEXO N° 06: GUIA DE ENTREVISTA EFECTUADA POR EL FISCAL ROBERTO CARLOS VILCHEZ LIMAY – ASESOR DEL GABINETE DE ASESORES DE LA FISCALÍA DE LA NACIÓN

UNIVERSIDAD CÉSAR VALLEJO

GUÍA DE ENTREVISTA

Título: "Deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático, Lima 2019-2021"

INDICACIONES: *El presente instrumento tiene por finalidad recabar opinión de miembros especializados en la materia, tanto a nivel judicial como fiscal en materia penal, así como de miembros de la PNP - DIVINDAT.*

Respecto a las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático, Lima 2019-2021, agradeceré responda a las siguientes preguntas, para lo cual se le pide responder a las siguientes preguntas con mayor sinceridad y precisión las siguientes preguntas:

Entrevistado (a): Roberto Carlos Vilchez Limay

Cargo/Profesión/Grado académico: Asesora del Gabinete de Asesores de la Fiscalía de la Nación, Abogado por la UNMSM

Institución: Ministerio Público

OBJETIVO GENERAL

Determinar las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático en Lima durante el periodo del 2019-2021

1. ¿Cómo define usted el concepto de Fraude Informático como institución jurídica, regulada por el Artículo 8° de la Ley Nº 30096?

   Es aquella conducta que consiste en diseñar; introducir, alterar, borrar, suprimir, clonar de datos informáticos o interferir o manipular el funcionamiento de un sistema informático, mediante el uso de las TICs (tecnologías de la información o de la comunicación), con la finalidad de obtener para sí o para otro un provecho ilícito en perjuicio de tercero.

2. De acuerdo a su experiencia, en términos porcentuales, ¿Cuál cree usted que es la incidencia de denuncias relacionadas al delito de Fraude Informático entre los Delitos Informáticos en Lima durante el periodo 2019 - 2021?

   Aproximadamente, debe ubicarse en el tercer escalafón de denuncias, después de los delitos contra la libertad e identidad sexual y de los delitos contra el patrimonio.

Firma Digital

Firmado digitalmente por VILCHEZ LIMAY Roberto Carlos FAU 20131370301 soft
Motivo: Doy V° B°
Fecha: 09.06.2022 16:22:35 -05:00

3. ¿Qué deficiencias legislativas puede advertir en el Artículo 8°[1] (Fraude Informático) de la Ley N° 30096 – Ley de Delitos Informáticos?

   Desde una perspectiva dogmática, el tipo penal prevé, de manera innecesaria, un elemento subjetivo de tendencia interna trascendente el cual consiste en "para obtener un provecho ilícito para sí o para otro"; siendo que, la lesión a la integridad y secreto del sistema informático se encuentra efectivo, indistintamente que pueda generar un beneficio económico o de otra índole en el sujeto activo.

4. ¿Cuál cree usted que sea el principal motivo por el cual se archivan a nivel preliminar las investigaciones por fraude informático?

   No necesariamente el archivo, a nivel de diligencias preliminares; empero, sí puede generar el sobreseimiento de la causa o la dificultad probatoria para el Ministerio Público, en su estrategia acreditativa en el juicio oral.

OBJETIVO ESPECÍFICO N° 01

Establecer los fundamentos por los que se debe eliminar las deficiencias legislativas en el artículo 8° (fraude informático) de la Ley N° 30096 - Ley de Delitos Informáticos

5. ¿Considera usted que mejorar la estructura normativa del delito de Fraude Informático estipulado en el Artículo 8° de la Ley N° 30096 – Ley de Delitos Informáticos, coadyuvará a la prevención del delito? (Fundamente su respuesta)

   No. El tópico de la prevención general o especial del delito no responden a las modificaciones dogmática en el tipo penal; sino, en la posibilidad de establecer una Política Criminal y Política Pública que enseñen el respeto a la integridad de los datos o sistemáticos informáticos ajenos para motivar una conducta socialmente adecuada.

6. ¿Qué opinión merece el aumento progresivo en la comisión del delito de Fraude Informático y el uso de las tecnologías digitales para tal fin?

   El avance de las TICs se encuentra en consonancia con el desarrollo de la ciencia; en consecuencia, son instrumentos socialmente aceptados, los que, lamentablemente, pueden ser usados para fines ilícitos, aún delictivos; sin embargo, no se puede limitar su uso porque iría en contra de la misma naturaleza del conocimiento humano.

   Lo que podría evaluarse, es optimizar la misma tecnología para desarrollar nuevas técnicas especiales de investigación que lucha contra esta clase de criminalidad.

---

[1] **"Artículo 8° Fraude informático:** El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el 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 no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social."

OBJETIVO ESPECÍFICO N°02

Analizar las propuestas para eliminar las deficiencias legislativas en el artículo 8° (fraude informático) de la Ley N° 30096 - Ley de Delitos Informáticos

7. ¿Qué opinión merece el planteamiento del incremento presupuestal de las siguientes instituciones públicas: DIVINDAT[2], Fiscalía de Ciberdelincuencia y Juzgados Penales, con la finalidad de reducir y/o erradicar la comisión del delito de Fraude Informático?

   Resulta correcto, toda vez que permitirá desarrollar nuevas líneas de indagación en la lucha contra la ciberdelincuencia. Conviene anotar que, actualmente, no existen juzgados penales especializados en la materia.

8. ¿Considera pertinente la aplicación de normas análogas[3] del Derecho Penal, peruano o internacional, ante las deficiencias legislativas del delito de Fraude Informático?, Explique.

   El análisis Comparado de Derecho, a fín de revisar las legislaciones extranjeras, como, principalmente, el estudio Convencional (Convención de Budapest), resulta necesario para optar por un modelo legislativo que permita la eficiencia y eficacia de la punición del tipo penal de fraude informático.

9. De acuerdo a su experiencia ¿Qué medida o medidas complementarias a la interposición de la denuncia del agraviado por el delito de Fraude Informático, se podrían implementar legislativamente con el objetivo de retrotraer el daño causado al estado anterior de la comisión del delito (Recuperación inmediata del patrimonio sustraído)?

   La recuperación inmediata de información o patrimonio, sobre la base del fraude informático, resulta difícilmente obtenible. Indistintamente de ello, el delito ya está consumado. La recuperación del patrimonio estaría más orientado al momento de la reparación civil.

OBJETIVO ESPECÍFICO N° 03

Establecer propuestas que coadyuven a mejorar la estructura normativa del artículo 8° (fraude informático) de la Ley N° 30096 - Ley de Delitos Informáticos

10. ¿Qué opina usted de la implementación de un registro de denuncias de delitos de Fraude Informático, bajo el control de la Superintendencia de Banca, Seguros y Afp?

    Resulta relevante contar con un registro de denuncias por esta clase de delitos, pero que no esté bajo la tutela de la SBS y AFPs, sino, más bien, por la DIVINDAT.

---

[2] **DIVINDAT:** División de Investigación de delitos de alta tecnología de la DIRINCRI – PNP.

[3] **Norma análoga:** Procedimiento lógico de aplicar una norma establecida para una situación determinada a un caso distinto pero semejante.

11. ¿Considera usted necesaria la capacitación de jueces, fiscales y funcionarios del Poder Judicial y el Ministerio Público, así como de miembros de la DIVINDAT - PNP, sobre los alcances de la Ley N° 30096 - Ley de Delitos Informáticos, casuística, aplicación de la Ley, índice de denuncias y modus operandi en la comisión de los mismos? Explique.

    La capacitación académico-profesional resulta siempre relevante. Las capacitaciones deben estar orientadas a recepcionar información de experiencias en otros países donde el fenómeno criminal de la ciberdelincuencia ha sido tratado con anterioridad a nuestro caso (por ejemplo, España, Colombia, Argentina y Chile).

12. Finalmente ¿Tiene usted alguna propuesta, comentario o solución alternativa que aportar al presente tema de investigación?

    Considero que, los mayores problemas en el tópico de la ciberdelincuencia estriban en los vacíos normativos que ostenta nuestra actual legislación (delito contra la propiedad intelectual mediante las TICs y el ciberterrorismo) y los temas procesales (agente encubierto cibernético y la prueba digital), donde debería concentrarse el debate y propuestas de aplicación.

FIRMA Y SELLO

Lima, 07 de junio de 2022..

ANEXO N° 07: GUIA DE ENTREVISTA Y FICHA DE VALIDACIÓN DE INSTRUMENTOS EFECTUADA POR EL CORONEL PNP DE LA DIVINDAT - LUIS EDGARDO HUAMÁN SANTAMARÍA

UNIVERSIDAD CÉSAR VALLEJO

GUÍA DE ENTREVISTA

Titulo: "Deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático, Lima 2019-2021"

INDICACIONES: El presente instrumento tiene por finalidad recabar opinión de miembros especializados en la materia, tanto a nivel judicial como fiscal en materia penal, así como de miembros de la PNP - DIVINDAT.

Respecto a las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático, Lima 2019-2021, agradeceré responda a las siguientes preguntas, para lo cual se le pide responder a las siguientes preguntas con mayor sinceridad y precisión las siguientes preguntas:

Entrevistado (a): Luis Edgardo Huamán Santamaría

Cargo/Profesión/Grado académico: Coronel PNP de la División de Investigación de Delitos de Alta Tecnología de la DIRINCRI, Abogado, Magister en Derecho Penal.

Institución: División de Investigación de Delitos de Alta Tecnología de la DIRINCRI – PNP

OBJETIVO GENERAL

Determinar las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático en Lima durante el periodo del 2019-2021

1. ¿Cómo define usted el concepto de Fraude Informático como institución jurídica, regulada por el Articulo 8° de la Ley Nº 30096?

   Lo que indica el Código el que diseña, introduce datos, altera, para obtener un provecho patrimonial, sin esa característica no habría delito, u obtener cualquier otra ventaja, utilizando los medios informáticos, donde el objeto del delito es otra cosa, en los delitos informáticos se utiliza la PC como medio del delito (delito de fraude informático) o como objeto del delito (cuando meten un Ransomware para secuestrar los datos y encripta su disco duro – es un ataque directo al sistema informático).

2. De acuerdo a su experiencia, en términos porcentuales, ¿Cuál cree usted que es la incidencia de denuncias relacionadas al delito de Fraude Informático entre los Delitos Informáticos en Lima durante el periodo 2019 - 2021?

   No cuento con la data de otros años solo de este año, al primer trimestre del año 2022 se ha reportado un total de 2012 denuncias a nivel Lima Metropolitana, a nivel nacional es visto por otra unidad. Si todas las denuncias llegan a la división como son investigadas, por norma la DIVINDAT debe aceptar todas las denuncias (así no sean de su competencia), la división transfiere al Ministerio Público y como sugerencia indica que: esta investigación debe ser vista por la DIPINCRI invocando el protocolo; cuando no ponemos sugerencias se entiende que será visto por la DIVINDAT, se colige que no todas las denuncias ingresadas son vista por la DIVINDAT, ante ello, hemos coordinado con la séptima región policial de Lima para que sean capacitados la DIPINCRI y las Comisarías, también cuando nos piden hacemos charlas educativas a las mismas comisarias DIPINCRI, como unidad sugiere que se de estricto cumplimiento al Protocolo.

3. ¿Qué deficiencias legislativas puede advertir en el Artículo 8°[1] (Fraude Informático) de la Ley N° 30096 – Ley de Delitos Informáticos?

   Los verbos rectores deben ser entendidos de forma copulativa y exclusiva, por ejemplo cuando la norma indica: "el que deliberada e ilegítimamente procura para si u otro un provecho ilícito en perjuicio de un tercero, mediante el diseño", que sucede cuando hace un diseño si no lo utiliza, no ha cometido aún el delito de fraude, puede entenderse que los verbos rectores deben aplicarse de forma dos o más, aclara que para la comisión del delito debe haber un despojo patrimonial de la víctima todo lo demás quedaría en tentativa, el delito es de resultado.

4. ¿Cuál cree usted que sea el principal motivo por el cual se archivan a nivel preliminar las investigaciones por fraude informático?

   Muchos fiscales adoptan la teoría funcionalista del derecho penal, apuntan a las ideas de Roxin respecto a la imputación objetiva, teoría de riesgos aquel que cree un riesgo entonces comete delito, se crea el riesgo al poseer bienes de cuidado, uno mismo crea el riesgo, es el criterio de los fiscales, son partidarios de la víctima o dogmática, es decir, se hecha la culpa al usuario. Les comento hacer de un tema álgido de la criminalidad, por ejemplo el famoso cuento de la maleta (delito de estafa agravada) mediante el uso de las TIC también

[1] **"Artículo 8° Fraude informático:** El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el 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 no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta

para suplantar la identidad, se da cuando uno esta navegando en Facebook y les llega una solicitud de amistad (de un familiar del extranjero) acepta la solicitud y comienzan a conversas, ojo que es el un perfil clonado, entre las conversaciones le indican que su familiar esta a punto de viajar a Perú se encuentra en el aeropuerto pero tiene un problema no puede viajar por no tener la vacuna pero sus maletas ya están en el avión quiere coordinar con la víctima para que lo reciba, dentro de ellas hay tablets, iphones, celulares, perfumes, entre otros (cosas caras), el delincuente le dice que dará un teléfono por el favor de recibir la maleta, le solicita su DNI y datos para que la maleta llegue a su domicilio, la comunicación ya se da por el WhatsApp, luego de unas horas llaman a la víctima por el tema de una maleta le comunican que la maleta en el aeropuerto esta excediendo de peso que se pondrá a decomiso y que debe pagar una penalidad, solicitando pago S/.17,000.00 Soles para que la maleta sea liberada y pase, indican una cuenta bancaria (cuenta receptora) del servicio de mensajería y transporte, horas después, llaman a la víctima identificándose como la SUNAT refiriendo que el equipaje fue pasado por los rayos X y se ha encontrado dinero en efectivo dentro de las laptos (remiten video de una simulación), la víctima llama al delincuente quien le indica que pague y que del dinero le dará una parte, la víctima solicita le indique cuanto debe pagar y le indican S/.50,000.00, algunas víctimas se dan cuenta y denuncian otros pagan; de todo ello quienes son los actores, en primer lugar el ingeniero social (quien rastrea los datos), diseña la suplantación por Facebook, el inductor el que dialoga, la víctima, supuesto agente de aduanas, todos sin identificarse, quien es el único que se puede identificar, el dueño de la cuenta receptora, ¿se puede producir el delito sin la cuenta receptora? No se puede porque no habría como recibir el dinero, puesto que toda la recepción del dinero es a través de las TIC, ellos no toman en cuenta los fiscales, por tanto, la gran mayoría sale en libertad.

OBJETIVO ESPECÍFICO N° 01

Definir las razones por la que se debe mejorar o erradicar las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático en Lima durante el periodo del 2019-2021

5. ¿Considera usted que mejorar la estructura normativa del delito de Fraude Informático estipulado en el Artículo 8° de la Ley N° 30096 – Ley de Delitos Informáticos, coadyuvará a la prevención del delito? (Fundamente su respuesta)

   Si claro, en primer lugar, indicar que los verbos rectores deben darse de forma copulativa y no solamente excluyente, además el artículo 8° debe ser apoyado por el Protocolo de trabajo

conjunto con el Ministerio Público, en cuanto a la pena se sugiere prisión preventiva no menos de un año para la cuenta receptora, en cuanto a la aplicación de una medida cautelar, esta debe darse a nivel administrativo o civil.

6. ¿Qué opinión merece el aumento progresivo en la comisión del delito de Fraude Informático y el uso de las tecnologías digitales para tal fin?

Todo comenzó con la pandemia y el uso masivo del internet, entonces ha hecho que la gente ya no salga a consumidor donde hasta era de libre acceso, puesto que no había pandemia, las compras por internet también se han masificado, se volvió tendencia, por ello se utilizaron mucho las TIC, no se puede recomendar no usar los móviles, pero si se puede sugerir el control del rubro de las comunicaciones, la seguridad informática, la cultura de cibers, nosotros mismos somos culpables; un sistema informático esta compuesto de tres elementos: hardware, Software y el Humanware (el hombre), siendo el más débil el Humanware, es el responsable, por ejemplo: el pishing, uno sabe que no debe hacer click en un link que son de dudosa procedencia, por eso cuando ustedes vean una página de dudosa procedencia deben copiar el dominio (URL) y colocarlo en páginas amigables, como: whois, exsalion o this person does not exist (se colocan en el buscador de Google) se coloca y busca el dominio e informe, por ejemplo: sale una publicación en Facebook que dice: "Vendo casa", copias el URL lo colocas en la pagina amigable y sale un informe de cuando fue creada, quien lo creo, el administrador, si esta todo privado debes dudar porque puede ser una pagina creada para estafar, si ha sido creada recientemente puede ser una pagina creada para estafar, estas son páginas amigables de inteligencia artificial.

OBJETIVO ESPECÍFICO N°02

Analizar las propuestas de mejorar o erradicar las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático en Lima durante el periodo del 2019-2021

7. ¿Qué opinión merece el planteamiento del incremento presupuestal de las siguientes instituciones públicas: DIVINDAT[2], Fiscalía de Ciberdelincuencia y Juzgados Penales, con la finalidad de reducir y/o erradicar la comisión del delito de Fraude Informático?

Si, se necesitan más herramientas, ustedes saben que el delito evoluciona los delincuentes se implementan de herramientas tecnológicas importantes, nosotros también nos estamos quedando atrás y necesitamos renovar nuestros equipos, se necesitan herramientas de última generación, por ejemplo: Inteligencia Artificial (IA) de Oracle Cloud Infrastructure (OCI), inteligencia de fuente abierta.

8. ¿Considera pertinente la aplicación de normas análogas[1] del Derecho Penal, peruano o internacional, ante las deficiencias legislativas del delito de Fraude Informático?, Explique.

   Si se encuentran vacíos o deficiencias en la ley, hay que acudir a normas extra penales o administrativas, o interpretaciones sistemáticas de las normas, pero teniendo en cuenta el Principio de Legalidad.

9. De acuerdo a su experiencia ¿Qué medida o medidas complementarias a la interposición de la denuncia del agraviado por el delito de Fraude Informático, se podrían implementar legislativamente con el objetivo de retrotraer el daño causado al estado anterior de la comisión del delito (Recuperación inmediata del patrimonio sustraído)?
   Resarcir el daño, aplicación de medidas reales, incautación de los medios comisivos, extinción de dominio, aquí algunas veces no hacemos extinción dominio eso deberíamos informar.

OBJETIVO ESPECÍFICO N° 03

Establecer propuestas que coadyuven a mejorar o erradicar las deficiencias legislativas en el tratamiento de la Ley N° 30096 - Ley de Delitos Informáticos - Fraude Informático en Lima durante el periodo del 2019-2021

10. ¿Qué opina usted de la implementación de un registro de denuncias de delitos de Fraude Informático, bajo el control de la Superintendencia de Banca, Seguros y Afp?
    Tenemos, pero es confidencial, no podemos compartirlo, con que finalidad podría tener el acceso la SBS, ellos no investigan, esos son datos personales que no pueden ser divulgados, es muy delicada.

11. ¿Considera usted necesaria la capacitación de jueces, fiscales y funcionarios del Poder Judicial y el Ministerio Público, así como de miembros de la DIVINDAT - PNP, sobre los

alcances de la Ley N° 30096 - Ley de Delitos Informáticos, casuística, aplicación de la Ley, índice de denuncias y modus operandi en la comisión de los mismos? Explique.

Si se considera necesario, para estar a la par y conversar del mismo tema, es bueno que los fiscales y jueces se capaciten, había cursos Online donde ha participado el Ministerio Público y Poder Judicial, de hace dos años de forma presencial, la idea es que se masifique o fomente más, tenemos una fiscalía de ciberdelincuencia que solamente abarca Lima Metropolitana, y también se tiene una Sala de Fiscalía Superior que se encuentra en Surco, quienes se encuentran aptas, las que necesitarían capacitarlas serían las fiscalías penales.

12. Finalmente ¿Tiene usted alguna propuesta, comentario o solución alternativa que aportar al presente tema de investigación?

Como les dije el ser más indefenso del sistema informático es el ser humano, se debe crear una cultura de cibercriminalidad en la ciudadanía, los medios de prensa deben participar, los colegios enseñarles a los niños, la ciberseguridad, por ejemplo: que pasaría si encuentras un USB en la mesa, te aseguro que lo pones en tu computadora, pero ahí te meten el virus.

CA 228633
Luis Edgardo HUAMAN SANTAMARIA
CORONEL PNP
JEFE DE LA DIVISIÓN DE INVESTIGACIÓN DE DELITOS DE ALTA TECNOLOGÍA - DIRINCRI PNP

FIRMA Y SELLO

Lima, 28 de mayo del 2022.

UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

I.1. Apellidos y Nombres: HUAMAN SANTAMARIA Luis Edgardo.

I.2. Cargo e institución donde labora: Coronel PNP - Jefe de la División de Investigación de Delitos de Alta Tecnología.

I.3. Nombre del instrumento motivo de evaluación: Guía de Entrevista

I.4. Autor/a (as) de Instrumento: Arellano Casimiro, Gisela Lisset y Galindo Martinez, Sofia Emilia

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.													X
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.													X
3. ACTUALIDAD	Este adecuado a los objetivos y las necesidades reales de la investigación.													X
4. ORGANIZACIÓN	Existe una organización lógica.													X
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.													X
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos													X
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.													X
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.													X

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación — **SI**
- El Instrumento no cumple con Los requisitos para su aplicación — **SI**

IV. PROMEDIO DE VALORACIÓN: 99

Lima, 01 de abril del 2022.

POLICIA NACIONAL DEL PERU - DIVINDAT - División Delitos Alta Tecnología

OA-228633
Luis Edgardo HUAMAN SANTAMARIA
CORONEL PNP
JEFE DE LA DIVISIÓN DE INVESTIGACIÓN DE DELITOS DE ALTA TECNOLOGIA - DIRINCRI PNP

DNI No: 22517797

ANEXO N° 08: FICHA DE VALIDACIÓN EFECTUADA POR LA ESPECIALISTA JUDICIAL DE JUZGADO DE LIMA NORTE JOSELYN GABRIELA PADILLA ROMERO.

UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

I.1. Apellidos y Nombres: Joselyn Gabriela Padilla Romero.
I.2. Cargo e institución donde labora: Especialista Judicial de Juzgado en el Segundo Juzgado de Investigación Preparatoria Transitorio de Carabayllo.
I.3. Nombre del instrumento motivo de evaluación: Guía de Entrevista.
I.4. Autor/a (as) de Instrumento: Arellano Casimiro, Gisela Lisset y Galindo Martínez, Sofia Emilia.

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.												X	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Este adecuado a los objetivos y las necesidades reales de la investigación.												X	
4. ORGANIZACIÓN	Existe una organización lógica.												X	
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.												X	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												X	
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.												X	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												X	

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación — **SI**
- El Instrumento no cumple con Los requisitos para su aplicación — **SI**

IV. PROMEDIO DE VALORACIÓN: 95

Lima, 1 de mayo del 2022.

PODER JUDICIAL DEL PERÚ
JOSELYN GABRIELA PADILLA ROMERO
ESPECIALISTA JUDICIAL DE JUZGADO
MODULO PENAL DE CARABAYLLO - PUNCHAUCA
CORTE SUPERIOR DE JUSTICIA DE LIMA NORTE

FIRMA DEL EXPERTO INFORMANTE
DNI N.°: 47454229

ANEXO N° 09: FICHA DE VALIDACIÓN REALIZADA POR LA MAGISTER Y ABOGADA LITIGANTE DEL ESTUDIO JURIDICO "MILAGROS" - POLA MILAGROS BENITES HUERTA

UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

I. **DATOS GENERALES**

I.1. Apellidos y Nombres: Benites Huerta Pola Milagros
I.2. Cargo e institución donde labora: Abogada litigante - Estudio Jurídico Milagros
I.3. Nombre del instrumento motivo de evaluación: Guía de Entrevista
I.4. Autor/a (as) de Instrumento: Arellano Casimiro, Gisela Lisset y Galindo Martinez, Sofia Emilia

II. **ASPECTOS DE VALIDACIÓN**

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.												X	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Este adecuado a los objetivos y las necesidades reales de la investigación.												X	
4. ORGANIZACIÓN	Existe una organización lógica.												X	
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.												X	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												X	
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.												X	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												X	

III. **OPINIÓN DE APLICABILIDAD**

- El Instrumento cumple con los Requisitos para su aplicación — X
- El Instrumento no cumple con Los requisitos para su aplicación

IV. **PROMEDIO DE VALORACIÓN:** 95

Lima,01 de abril del 2022.

FIRMA DEL EXPERTO INFORMANTE
DNI No: 40334574
Pola M. Benites Huerta
ABOGADA
CAL. N° 36671

ANEXO N° 10: FICHA DE VALIDACIÓN REALIZADA POR EL MAGISTER Y ABOGADO LITIGANTE INDEPENDIENTE MICKAEL ANDRÉS ESCUDERO VILLACORTA

UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

I. **DATOS GENERALES**

I.1. Apellidos y Nombres: Mickael Andrés Escudero Villacorta
I.2. Cargo e institución donde labora: Abogado litigante independiente
I.3. Nombre del Instrumento motivo de evaluación: Guía de Entrevista
I.4. Autor/a (as) de Instrumento: Arellano Casimiro, Gisela Lisset y Galindo Martinez, Sofia Emilia

II. **ASPECTOS DE VALIDACIÓN**

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.												X	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Este adecuado a los objetivos y las necesidades reales de la investigación.												X	
4. ORGANIZACIÓN	Existe una organización lógica.												X	
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.												X	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												X	
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.												X	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												X	

III. **OPINIÓN DE APLICABILIDAD**

- El Instrumento cumple con los Requisitos para su aplicación — X
- El Instrumento no cumple con Los requisitos para su aplicación

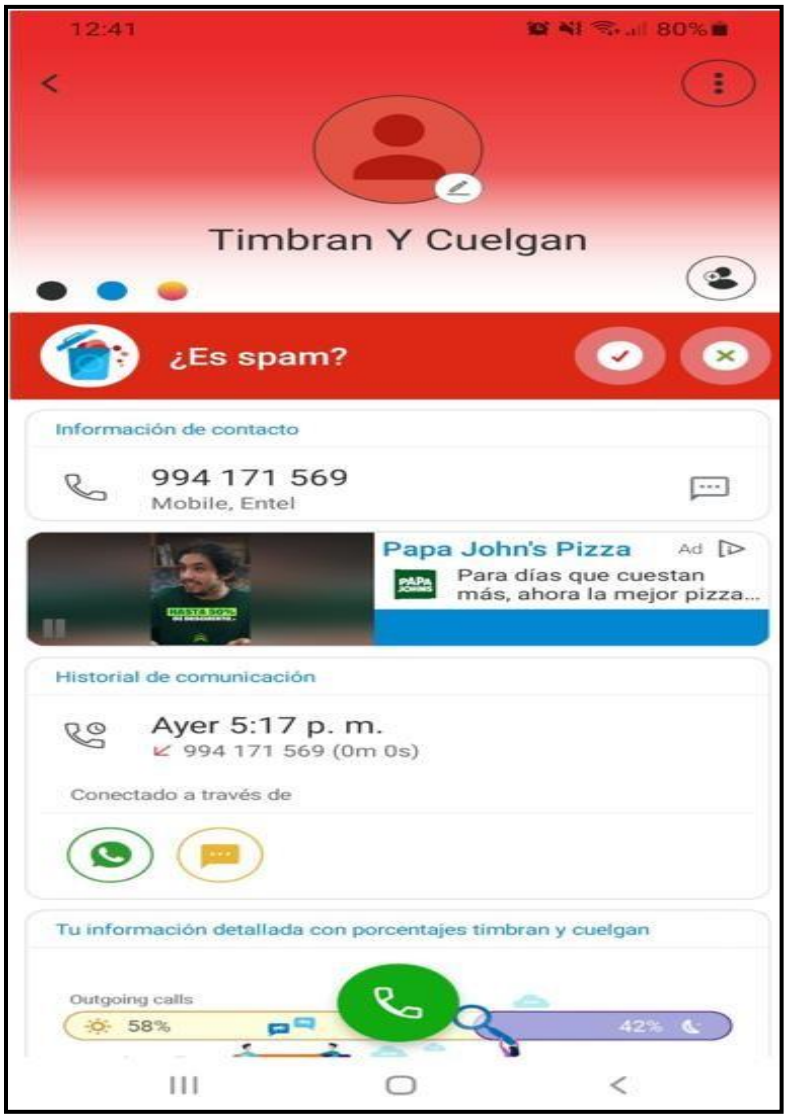
IV. **PROMEDIO DE VALORACIÓN:** 95

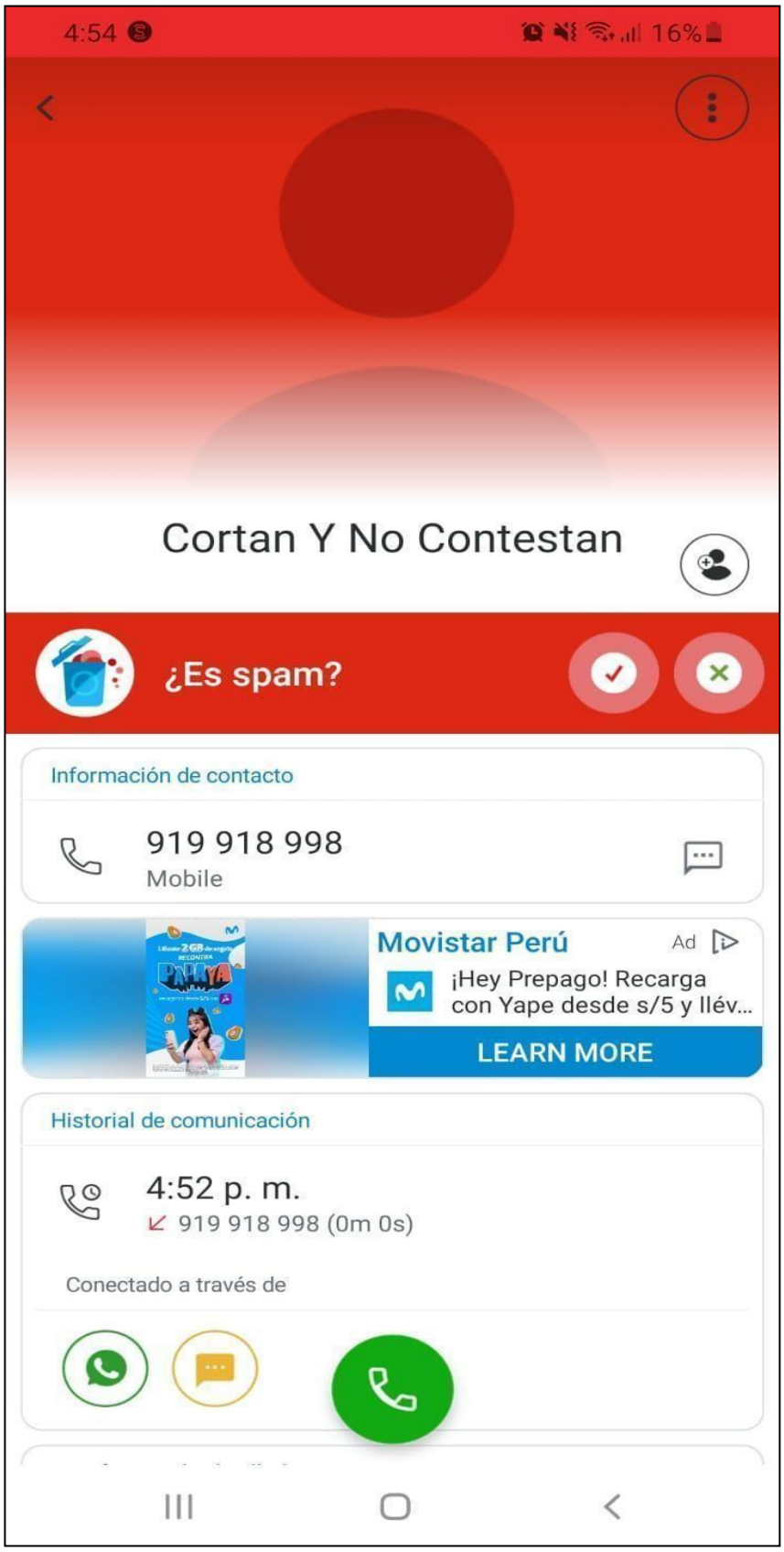
Lima, 01 de abril del 2022

MG. MICKAEL ANDRÉS ESCUDERO VILLACORTA
ABOGADO
CAL 57057

FIRMA DEL EXPERTO INFORMANTE
DNI No: 42953036
Reg. CAL N° 57057

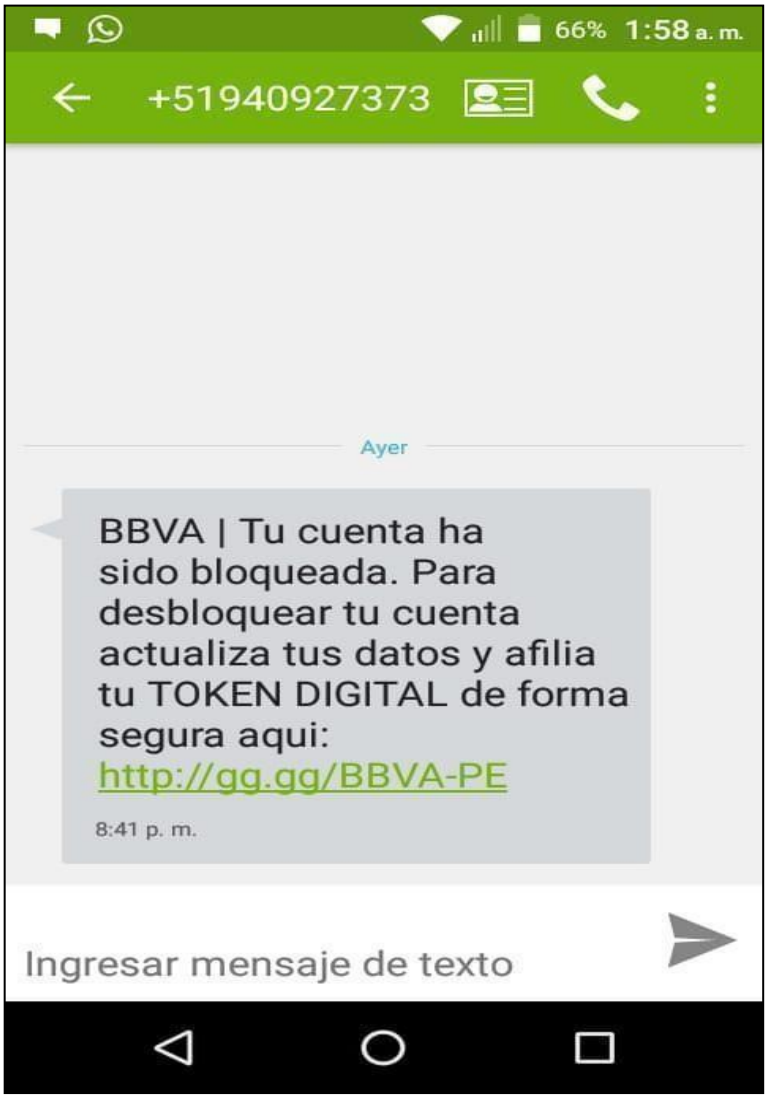
ANEXO N° 11: IMAGENES DE LLAMADAS A CELULAR DE NÚMEROS DESCONOCIDOS IDENTIFICADOS POR EL APLICATIVO GRATUITO *TRUECALLER* COMO "TIMBRA Y CUELGA" AL CONTESTAR LA LLAMADA SE ESCUCHA UN SILENCIO DE UNOS MINUTOS Y POSTERIORMENTE SE CUELGA, EN ESOS MINUTOS QUIEN LLAMA HA INTERCEPTADO LA LÍNEA Y EL MISMO CELULAR PUDIENDO TENER ACCESO A LA INFORMACIÓN QUE CONTIENE, ESTE HECHO SE CONFIGURA EN EL DELITO INFORMÁTICO DE FRAUDE INFORMÁTICO EN LA MODALIDAD DE INTERFERENCIA O MANIPULACIÓN EN EL FUNCIONAMIENTO DE UN SISTEMA INFORMÁTICO - LLAMADA PERDIDA.




4:54
16%
Cortan Y No Contestan
¿Es spam?
Información de contacto
919 918 998
Mobile
Movistar Perú
Ad
¡Hey Prepago! Recarga con Yape desde s/5 y llév...
LEARN MORE
Historial de comunicación
4:52 p. m.
919 918 998 (0m 0s)
Conectado a través de

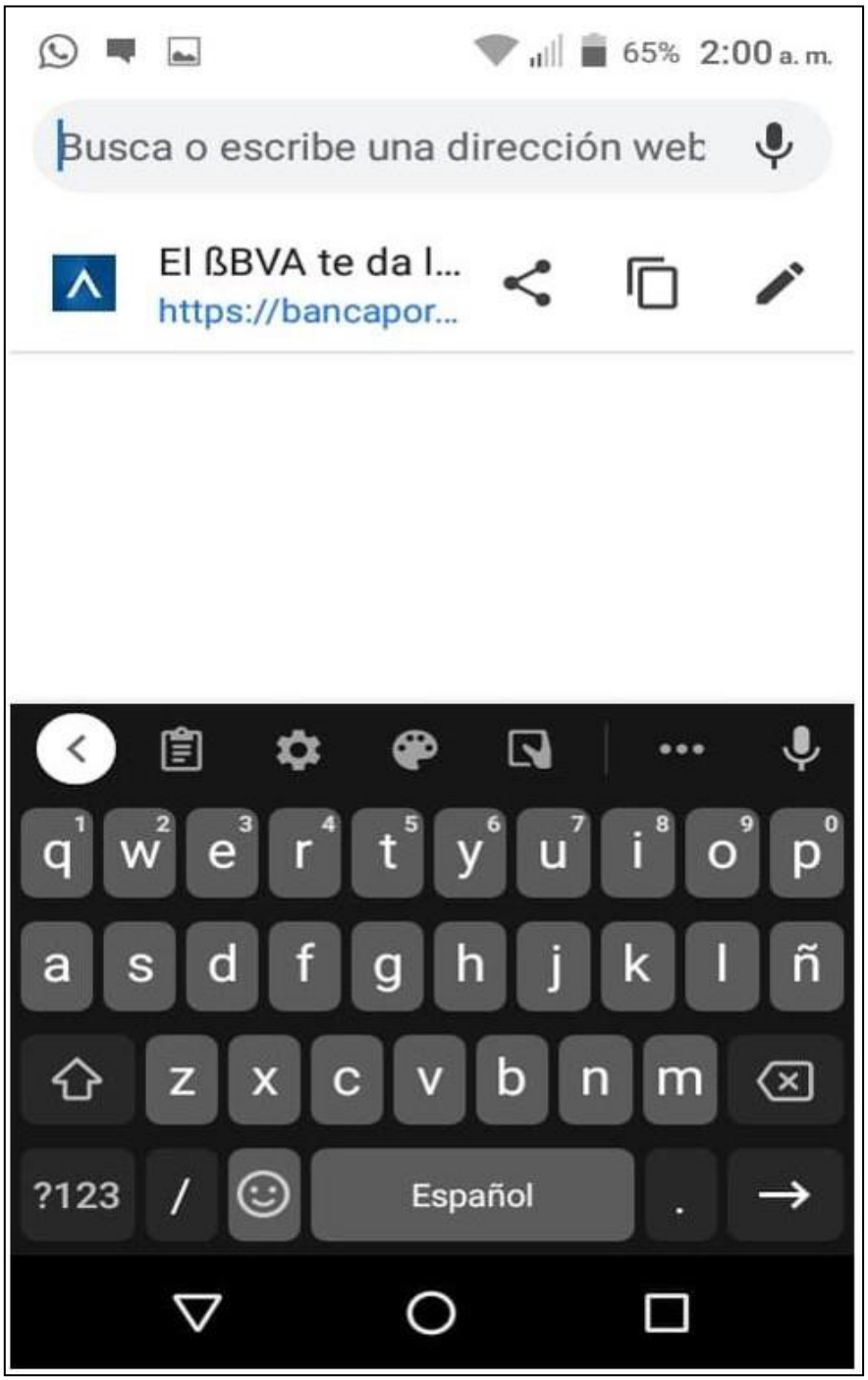
ANEXO N° 12: CASO BBVA: GISELA ARELLANO CASIMIRO (UNA DE LAS AUTORAS DE LA PRESENTE INVESTIGACIÓN) FUE VÍCTIMA DEL "DELITO INFORMÁTICO CONTRA EL PATRIMONIO - FRAUDE INFORMÁTICO - EN LA MODALIDAD DE INTERFERENCIA O MANIPULACIÓN EN EL FUNCIONAMIENTO DE UN SISTEMA INFORMÁTICO - PHISHING, A QUIEN NUNCA SE LE DEVOLVIÓ SU DINERO (MONTO S/.1000.00 SOLES).

HECHO 1: Remitieron un SMS (Mensaje de texto) como se observa de la captura a las 00:50 horas del día 15 de junio del 2020, sin conocimiento de la nueva modalidad de delito, se ingresó al link para verificar la causa del "BLOQUEO DE CUENTA", llevando a una "PÁGINA FALSA DEL BANCO CONTINENTAL".

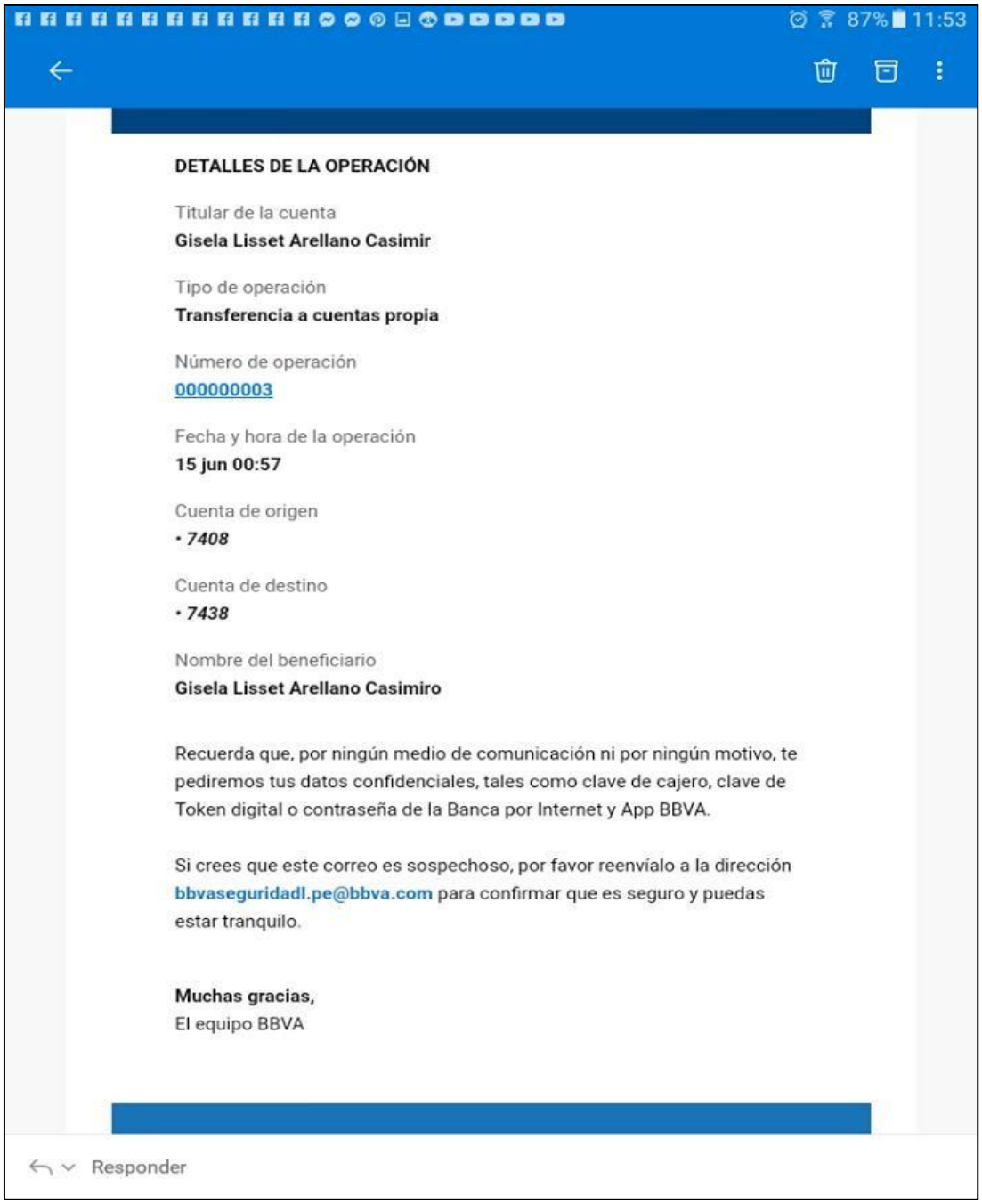


HECHO 2: La "PÁGINA FALSA" tenía todas las características de la página real del Banco, más el "Candado de seguridad" no se verificaba en la parte superior izquierda al lado del link, como se puede observar en la imagen. Se entró al link y se brindó el dato que se solicitaba (DNI y Clave de La Banca por internet).

HECHO 3: Posterior a brindar los datos solicitados, llego un SMS (Mensaje de texto 2), como se observa de la imagen, donde brindó un código para el "DESBLOQUEO DE LA CUENTA", se realizó el llenado con el código, pero no salía mensaje de confirmación por lo que se dejó la banca para apersonarse al día siguiente al Banco a solicitar información del supuesto "BLOQUEO DE CUENTA".



HECHO 4: Minutos después, llego un correo electrónico al Gmail asociado a la Banca por internet del usuario agraviado indicando que se había realizado una transferencia exitosa, a ello la usuario reporto lo sucedido y procedió a ingresar a su Banca por Internet a fin de verificar dicha transferencia y resulto que se había transferido el monto de S/.999.00 Soles a una cuenta desconocida, situación que también se reportó a la institución crediticia.



87% 11:53

DETALLES DE LA OPERACIÓN

Titular de la cuenta
Gisela Lisset Arellano Casimir

Tipo de operación
Transferencia a cuentas propia

Número de operación
000000003

Fecha y hora de la operación
15 jun 00:57

Cuenta de origen
• 7408

Cuenta de destino
• 7438

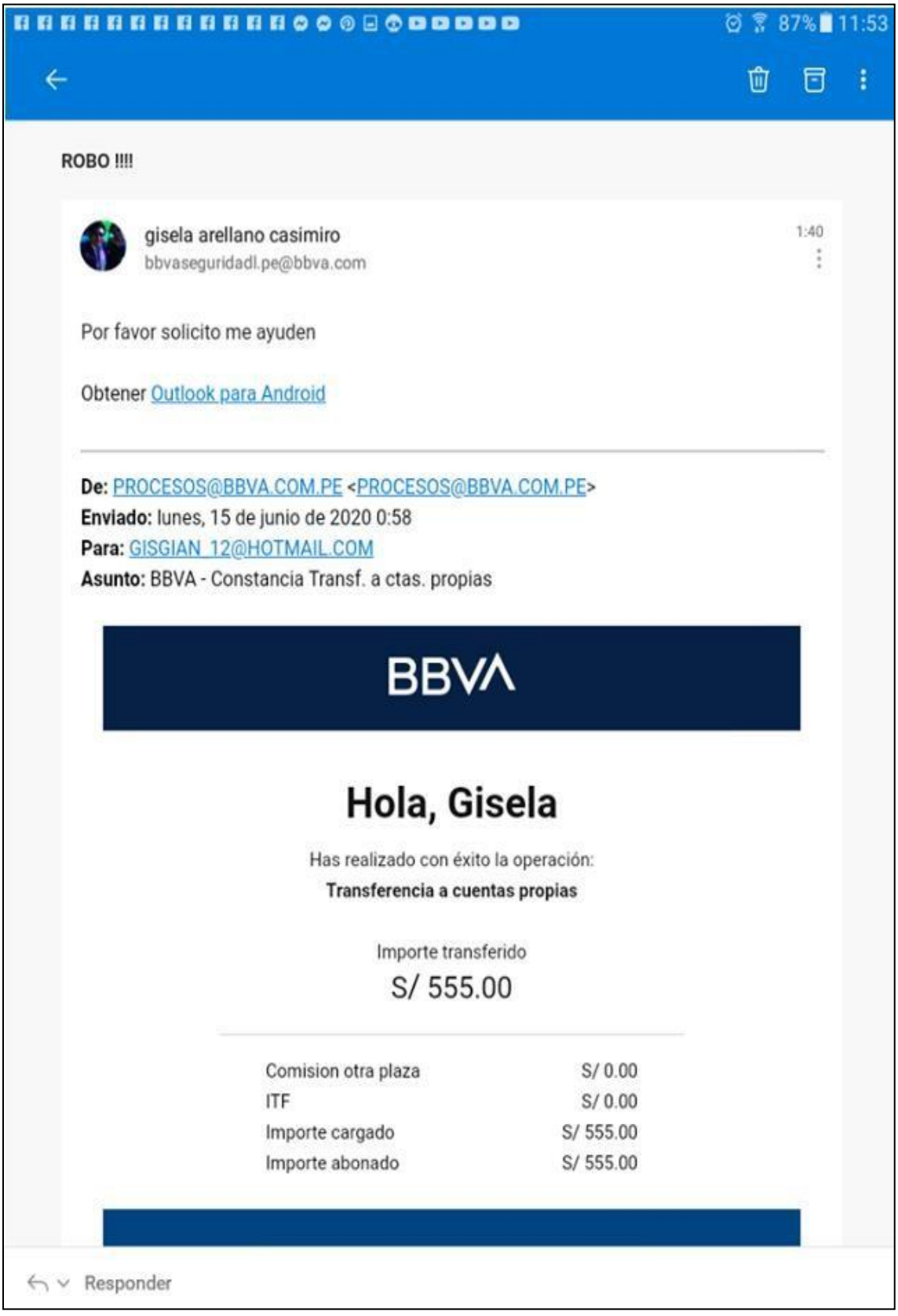
Nombre del beneficiario
Gisela Lisset Arellano Casimiro

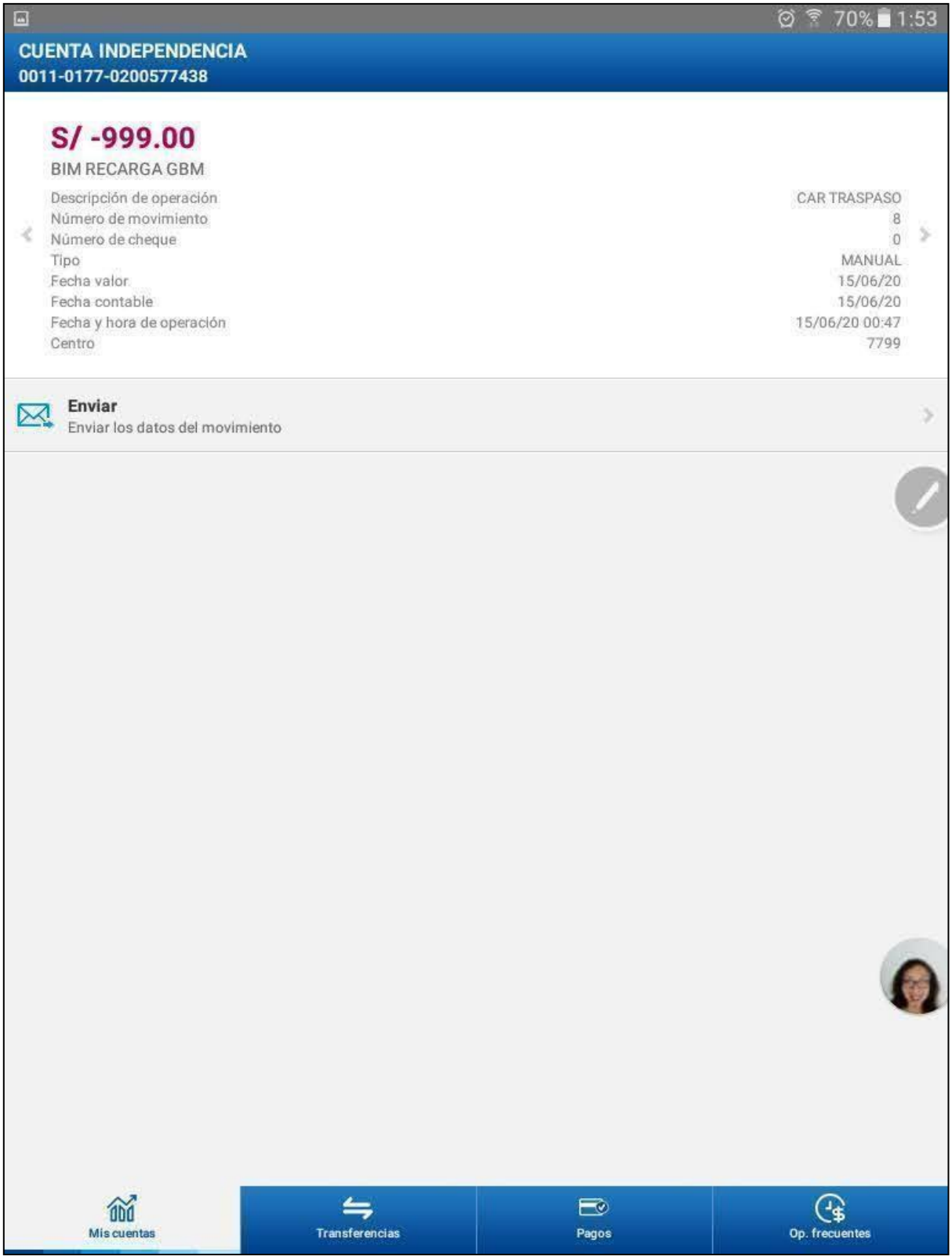
Recuerda que, por ningún medio de comunicación ni por ningún motivo, te pediremos tus datos confidenciales, tales como clave de cajero, clave de Token digital o contraseña de la Banca por Internet y App BBVA.

Si crees que este correo es sospechoso, por favor reenvíalo a la dirección **bbvaseguridadl.pe@bbva.com** para confirmar que es seguro y puedas estar tranquilo.

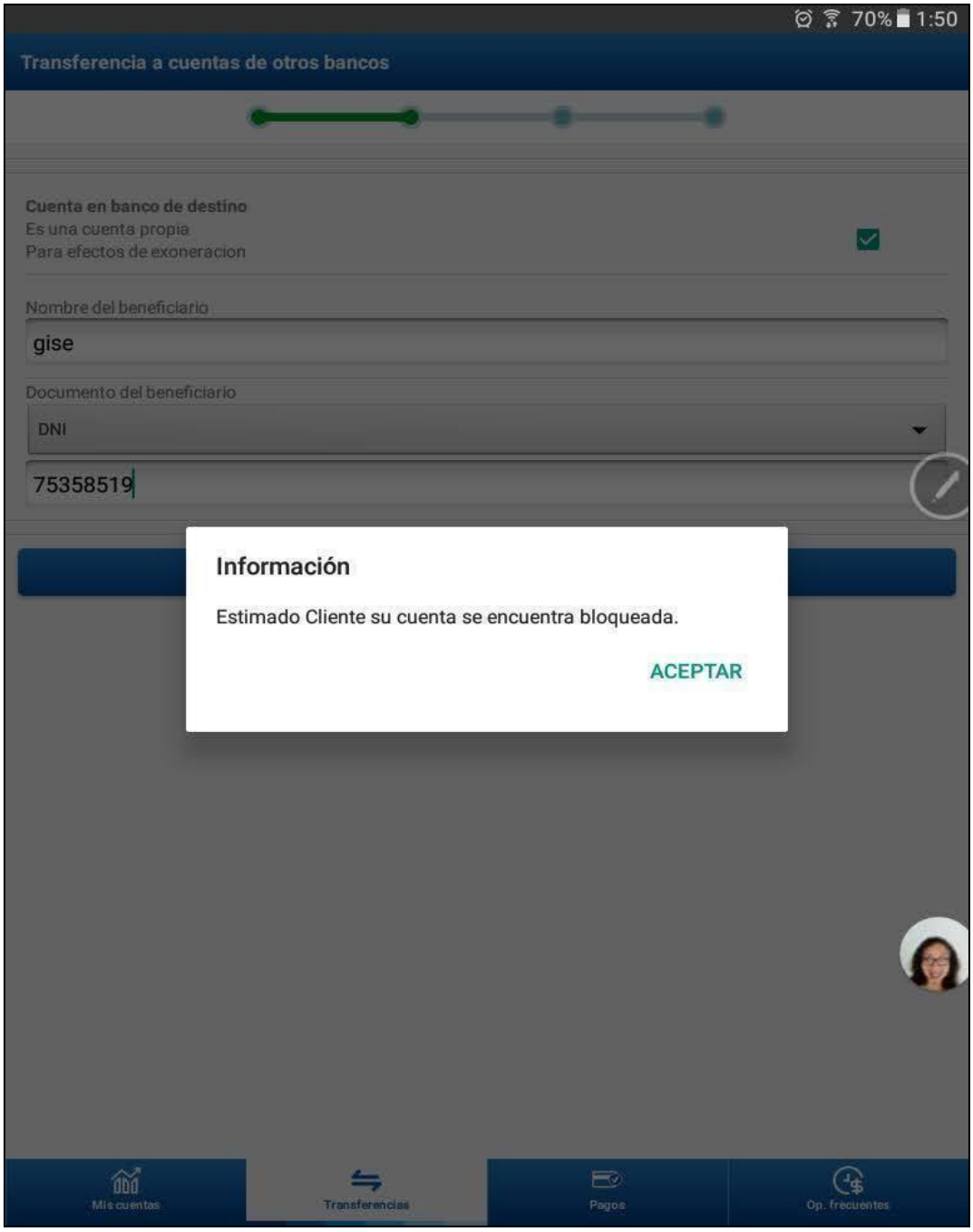
Muchas gracias,
El equipo BBVA

Responder

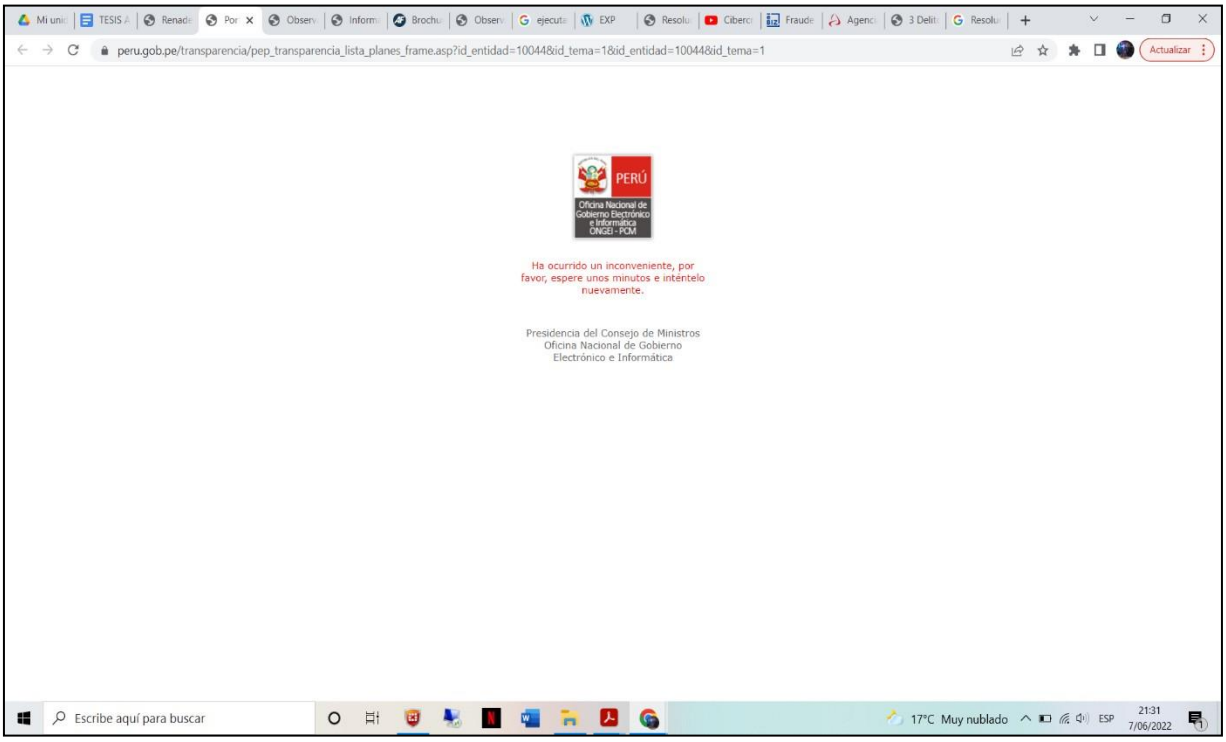

87% 11:53
ROBO !!!!
gisela arellano casimiro
bbvaseguridadl.pe@bbva.com
1:40
Por favor solicito me ayuden
Obtener Outlook para Android
De: PROCESOS@BBVA.COM.PE <PROCESOS@BBVA.COM.PE>
Enviado: lunes, 15 de junio de 2020 0:58
Para: GISGIAN_12@HOTMAIL.COM
Asunto: BBVA - Constancia Transf. a ctas. propias
BBVA
Hola, Gisela
Has realizado con éxito la operación:
Transferencia a cuentas propias
Importe transferido
S/ 555.00
Comision otra plaza S/ 0.00
ITF S/ 0.00
Importe cargado S/ 555.00
Importe abonado S/ 555.00
Responder


70% 1:53
CUENTA INDEPENDENCIA
0011-0177-0200577438
S/ -999.00
BIM RECARGA GBM
Descripción de operación CAR TRASPASO
Número de movimiento 8
Número de cheque 0
Tipo MANUAL
Fecha valor 15/06/20
Fecha contable 15/06/20
Fecha y hora de operación 15/06/20 00:47
Centro 7799
Enviar
Enviar los datos del movimiento
Mis cuentas
Transferencias
Pagos
Op. frecuentes

HECHO 5: Ante tal situación se procedió a bloquear la cuenta, y realizar la queja en el Libro de reclamaciones de la entidad, así como de forma presencial, a ello, el Banco Continental no dio solución y se dio por perdido el monto, ***se puede advertir ante tal hecho el total desdén, desinterés, despreocupación, indiferencia y apatía de las instituciones crediticias ante hechos delictivos que afecta a sus propios usuarios*****.**



ANEXO 13: Se advierte la caída de la página web del Portal del Ministerio Público, pestaña Portal de Transparencia, se anexa hipervínculo (Recuperado con fecha 07.06.2022 a horas 21:30 p.m.): https://www.peru.gob.pe/transparencia/pep_transparencia_lista_planes_frame.asp?id_entidad=10044&id_tema=1&id_entidad=10044&id_tema=1



ANEXO 14: Captura de pantalla del inicio del aplicativo Yape (billetera digital), advirtiendo a los usuarios tener precaución con el delito de fraude informático, delito que atañe a todos los estratos de la población.

ANEXO 15: Fotografía tomada a las investigadoras en las inmediaciones de la División de Investigación de Delitos de Alta Tecnología - DIVINDAT, ubicado en la Av. España 323 piso 09 - Distrito de Cercado de Lima.

INVESTIGADORA - AUTORA SOFIA EMILIA GALINDO MARTINEZ

INVESTIGADORA - AUTORA GISELA LISSET ARELLANO CASIMIRO

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Autenticidad del Asesor

Yo, VASQUEZ TORRES ARTURO RAFAEL, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Deficiencias Legislativas en el tratamiento de la Ley N° 30096, Ley de Delitos Informáticos - Fraude Informático, Lima 2019 – 2021", cuyos autores son GALINDO MARTINEZ SOFIA EMILIA, ARELLANO CASIMIRO GISELA LISSET, constato que la investigación cumple con el índice de similitud establecido, y 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, 08 de Julio del 2022

Apellidos y Nombres del Asesor:	**Firma**
VASQUEZ TORRES ARTURO RAFAEL **DNI:** 41627787 **ORCID** 0000-0002-8513-4483	Firmado digitalmente por: AVASQUEZTOR el 08-07-2022 19:17:30

Código documento Trilce: TRI - 0328365

INVESTIGA UCV