UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Fraude informático en los sistemas de seguridad financiero, distrito fiscal de Lima Centro 2022

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Derecho Penal y Procesal Penal

AUTORA:

Rosas Marroqui, Brenda Lisset (orcid.org/0000-0002-1404-5934)

ASESOR:

Dr. Rodriguez Figueroa, Jose Jorge (orcid.org/0000-0002-0265-9226)

Mg. Nieto Fernandez, Gaby Jessica (orcid.org/0000-0003-0303-9915)

LÍNEA DE INVESTIGACIÓN:

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

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía

LIMA – PERÚ

2023

Dedicatoria

El presente trabajo está dedicado a Dios que siempre me ha concedido la gracia de cuidarme y protegerme, a mi querida madre María Margarita Marroqui Peña quien me enseñó a ser fuerte y afrontar los retos que cada día aparecen en nuestro camino y finalmente a mi esposo e hijos por la paciencia y comprensión en este largo camino de estudios.

Agradecimiento

A mi Asesora que con su paciencia y dedicación mi inspiro a seguir adelante y no rendirme y a mi hermana Vanessa Karina Rosas Marroqui por su apoyo incondicional en el desarrollo de la presente tesis.

Índice de contenidos

Resumen

En la presente investigación tiene como objetivo general analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias del distrito fiscal de Lima Centro 2022, ello en virtud a que no se ha desarrollado una cultura de prevención y uso responsable de las redes de internet a fin de evitar vulneraciones en los sistemas informáticos que contiene información reservada. La metodología que se ha utilizado en la investigación es de tipo básica aplicada, con enfoque cualitativo y diseño de la teoría fundamentada, se ha aplicado como técnica la entrevista a 10 participantes (fiscales, jueces y abogados) con la finalidad de recoger información de expertos y de lo cual se obtuvo respuestas al problema planteado. Finalmente, lo que se ha buscado es analizar si era posible establecer responsabilidad penal a las instituciones bancarias en el delito de fraude informático por la falta de implementación de sistemas de seguridad adecuados.

Palabras clave: Fraude informático, sistemas de seguridad, responsabilidad penal.

Abstract

In the present investigation, the general objective is to analyze how the treatment of the crime of computer fraud affects the financial security systems that increase the complaints of the fiscal district of Lima Centro 2022, this by virtue of the fact that a culture of prevention and responsible use of Internet networks has not been developed in order to avoid violations in computer systems that contain reserved information. The methodology that has been used in the investigation is of a basic applied type, with a qualitative approach and design of the grounded theory, the interview with 10 participants (prosecutors, judges and lawyers) has been applied as a technique in order to collect information from experts and from which responses to the problem posed were obtained. Finally, what has been sought is to analyze whether it was possible to establish criminal liability of banking institutions in the crime of computer fraud due to the lack of implementation of adequate security systems.

Keywords: Computer fraud, security systems, criminal liability.

I. INTRODUCCIÓN

Rodríguez (2018) señala que el internet es un medio que se utiliza para el intercambio libre de comunicación, consulta, obtención de información entre usuarios, por medio del internet se pueden realizar transacciones financieras, trámites y comunicación interpersonal por vía electrónica como envíos de mensajes, programas ejecutables, servicios de noticias, acceso remoto, transferencia de ficheros y otros; Gioia (2019) indica, que el avance de la tecnología ha evolucionado significativamente, permitiendo que a través de ella se pueda compilar, almacenar y recuperar grandes cantidades de información en la base de datos; Cisneros (2022) citando a Mesa señala que las circunstancias que dan lugar al crecimiento de los delitos informáticos por la falta de mecanismos adecuados de detección y prevención de riesgos.

A nivel Internacional

Los países de Chile y México fueron blancos de ciberataques de gran magnitud, pudiéndose así advertirse los niveles de vulnerabilidad de las entidades del sistema financiero, debido a la ausencia de leyes y una adecuada protección, por lo tanto es necesario garantizar que se desarrollen políticas y medidas de protección. (Mansilla, 2020)

Estados Unidos se tiene el Acta Federal de Abuso computacional que modifica el acta de fraude y de Abuso computacional, en Alemania se dictó la segunda ley para la lucha contra la ciber criminalidad económica y España en el artículo 264-2 del Código Penal español, es decir en diversos países se han dictado normas que regulan y tipifican las conductas realizadas por medios informáticos. (Vences, 2019, p.87 y 89)

En ese sentido si bien existen países en los cuáles se ha regulado en materia penal, sin embargo con el avance de la tecnología existen diversidad de conductas delictivas que han causado un daño importante a nivel internacional, con lo que se demuestra que se existen brechas de necesidades por cubrir en materia cibernética, asimismo aún hay países donde no se ha regulado los delitos informáticos lo cual es

necesario que lo realicen a fin de proteger los bienes de los usuarios que utilizan la tecnología. (Vences, 2019, p.132)

El crecimiento a nivel mundial del comercio electrónico vía Internet, en los servicios de base de datos en la nube, la necesidad de proteger las redes ha aumentado y el acceso remoto a la información, lo que hace que la seguridad funcione en bases de datos cada vez más exigentes y especializadas (Gioia, C. 2019)

Mayer, L. y Oliver, G. (2020) señalan que el fraude informático y la estafa están vinculadas, un ejemplo de ello es que en la normativa alemana y española la regulan de forma conjunta, debido a que ambos afectan bienes patrimoniales, pero por distintos medios (p.154)

En los países de América Latina, el problema se presentó a nivel cultural, tecnológico, político, comercial, educativo, económico y social, a lo que sin duda ayudó la tecnología de información, internet, los sistemas informáticos, las redes sociales, los servicios y plataformas virtuales en celulares y computadoras (Ayma, 2020, p.17)

A nivel Nacional

El fraude informático se encuentra previsto en el artículo 8 de la Ley N° 30096 modificada por el artículo 1 de la Ley N° 30171, ello a fin de proteger los derechos patrimoniales de las personas.

Que, estas actividades ilícitas se presentan debido a que el Estado a través de la Ley N° 26702 y lo señalado en el artículo 3 de la Circular N° G-140-2009 Gestión de la seguridad de la información se establece criterios mínimos de la seguridad de la información, las empresas privadas y entidades financieras vienen promoviendo la realización de transacciones financieras a través de plataformas informáticas a fin de agilizar su trámite.

Condori, R. (2020) señala que, a pesar de los esfuerzos de la empresa privada el uso de la tecnología ha tenido efectos negativos, puesto que algunos ciudadanos haciendo uso de sus conocimientos tecnológicos lo han utilizado para crear una nueva forma de delinquir a través de las redes informáticas, como el fraude informático de

transacciones ilegales en beneficio de los ciberdelincuentes dando como resultado la afectación de los derechos patrimoniales de las personas, ello por falta de conocimiento en la utilización de los aplicativos informáticos. p.9)

En el Perú las instituciones públicas y privadas son las que se encuentran constantemente expuestas a amenazas de seguridad de sus datos, toda vez que, si sus datos u operaciones son manipulados por terceras personas o a través de los diversos servicios de aplicativos informáticos que las hace asequibles e implica un grave riesgo para la organización.

Según el reporte estadístico sobre ciberdelitos publicado por el Observatorio Nacional de Política Criminal del Ministerio de Justicia y Derechos Humanos lo datos de ingreso de denuncia por delito de fraude informático fueron los siguientes: 5878 en el año 2019, 6946 en el año 2020 y 10,924 en el año 2021, acotándose que 3 de cada 4 ciberdelitos en el Perú están relacionados a la comisión del delito antes mencionado.

Otro factor que incide en el crecimiento de los delitos cibernéticos es también el analfabetismo digital que está relacionado con el alto nivel desconocimiento de las nuevas tecnologías, su insuficiencia e ingenuidad generan una situación favorable para la intervención de la ciberdelincuencia con una alta probabilidad de éxito. (Picoy 2020)

Ahora bien, Carrera (2021) citando a Zevallos y Solís, menciona que los delitos de fraude informáticos han aumentado con la emergencia sanitaria por el Covid-19, que ha generado que las conductas delictivas de tipo cibernético se hayan visto incrementadas exponencialmente, dando lugar a que las autoridades responsables el Ministerio Público y la Unidad policial especializada presenten un aumento desbordado de casos de ciberdelitos, que comprometen bienes jurídicos tutelados por la legislación, y lo cual impone un reto a las autoridades de lucha contra este flagelo, a fin de identificar y judicializar a los responsables. Asimismo, Gioia, C. (2019) indica que a lo largo de la historia todo avance de la tecnología puede ser utilizado en beneficio de la sociedad o para realizar actividades ilícitas. (p.3)

Mansilla (2020) señala que en el Perú los ciberataques en el sector financiero y bancario han crecido exponencialmente y que el nivel de incidencia alcanza a un 28.63%.

Las organizaciones son las que tienen mayores problemas de seguridad en sus bases de datos, lo cual da lugar al crecimiento del ciberdelito porque el delincuente depende de esta falla para cometer el delito, por ello es importante cumplir con las normas y parámetros legales a fin de evitar la desprotección de aquellos que están frente a esta situación. (Acosta et al. 2020)

Sin embargo, a pesar de la existencia de la Ley N° 30076 que sanciona la conducta ilícita del fraude informático, no se ha llegado a desarrollar una cultura de prevención y uso responsable de la tecnología con la finalidad de proteger al usuario tecnológico y así de esta manera evitar las vulneraciones y/o afectaciones a los sistemas informáticos que contienen información reservada, a fin de lograr disminuir la cantidad de denuncias por dicho delito, sino muy por el contrario se aprecia un aumento debido a esta nueva forma de delinquir aprovechándose las redes de internet y el desconocimiento del uso de programas de seguridad de parte de los usuarios.

A nivel Local

En el Ministerio Público, se ha podido advertir en el contexto de las investigaciones un elevado incremento de los delitos informáticos especialmente en el Fraude Informático (Vázquez, 2022 citando a El Peruano 2021), debido a que los delincuentes fácilmente vulneran los sistemas de seguridad financieros implementados, logrando así causar un perjuicio patrimonial a los usuarios, sin embargo en las investigaciones no se ha logrado establecer el grado de responsabilidad de las instituciones financieras que brindan el servicio y demás participantes, ello teniendo en cuenta que a través de los diversos sistemas jurídicos se busca dar seguridad a las personas garantizándoles el ejercicio de los derechos y el cumplimiento de las obligaciones estipuladas en el derecho sustantivo y adjetivo que le permite hacer valer sus derechos. (Ayma, 2020, p.20)

Según Creswell (2014) citado por Arias et. al., (2022) señalan que el problema general es un enunciado enmarcado en modo de pregunta que permite al investigador identificar que debe hacer para responderla. Es decir, el problema general se puede encontrar como otro título, pero aún se limita al enunciado del problema. (p.13)

Bernal (2010) señala que en la pregunta general se debe tener en cuenta la naturaleza del problema y el título de la investigación y las preguntas específicas son sobre ciertos aspectos del problema general.

Ahora bien, de lo precedentemente expuesto en el presente estudio se formuló como problema general: ¿De qué manera el tratamiento del delito de Fraude Informático repercute en los sistemas de seguridad financiero que incrementa las denuncias del distrito fiscal Lima Centro 2022? y los problemas específicos: ¿De qué manera el robo de datos informáticos disminuye con la utilización adecuada de la información de la base de datos de las entidades financieras del distrito fiscal Lima Centro 2022? y ¿Cómo la alteración de sistemas o software implican responsabilidad de la entidad financiera debido a la falta de respeto de los accesos de la información establecidos del distrito fiscal Lima Centro 2022?

1.1 Justificación de la Investigación

Hernández y Mendoza (2018) señala que es necesario justificar la investigación realizada en base a los objetivos y preguntas de investigación, lo que significa exponer las razones por las cuales es importante o necesario realizar el estudio (el para qué del estudio). (p. 44-45)

1.1.1 Justificación Teórica

Bernal (2010) señala que hay justificación teórica cuando el objetivo es generar reflexión y discusión sobre los conocimientos que existen.

Se justifica teóricamente porque era necesario propiciar la reflexión y debate a través de la recopilación, estudio y análisis de información de la diversas fuentes e instrumentos normativos, respecto si el delito de Fraude Informático regula responsabilidad compartida entre el intruso (investigado) y la institución financiera,

respecto a las transacciones financieras con sistema de seguridad financiero realizadas mediante dispositivos electrónicos en el distrito fiscal de Lima Centro, lo cual será de gran importancia para el correcto análisis de la calificación de la imputación por parte del operador de justicia penal en este tipo de delitos.

1.1.2 Justificación Practica

Bernal (2010) señala que se considera así, si su tratamiento ayuda a resolver un problema o sugiere estrategias que contribuyen a resolverlo.

La investigación se justifica prácticamente porque a través del estudio se buscó aportar información respecto del alcance de la responsabilidad penal por delito de Fraude Informático a la entidad financiera, ello en virtud a que deben garantizar la seguridad de la información de la base de datos de los usuarios a través de sistemas de seguridad que controlen la confidencialidad, integridad y disponibilidad, conforme lo establece las normas nacionales e internacionales y lo cual va a dar lugar a que las instituciones financieras implementen una gestión de riesgos y prevención de fraudes adecuada que va a permitir disminuir la incidencia delictiva en este tipo de delitos.

1.1.3 Justificación Metodológica

Bernal (2010) señala que ésta surge cuando la investigación propone un nuevo método o una estrategia para obtener información valida y fiable.

La justificación metodológica se basó en la recopilación de información con enfoque cualitativo, lo cual permitió que a través del análisis de la información de fuentes doctrinarias y legales se genere el debido conocimiento respecto a la responsabilidad de la entidad financiera ante la comisión de un delito de fraude informático, lo cual será de gran utilidad e impacto en mejorar la norma penal.

1.1.4 Justificación Legal porque no existe una interpretación adecuada de la norma que indique si a la entidad financiera le alcanza responsabilidad penal en el delito de fraude informático por la administración de la base de datos de los usuarios con sistemas de seguridad y prevención de fraudes.

1.2 Objetivos de la Investigación

Los objetivos de investigación definen lo que se quiere lograr, porque todo comienza con un problema y es algo que debe ser abordado, el objetivo actúa para solucionar el problema, los objetivos tienen como tarea investigar el problema, pero no de resolverlos. (Ocegueda, 2004 citado por Arias et. al, 2022, p.32)

1.2.1 Objetivo general

Bernal (2010) señala que refleja la naturaleza del problema y el título de la investigación.

- Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022

1.2.2 Objetivos específicos

Bernal (2010) señala que se deriva del objetivo general y se plantean hacia el logro de una parte de dicho objetivo.

- Evaluar si el delito de fraude informática regula responsabilidad penal de la entidad financiera en relación a los sistemas de seguridad financiero del distrito fiscal Lima Centro 2022
- Identificar los riesgos de los sistemas de seguridad financiero que incrementan las denuncias en el distrito fiscal Lima Centro 2022

1.3 Supuestos Jurídicos

Hernández y Mendoza (2018) señalan que los supuestos jurídicos son explicaciones tentativas del problema planteado que vienen hacer la guía del estudio. Son las contestaciones provisionales de las preguntas de la investigación que pueden ser confirmadas o no.

1.3.1 Supuesto Jurídico General

El fraude informático en los sistemas de seguridad financiero incrementa denuncias, del distrito fiscal de Lima Centro 2022.

1.3.2 Supuesto Jurídico Específico

Le alcanza responsabilidad penal a la entidad financiera por delito de fraude informático del distrito fiscal de Lima Centro 2022.

II. MARCO TEÓRICO

Estado de la Cuestión

2.1 Delito Informático – Fraude Informático

A nivel nacional

Condori (2020), plantea como **problema** que el delito de fraude informático no tipifica en todos sus ámbitos la forma en que se comete este delito, pues existe un vacío normativo respecto a los delitos cometidos fuera del país a través de aparatos electrónicos, señalando como **objetivo** el poder determinar las situaciones jurídicas del fraude informático y la protección penal del delito contra el patrimonio y señala como su **metodología** la aplicación de un estudio descriptivo, bajo el diseño socio crítico de la fenomenología y de tipo no experimental y con un enfoque cualitativo; **concluyendo** que el fraude informático repercute negativamente en el patrimonio de los agraviados, ello debido a la falta de una adecuada investigación. Ahora bien, como **análisis** es posible señalar que el estudio realizado es correcto, porque efectivamente se evidenció que no existen lineamentos adecuados para la atención de los casos de delito de fraude informático por el avance de las tecnologías.

Quispe (2020), plantea como **problema** la existencia de una elevada cantidad de denuncias por fraude informático de cuentas bancarias por compras efectuadas por internet, las cuáles han sido archivadas preliminarmente o en la investigación preparatoria, señalando como **objetivo** la necesidad de establecer los elementos que determinan el archivo de los casos por delito de fraude informático y señala como su **metodología** la aplicación de un enfoque cualitativo; **concluyendo** que las empresas financieras y de telefonía no cooperan en las investigaciones, así como tampoco se cuenta con tecnología, infraestructura y personal competente en la policía nacional y el Ministerio Público, de otro lado señala que la falta de identificación del autor del delito se presenta porque no es fácil identificar al operador de la información y que la falta de indicios reveladores se da porque la falta de información de parte de las

entidades financieras y de telefonía, como **análisis** es posible señalar que el estudio realizado ha dado lugar a determinar que las investigaciones son archivadas por la falta de cooperación de las entidades bancarias y de telefonía, así como la falta de individualización se debe a la falta de información adecuada que permita establecer el autor que opera la información.

Carrera (2021) plantea como **problema** que las denuncias por delito informático se ven incrementadas y muchas de las investigaciones han sido archivadas, generando carga procesal e inseguridad en las víctimas, señalando como **objetivo** el poder determinar las carencias en las investigaciones por delitos de fraude informático y señala como su **metodología** la aplicación de un estudio básico, bajo el diseño fenomenológico y con un enfoque cualitativo; **concluyendo** que la falta de capacidad de conocimiento sobre delitos informáticos, capacidad operativa y elevada carga procesal en el Ministerio Público, Policía Nacional y servidores públicos dan lugar a que no se logre identificar al autor del delito, así como también la falta de la aplicación normativa y actualización de la misma genera ineficacia. Ahora bien, como **análisis** es posible señalar que el estudio realizado es correcto ya que el avance de la tecnología crece con pasos agigantados a comparación del avance normativo en nuestro país, lo cual ocasiona la falta de capacitación y correcta investigación en esta clase de delitos.

Cisneros (2022) plantea como **problema** que para identificar al imputado en las diligencias preliminares se requiere conocer algunos datos de la tarjeta de la víctima, señalando como **objetivo** el poder reconocer los motivos que impiden identificar al imputado del delito de fraude informático y señala como su **metodología** la aplicación de un estudio básico, bajo el diseño no experimental y con un enfoque cualitativo; **concluyendo** que la falta de interés del agraviado, apoyo por parte de las entidades financieras dan lugar a la falta de identificación del sujeto activo del delito de fraude informático. Ahora bien, como **análisis** es posible señalar que el estudio realizado es correcto, porque efectivamente se puede advertir que la parte agraviada y las entidades bancarias no brindan la información necesaria para lograr identificar al autor del delito de fraude informático.

Novoa (2022), plantea como **problema** las dificultades para identificar y determinar a los autores del delito, por la falta de cooperación de los operadores de comunicaciones, la policía nacional del Perú, la cooperación internacional, la falta de conocimiento informático de los jueces y fiscales en los casos de vulneración del derecho a la intimidad, señalando como **objetivo** determinar la incidencia delictiva del delito informático en la vulneración del derecho a la intimidad en un juzgado unipersonal, 2022 y señala como su **metodología** la aplicación de un enfoque cuantitativo, un diseño transversal no experimental y correlacional; **concluyendo** que el injusto penal de sistemas y datos informáticos incide en su dimensión de confidencialidad, integridad de manera moderada en la vulneración del derecho a la intimidad, como **análisis** es posible señalar que el estudio realizado no es muy claro cuando indica respecto de la incidencia que genera el delito informático en la vulneración del derecho a la intimidad, pues las conclusiones arribadas no aterrizan señalando de qué manera es que se vulnera el citado derecho fundamental, es muy genérico.

Vargas (2022), en su investigación plantea como **problema** el incremento de ofertas fraudulentas en las redes que no se encuentran tipificadas en la Ley N° 30096 y lo cual dificulta el trabajo de investigación de la policía nacional del Perú y del Ministerio Público, generando inseguridad jurídica, señalando como **objetivo** la necesidad de tipificar la estafa básica en el Código Penal sancionándose con penas más graves a los sujetos que hacen uso del internet para cometer este tipo de delitos y señala como su **metodología** la aplicación de un enfoque cualitativo, con un tipo de investigación aplicada y con diseño de teoría fundamentada; **concluyendo** que debido a la pandemia se ha incrementado los delitos por estafa mediante el uso del internet y las TIC's, por lo que la tipificación del delito de estafa básica en la norma sustantiva permitirá reducir la impunidad en estos delitos, asimismo señala que los problemas que tiene la policía y fiscales es la falta de equipos informáticos y personal competente para poder obtener evidencias digitales, finalmente se indica que es necesario aumentar la pena cuando intervienen pluralidad de agentes en delitos informáticos, como **análisis** es posible señalar que el estudio realizado coincide con otros estudios

en el sentido de la falta de personal e infraestructura, sin embargo no estoy de acuerdo que la elevación de las penas va a reducir el incremento e impunidad de este tipo de delitos.

Vásquez (2022), en su investigación plantea como **problema** que el avance de la tecnología ha dado lugar a nuevas conductas delictivas que deben ser incorporadas en el ordenamiento penal, señalando como **objetivo** el poder determinar la necesidad de incorporar en el ordenamiento sustantivo nuevas formas de conductas delictivas de delitos informáticos a fin de evitar la impunidad y señala como su **metodología** la aplicación de un enfoque cualitativo, tipo de investigación básica, descriptiva; **concluyendo** que existe la necesidad de implementar alternativas de tipificación de conductas delictivas por delito informático que se vienen presentando por el uso del internet, así como las investigaciones son burocráticas y se extienden demasiado generando impunidad, como **análisis** es posible señalar estoy de acuerdo con que se tipifiquen las conductas nuevas que se advierten por el avance de las tecnología.

A nivel internacional

Vences (2019), en su investigación plantea como **problema** que en la actualidad existen una serie de conductas ilícitas que los sistemas informáticos potencializan y que cada vez es más difícil lograr identificar al autor, de allí la necesidad de normar dichas conductas delictivas, señalando como **objetivo** la necesidad de normar las conductas delictivas que no se encuentran tipificadas a fin de evitar la impunidad y señala como su **metodología** la aplicación de un enfoque cualitativo; **concluyendo** que el internet es una herramienta tecnológica que si bien permite transmitir información también permite el acceso a los delincuentes para una mala utilización de la misma, que cada vez son más continuas, la gran mayoría de usuarios y delincuentes desconocen de los tipos de delitos informáticos, sin embargo es importante que los ataques a la información deben servir como mecanismos de prevención para no ser víctimas de delitos cibernéticos, de allí la necesidad de regular dichas conductas ilícitas que se hayan cometido en cualquier país a fin de reducir el incremento de la delincuencia cibernética, como **análisis** el estudio realizado es muy

genérico porque solo se limita a determinar que las conductas delictivas por el uso de la tecnología informática debe ser regulado en una norma, sin embargo no brinda mayor aporte en los tipos de conducta que deben ser reguladas como delito informático.

Gioia (2019), en su investigación plantea como **problema** que en la actualidad la tecnología facilita la posibilidad de recolectar y guardar información en base de datos, lo cual posibilita que se incrementen los delitos informáticos, de allí la necesidad de salvaguardar los accesos a la base de datos utilizando auditorías de datos para la obtención de evidencias, señalando como **objetivo** la necesidad de contar con una metodología de análisis forense de la base de datos que señale pautas o guías en la actuación pericial a fin de obtener prueba digital válida en un juicio y señala como su **metodología** la aplicación de un enfoque cualitativo; **concluyendo** que no existe una metodología forense que sirva de guía a los peritos informáticos en la evaluación de un caso, asimismo indica que es necesario la estandarización de procesos en las jurisdicciones a fin de salvaguardar la evidencia digital y se ha logrado demostrar que la aplicación de la metodología ForenseDB evita errores u omisiones en el tratamiento de la prueba digital y brinda garantía y asegura la cadena de custodia, por otro lado la auditoría universal de base de datos permite verificar acciones maliciosas, generando así prueba digital para los casos, las nuevas tecnologías de base de datos y aumento de riesgos dan lugar a la necesidad de contar con una metodología de auditoría de datos con fines preventivos, probatorios y correctivos, como **análisis** es posible señalar que el estudio realizado propone un buen aporte y beneficio sobre la forma de protección de las bases de datos aplicando una metodología forense de auditoría.

Santos (2020), en su investigación plantea como **problema** que muchas investigaciones pese a que existen normas que regulan el delito informático no prosperan debido a la falta de pruebas, señalando como **objetivo** definir la capacidad regulatoria de los delitos informáticos y los medios probatorios y señala como su **metodología** la aplicación de un enfoque cualitativo; **concluyendo** que existe una falta de preparación al personal en la materia y políticas de concientización para erradicarlo, en cuanto a los medios probatorios la mayoría de casos se prueba a través

de la evidencia digital obtenida de las pericias forenses, como **análisis** es posible señalar que las conclusiones arribadas no aportan en mucho debido a su generalidad, puesto que no se aterriza señalando cual es la problemática presentada en la obtención de los medios de pruebas para acreditar el delito informático.

Castillo (2021), en su investigación plantea como **problema** que la coyuntura de la emergencia sanitaria por el Covid 19 ha generado el aumento del ciber delito, siendo uno de ellos el que frecuentemente lleguen correos o mensajes fraudulentos respecto de la cuenta bancaria, a fin de obtener información privilegiada con fines patrimoniales, señalando como **objetivo** el estudio de la norma criminal Colombiano respecto de delitos informáticos, especialmente el phishing a fin de determinar su eficacia e insumos para la adopción de medidas y señala como su **metodología** la aplicación de un enfoque cualitativo; **concluyendo** que es necesario implementar acciones preventivas y aumentar las que existen, asimismo se debe reducir el analfabetismo digital para que disminuyan los índices delictivos, es indispensable educar a los usuarios sobre las buenas prácticas de ciberseguridad, como **análisis** es posible señalar que las conclusiones arribadas son correctas y adecuadas en tanto que los usuarios no se generen una cultura de ciberseguridad en el uso de los sistemas informáticos a través del internet no se reducirá la ciberdelincuencia.

Ochoa (2021), en su investigación plantea como **problema** que el avance de las tecnologías de la información dan lugar a que fácilmente se vulnere los espacios cibernéticos generando así la comisión de delitos que no pueden ser evidenciados, señalando como **objetivo** evaluar los desafíos globales provenientes del ciberdelito en la legislación latinoamericana y la capacidad para combatirlo y señala como su **metodología** la aplicación de un enfoque cualitativo; **concluyendo** que el ciberdelito es un problema que afecta a todos los países del mundo, ya que al no contarse con políticas de Estado sobre seguridad informática y defensa de los datos de los ciudadanos los exponen a la impunidad, asimismo señala que las normativas no son suficientes para controlar los actos ilícitos sino se deben dictar políticas de ciberseguridad y cultura cibernética en los usuarios, toda vez que ante la inexistencia de éstas las empresas hacen uso de sus bases de datos sin control alguno, es por ello

que la cooperación internacional sería una de las maneras de mejorar el control y regulación de los ciberdelitos, de otro lado indica que los casos analizados del Ecuador demuestran las escasas medidas de seguridad informática y la ausencia de políticas en ciberdelito, por lo que es necesario que se regule la protección de los datos, como **análisis** es posible señalar que se ha realizado un buen análisis, en tanto que efectivamente la falta de políticas de parte de los estados en materia de protección de datos y seguridad informática genera impunidad en los accionares ilícitos de los ciberdelincuentes.

2.2 Sistemas de seguridad Financiera

A nivel nacional

Ayma (2020), en su investigación plantea como **problema** la falta de control de las redes de datos no permite establecer sistemas de seguridad adecuados, señalando como **objetivo** el poder establecer si los delitos informáticos guardan relación con el proceso de investigación preliminar en el distrito de Lima Norte, y señala como su **metodología** la aplicación de un enfoque cualitativo; **concluyendo** que el secreto bancario reconocido constitucionalmente constituye un obstáculo en la persecución del delito de fraude informático, así como de la recuperación del dinero porque es imposible bloquear el cobro, motivo por el cual debe modificarse la ley y se implemente una plataforma de antifraude intersectorial para actuación inmediata en este tipo de delitos. Ahora bien, como **análisis** es posible señalar que el estudio realizado es correcto, porque efectivamente debido al derecho al secreto bancaria se protege de cierta manera la comisión del delito de fraude informático por el avance de las tecnologías.

Mansilla (2020), en su investigación plantea como **problema** que la digitalización de los servicios financieros ha abierto una brecha de riesgos de ciberataques en sus sistemas de información, señalando como **objetivo** el determinar la necesidad de proponer un programa de cumplimiento de ciberseguridad en las entidades del sistema financiero peruano a fin de que se adopten medidas de ciberseguridad y señala como su **metodología** la aplicación de un enfoque

comparativo el cual permitirá determinar la medidas que pueden ser adoptadas; **concluyendo** que la economía digital ha conducido a una apertura de riesgos digitales en las entidades financieras, situación que permite establecer la necesidad de implementar un sistema de cumplimiento de ciberseguridad, asimismo en el Perú no se cuenta con un reglamento que regule la gestión de riesgos digitales, por lo que es necesario implementar un programa de cumplimiento de ciberseguridad. Ahora bien, como **análisis** es posible señalar que el estudio realizado es correcto, en tanto que con la implementación de un programa de cumplimiento de ciberseguridad va a dar lugar a una mayor confianza y actuara en la prevención de riesgos para evitar la comisión del delito de fraude informático por el avance de las tecnologías.

Cruz (2021), en su investigación plantea como **problema** que el incremento de las transacciones realizadas por medio del internet, es utilizado por bandas para cometer diversos delitos como el de estafa, señalando como **objetivo** el poder determinar el número de casos resueltos en las diversas modalidades del delito de estafas u otras defraudaciones en la DIVIEOD- DIRINCRI PNP, durante el periodo 2018 - 2021 en Lima Metropolitana y señala como su **metodología** la aplicación de un enfoque cuantitativo; **concluyendo** que el secreto bancario reconocido constitucionalmente dificulta la persecución del delito de fraude informático, así como de la recuperación del dinero porque es imposible bloquear el cobro, motivo por el cual debe modificarse la ley y se implemente una plataforma de antifraude intersectorial para actuación inmediata en este tipo de delitos. Ahora bien, como **análisis** es posible señalar que el estudio realizado es correcto, porque efectivamente debido al derecho al secreto bancaria se protege de cierta manera la comisión del delito de fraude informático por el avance de las tecnologías.

Choque (2022) en su investigación plantea como **problema** el alarmante incremento de las cifras por delito informático debido a la falta de prudencia de los usuarios en el uso de las tecnologías de información con garantía de seguridad y protección de su información, señalando como **objetivo** el poder determinar cómo influye la tecnología de la información en la comisión del delito de estafa y señala como su **metodología** la aplicación de un estudio de tipo aplicada, bajo el diseño no

experimental y con un enfoque cuantitativo; **concluyendo** que el uso inadecuado de las tecnologías de la información no contribuye en tipificación del delito de estafa del distrito judicial de Tacna y que el uso inapropiado de recursos y de herramientas contribuye en la tipificación del delito de estafa del distrito judicial de Tacna. Ahora bien, como **análisis** es posible señalar que el estudio realizado es correcto, en tanto que se basa en un distrito judicial donde no existe una mayor incidencia delictiva por delitos informáticos.

Montalvo (2022), en su investigación plantea como **problema** la falta de estándar de sistemas de seguridad informáticos para salvaguardar los datos de tarjetas de pago de las entidades bancarias, señalando como **objetivo** el de proponer si los delitos informáticos se relacionan con el proceso de investigación preliminar en el distrito de Lima Norte, y señala como su **metodología** la aplicación de un enfoque cualitativo; **concluyendo** que para disminuir el fraude cibernético es necesario contar con un estándar de seguridad PCI-DSS, PCI-CP, ISO27001 y de la inteligencia artificial como el Machine learning y biométrico a fin de proteger la información asimismo se necesita contar con un buen nivel de red y equipos informáticos que protejan la información, también se debe utilizar el chip en las tarjetas, cifrado de datos, capacitación, contar con un programa de código seguro e implementación de la inteligencia artificial en la red interna y externa de las tarjetas de pago, como **análisis** es posible señalar que el estudio analiza adecuadamente la necesidad de contar con patrones de seguridad para salvaguardar los datos de las tarjetas de pago a fin de evitar el incremento de los fraudes cibernéticos .

A nivel Internacional

Romano (2019), en su investigación doctoral plantea como **problema** que durante muchos años el delito informático ha tomado fuerza, motivo por el cual es necesario buscar soluciones a todas aquellas amenazas informáticas, señalando como **objetivo** la búsqueda de conocimientos útiles para los operadores de justicia, que les permita conocer los conceptos informáticos a fin de reducir la ciberdelincuencia y sancionar los casos evitando la impunidad y señala como su **metodología** la

aplicación de un enfoque cualitativo; **concluyendo** que a lo largo de los años los ataques DoS han crecido exponencialmente causando graves daños, motivo por el cual es necesario la propuesta de una normativa que regule dicha materia, a fin de que las empresas cuenten con medios de ciberseguridad básicos y así con ello evitar grandes pérdidas económicas y reducir las cifras de ataques, como **análisis** es posible señalar el estudio realizado hace un buen aporte, en tanto que podemos advertir que es un gran problema la falta de cultura de las empresas de contar con sistemas de seguridad adecuados en la protección de los datos.

Londoño (2020), en su investigación plantea como **problema** que debido al comercio electrónico los ciudadanos realizan millones de transacciones por internet, de los cuáles los bancos deben contar con medidas de seguridad que cautelen la identidad y autorización del cliente, sin embargo debido a la falta de seguridad informática se han cometido delitos de fraude informático, por lo que es indispensable analizar la responsabilidad objetiva en las operaciones electrónicas de las entidades financieras, señalando como **objetivo** es plantear si existe responsabilidad objetiva en las entidades financieras por la falta de seguridad en las plataformas digitales donde se realizan operaciones electrónicas bancarias y señala como su **metodología** la aplicación de un enfoque cuantitativo; **concluyendo** que existe una tendencia sobre responsabilidad objetiva por riesgo, sin embargo el operador de justicia valora la diligencia y cuidado como si se tratara de responsabilidad por culpa, asimismo indica que de acuerdo al estudio y análisis de todos los elementos para determinar la responsabilidad por fraude de las entidades bancarias se debe aplicar el régimen subjetivo de responsabilidad y no la responsabilidad objetiva, toda vez que el cuidado y diligencia deben ser realizados por ambas partes (banco-cliente), debido a la asunción de riesgos por los mecanismos electrónicos usados, pues en todo caso el perjuicio patrimonial debe ser asumido por quien incumplió con sus obligaciones y en caso de concurrencia de culpa, cada uno asumirá en proporción a la falta de cuidado, pues no podría aplicarse la responsabilidad extracontractual en actividades de riesgo en temas financieros, como **análisis** es posible señalar que la investigación realizada evalúa los dos tipo de responsabilidad (subjetiva y objetiva) señalando que ante una

conducta riesgosa no es factible la responsabilidad extracontractual, sin embargo a mi criterio es necesario analizar caso por caso a fin de poder determinar si efectivamente existe o no la posibilidad de que se presente la responsabilidad objetiva.

Apolinario (2022), en su plantea como **problema** que las plataformas digitales ofrecidas por las entidades financieras no son seguras generando un riesgo en los usuarios, señalando como **objetivo** plantear la creación de un centro de respuesta a incidentes de seguridad informática para medios de pago digitales en el Ecuador y señala como su **metodología** la aplicación de un enfoque cualitativo; **concluyendo** que se seleccionó como CSIRT el tipo de coordinación y modelo combinado, debido a que se debe centralizar las incidencias en la comunidad y a la vez con otros CSIRT nacionales e internacionales, como **análisis** es posible señalar que la investigación ha realizado un buen estudio respecto a la creación de una entidad que se ocupe del control de la ciberseguridad en el ámbito financiero del Ecuador, el cual es uno de los principales problemas a nivel internacional.

López (2022), en su investigación plantea como **problema** que la incorporación de nuevas tecnologías ha dado lugar a la creación de productos en las entidades financieras de Colombia, los cuáles corren riesgos de ataques cibernéticos respecto de la información de los usuarios, afectándose con ello la confianza y continuidad del negocio, señalando como **objetivo** establecer guías o pautas sobre las condiciones mínimas de ciberseguridad que deben contar los productos ofrecidos por las entidades financieras, y señala como su **metodología** la aplicación de un enfoque cualitativo; **concluyendo** que en la actualidad las entidades financieras no cuentan con instrumentos que les permitan conocer de las condiciones mínimas de ciberseguridad, asimismo tampoco tienen una hoja de ruta de cómo deben actuar ante los constantes avances tecnológicos sobre los productos digitales que implementan, de otro lado también indica que la voluntad de las entidades financieras de proteger su data es mínima, es por ello que es necesario plantear una herramienta guía donde indique cuáles son las condiciones mínimas de ciberseguridad que se deben tener en cuenta en la creación de sus productos digitales con la finalidad de brindar confianza al usuario, como **análisis** es posible señalar que la investigación propone una buena

alternativa de protección de datos de los usuarios que utilizan las plataformas digitales implementadas por las entidades financieras a fin de evitar vulneraciones, seguridad y confianza al público usuario.

Mamani (2022), en su investigación plantea como **problema** que a pesar de que el gobierno Boliviano ha dictado lineamientos de seguridad de la información, estos a la fecha no han dado resultados, de allí la necesidad de proponer un procedimiento de gestión de seguridad de la data informática en las instituciones públicas que garantice la información que manejan, señalando como **objetivo** es plantear un sistema de gestión de seguridad de la información en las instituciones públicas que garanticen la reserva, integridad y disponibilidad de su base de datos y señala como su **metodología** la aplicación de un enfoque mixto cuantitativo y cualitativo; **concluyendo** que es indispensable la creación de un sistema de gestión de seguridad de la información en entidades públicas y privadas que manejen base de datos donde se debe garantizar la reserva, probidad y disponibilidad de la base de datos, toda vez que pese a que existen normas emitidas en el Estado éstas no se cumplen en su totalidad por parte de las instituciones, de allí la necesidad de que se implemente un sistema de gestión de seguridad de la información a fin de poder evaluar las necesidades de la entidad y concientizar la importancia de proteger la información, como **análisis** es posible señalar que el estudio nos aporta con una alternativa de política de seguridad de la información concientizando a las instituciones de la importancia que tiene el proteger su base de datos.

2.3 Definición de Categorías

2.3.1 Definición de delito Informático - Fraude Informático

Villavicencio (2014) señala que el delito informático es toda conducta que vulnera los sistemas de seguridad, es decir son intrusiones en las computadoras, correos o base de datos a través de una clave de acceso, realizadas por medio de la tecnología digital.

Carrera (2021) citando a Dass señala que el delito informático es todo dispositivo aislado o conjunto que se encuentra conectados o relacionados que afecta elemento o tratamientos electrónicos a través de datos o programas de ejecución.

Choque (2022) citando a Villavicencio señala que los delitos informáticos son aquellas acciones destinadas a vulnerar los sistemas de seguridad a fin de ingresar a equipos de cómputo, correos electrónicos o base de datos por medio de la manipulación de las claves de acceso y a través de la utilización de las tecnologías.

Zevallos (2020) en su artículo señala que el delito informático es aquella conducta que vulnera los sistemas de seguridad por medio de una clave de acceso, accionar que solo pueden ser realizadas por medio de la tecnología.

La ley N° 30096 (2013) Ley de Delitos Informáticos desarrolla el delito de fraude informático señalando:

“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,” (p. 505485)

Carrera (2021) señala que el delito informático en su forma de fraude informático viene hacer la transmisión de datos, que actualmente es fácil de obtenerla a través de modificaciones efectuadas de una misma computadora en el domicilio o la de enviar datos de una computadora a otra.

Cisneros (2022) citando a Saltos, Robalino y Pazmiño señala que el fraude informático consiste en robar información de una persona que hace uso del internet debido a la facilidad con la que se puede obtener y a la vez procura un beneficio patrimonial a un tercero.

Cisneros citando a Villavicencio sostiene que el delito informático es un delito de resultado porque es necesario que se cause un perjuicio a un tercero.

Condori (2020) citando a Aboso señala que el fraude informático es el traslado de dinero ajeno a una cuenta propia o de tercera persona o la eliminación de datos económicos que causan un perjuicio en el estado financiero personal.

Condori (2020) citando a Costa señala que el fraude informático es la acción u omisión para vulnerar las normas jurídicas con la finalidad de causar un perjuicio patrimonial en sus víctimas.

Vinelli (2021) señala que el delito de fraude informático requiere de la manipulación de un sistema informático a fin de beneficiarse económicamente.

Bramont Arias (2017) señala que el delito informático es aquel que requiere de un sistema informático de procesamiento de datos o de envío de datos.

2.3.2 Definición de sistemas de Seguridad Financiero

Mansilla (2020) citando a la Circular SBS N° G-140-2009, señala que la seguridad de la información viene hacer la adecuada composición de políticas, procedimientos, estructura organizacional e instrumentos informáticos especializados con la finalidad de que la información cumpla con los criterios de confidencialidad, integridad y disponibilidad.

Según el ISO N° 27001 la seguridad de la información viene hacer aquella actividad cuyo objetivo es asegurar que la información de una entidad sea usada de manera adecuada, es decir respetando los accesos de información implementados.

Mansilla (2020) citando a la Unión Internacional de Telecomunicaciones señala que la ciberseguridad es el conjunto de políticas, instrumentos, directrices, actividades, prácticas idóneas, seguros y tecnologías que son usados con la finalidad de proteger la base de datos de las entidades y a los usuarios.

López y Rodríguez (2022) citando al BID señalan que la ciberseguridad es la intrusión permanente en todos los ámbitos de la vida humana debido a la innovación tecnológica que se presentan en el acceso digital, conexión, seguridad y defensa internacional, justicia y comercio electrónico.

Romano (2019) citando a Pacheco y Caballero señala que la seguridad informática versa sobre una serie de herramientas que se definen como un conjunto de medidas preventivas, de detección, corrección que buscan salvaguardar la integridad, confidencialidad y disponibilidad de los caudales informáticos. Asimismo, señala que la seguridad de la información tiene como finalidad garantizar que los riesgos de los datos sean evidenciados y minimizados de modo tal que se adapten a los posibles cambios de las tecnologías.

Mamani (2022) señala que la seguridad de la información es el conjunto de medidas de prevención que controla, salvaguardan y preservan la información con la que se cuenta y se transforma. Asimismo, indica que la seguridad de la información debe prevenir y solucionar los riesgos a fin de eliminarlos de ser posible.

2.4 Marco Filosófico

Hernández y Mendoza (2018) define a la investigación como el conjunto de procesos metódicos y empíricos que se aplican en un problema para la obtención de un resultado, permitiendo así ampliar los conocimientos.

Mario Bunge (2017) señala que la metodología de la investigación proviene de la ciencia con la finalidad de crear y desarrollar conocimientos, ya que a través de los métodos teóricos las teorías justifican no solo los hechos descritos sino también los modelos conceptuales de los hechos, lo cual permite explicar y predecir los hechos de un determinado tipo.

2.5 Marco Histórico

Ayma (2020) señala que en el Perú el delito informático inicialmente se tipificó en el artículo 186.3 segundo párrafo del Código Penal, posteriormente se reguló en los artículos 207a, 207b, 207c, 207d, del capítulo X del mismo cuerpo legal antes citado, los mismos que en el año 2013 fueron derogados, finalmente fueron regulados normativamente por Ley N° 30096 la cual está estructurada por siete capítulos, la misma que fue modificada en parte por la Ley N° 30171, ello en virtud de adecuación de los estándares señalados en el convenio de Budapest.

2.6 Marco Conceptual

Delito Informático: Constituye una actividad ilícita que realiza una persona por el mal uso del sistema informático en contra de personas naturales o jurídicas, robando información y vulnerando la normativa existente. (Ayma, 2020).

Fraude Informático: Viene hacer la introducción de datos falsos por la manipulación de los datos de los ordenadores de las empresas al eliminar los sistemas de seguridad, ello a fin de realizar operaciones en línea sin la autorización de las empresas. (Ayma, 2020).

Seguridad Informática: Es la protección del software o hardware del propietario. (Mamani, 2022).

Seguridad de la Información: Es la garantía que se otorga ante los posibles riesgos de ataques de la información. (Mamani, 2022)

Pishing: Es una modalidad del fraude informático que tiene como fin robar la información de los titulares de las tarjetas de crédito o débito. (Ayma, 2020).

Base de datos: Es la que está conformada por toda la información almacenada en sistemas operativos de computadoras privadas.

Ataque a una red: Viene hacer aquel ingreso de un hacker por medio de una red a los ordenadores de una empresa a fin de extraer la información. (Ayma, 2020).

Sistema Informático: Es el conjunto de programas que permite almacenar o guardar información de manera automatizada.

Cibercriminología: Cámara (2020) citando a Jaishankar la define como el estudio del origen de los delitos que suceden en un entorno digital y su repercusión en el espacio físico.

Perfil del delincuente: Es el sujeto que cuenta con conocimiento especializado y habilidades en el uso del sistema informático. (Villavicencio, 2014)

Hacker: Cámara (2020) señala que es aquella persona experta en informática y redes, cuenta con el conocimiento en programación, hardware y software.

Cracker: son personas que utilizando sus conocimientos cambian el procedimiento de los sistemas y redes. (Cámara, 2020).

Phisher: Son aquellos sujetos que buscan obtener los datos personales y bancarios de una persona con la finalidad de beneficiarse patrimonialmente, para lo cual utilizan correos electrónicos con un malware. . (Cámara, 2020).

III. METODOLOGÍA

3.1 Tipo y diseño de investigación:

3.1.1 Tipo de investigación:

Según el metodólogo Vara (2010) señala que la investigación es básica o aplicada porque se busca a través de los resultados aportar conocimientos para resolver los problemas presentados.

Arias et al. (2022) señala que es una investigación básica porque ayuda a mejorar el conocimiento de un fenómeno, se evalúa datos para hallar lo desconocido.

De acuerdo a la investigación del delito de Fraude informático es básica porque se pretende determinar si la normatividad vigente regula responsabilidad penal objetiva por parte de las entidades financieras en el mencionado delito.

3.1.2 Diseño de investigación:

El diseño de la presente investigación relacionada al delito de fraude informático y sistemas de seguridad es con enfoque cualitativo lo cual conforme lo señalaron Hernández y Mendoza (2018) la investigación cualitativa se basa en entender los fenómenos examinando a los participantes desde su propio ambiente y vinculándolo al contexto, con ello se busca conocer más a fondo lo que se va a investigar, el mismo que utiliza como diseño metodológico, la teoría fundamentada, la misma que conforme señalan De la Espirella y Gómez (2020) es un método cualitativo que se enfoca en derivar o generar información a partir de datos para establecer una teoría o modelo. Este método está diseñado para generar conceptos y teorías basados en el conocimiento.

3.2 Categorías y Sub categorías:

De acuerdo a la presente investigación se cuenta con las siguientes categorías:

Fraude Informático

Cisneros (2022) citando a Saltos, Robalino y Pazmiño sostiene que el delito de fraude informático consiste en sustraer información de una persona que hace uso del internet debido a la facilidad con la que se puede obtener y a la vez procura un beneficio patrimonial a un tercero.

Sub Categoría A: robo de datos

Condori (2020) citando a Villavicencio señala que es un acto realizado con la finalidad de burlar el sistema de seguridad e ingresar a una base de datos usando una clave de acceso a través del uso de la tecnología.

Sub categoría B: Alterar o dar mal uso a sistemas o software

Condori (2020) citando a Jiménez señala que consiste en modificar o reescribir código para fines no autorizados. Este tipo de operaciones requieren conocimientos informáticos avanzados.

Sistemas de seguridad en las entidades financieras

Mansilla (2020) citando a la Circular SBS N° G-140-2009, señala que la seguridad de la información viene hacer la adecuada composición de políticas, procedimientos, estructura organizacional e instrumentos informáticos especializados con la finalidad de que la información cumpla con los criterios de confidencialidad, integridad y disponibilidad.

Sub Categoría C: utilización adecuada de información

Ayma (2020) señala que está referido a noticias relacionadas con la acumulación de información. Productos informáticos que ayudan a su negocio.

Sub Categoría D: Respeto de los accesos de la información establecidos.

Ayma (2020) señala que son claves de acceso de un sistema operativo de la institución, las cuáles contienen caracteres de letras y números combinados y que solo es conocido por los responsables.

La tabla de matriz apriorística

La tabla de matriz apriorística se adjuntará como anexo 1.

3.3 Escenario de estudio:

Cisneros (2022) citando a Taylor y Bogdan señala que el escenario de estudio es el espacio determinado de donde se recoge la información.

El objeto de estudio de la presente investigación es referente al delito de fraude informático que se ha estado suscitando en la actualidad y los sistemas de seguridad financiero que no son idóneos para la protección de datos de los usuarios que utilizan las plataformas tecnológicas ofrecidas por las entidades financieras, con la finalidad de agilizar el comercio y transacciones financieras, lo cual es aprovechado por los ciber delincuentes para vulnerar los sistemas de seguridad, manipulando las computadoras de las entidades a fin de causar un perjuicio patrimonial a los usuarios, asimismo, el objetivo de la presente investigación es el de analizar de qué manera el tratamiento del fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias en el distrito fiscal de Lima Centro 2022.

Los sujetos de estudio son los imputados que se evidencian a través de las carpetas fiscales, en las mismas que se encuentra su declaración y es a través de ésta que se va a poder analizar el grado de su autoría y participación, así como de generar evidencia digital de la forma como se llegó a vulnerar los sistemas de seguridad de los ordenadores donde se encuentran almacenadas la base de datos de los usuarios de las entidades bancarias, así como si existe responsabilidad de terceros, ello durante el periodo de la investigación.

Lugar en las fiscalías de ciberdelincuencia de Lima Centro 2022, dado que existe una mayor incidencia delictiva e incremento de denuncias por delito de fraude informático, debido a la vulneración de los sistemas de seguridad de la información,

ello debido a que la ciudad de Lima es donde se concentra la mayor cantidad de población, las nuevas tecnologías por ser la capital del país, así como se encuentran las principales entidades bancarias, así como la mayor incidencia delictiva en el delito materia de investigación..

3.4 Participantes:

Arias et al. (2022) señalan que la población es el conjunto de personas con características parecidas o comunes entre sí.

En la presente investigación los participantes son:

Fiscales especializados en ciberdelincuencia, quiénes investigan este tipo de delitos y conocen de primera mano las incidencias delictivas y las problemáticas existentes para la investigación del delito.

Jueces quiénes son los que resuelven los casos por delito de fraude informático.

Abogados Defensores, quienes ejercen la defensa de los autores del delito.

3.5 Técnicas e instrumentos de recolección de datos:

Técnicas

Cisneros (2022) citando a Hurtado señala que la técnica es de la observación es la forma inicial de analizar el fenómeno directamente y ello se presenta cuando se aplica la entrevista en la investigación cualitativa.

I**nstrumentos**

Hernández y Mendoza (2018) señala que la entrevista es la concertación de una reunión entre dos personas para intercambiar información.

En la presente investigación se aplicará entrevistas con preguntas abiertas cuyo instrumento a utilizarse es la Guía de entrevistas que guardan relación con las categorías y sub categorías y el análisis de información.

3.6 Procedimiento de recolección de datos:

Hernández y Mendoza (2018) sostiene que la recolección de datos es esencial en una investigación cualitativa, siendo su propósito la obtención de datos informativos, los mismos que son recopilados para su examen y comprensión y así dar respuesta a las interrogantes de la investigación y generar conocimiento.

La recolección de datos será a través de la guía de entrevistas relacionada a delito de fraude informático y sistemas de seguridad de la información por el robo de datos, la alteración o mal uso de los sistemas o software, la utilización adecuada de información, y respeto de los accesos a la información establecidos. La información acopiada ha servido para la elaboración de la matriz de triangulación y que luego han sido contrastados con el análisis teórico logrando un resultado más satisfactorio.

En caso de presentarse controversia, contradicción, conflicto o discordia entre los entrevistados y el análisis documental se procederá a la triangulación de las categorías o sub categorías. La discordia debe hacerse por teórico metodológico, autores, práctico por tema o especialidad y se debe hacerse un análisis crítico.

3.7 Rigor científico:

Confiabilidad de instrumentos de recolección de datos

Con la aplicación de los instrumentos a una muestra de 10 participantes (fiscales, jueces y abogados) especialistas en ciber delincuencia de características similares, la información recabada se tabulo en una matriz de Excel, por consiguiente, los cuestionarios cuentan con un nivel de confiabilidad óptima.

Dependencia

El presente estudio cualitativo se basa en las métodos e instrumentos de recopilación de datos.

Transferibilidad

En la presente investigación el resultado se va a obtener porque se va a realizar un estudio minucioso del problema, ello a fin de lograr el objetivo del estudio.

Confortabilidad y audibilidad

En la investigación se va a clasificar y examinar el resultado de los datos con el objeto de llegar a tener una respuesta al problema planteado.

Validación

Los instrumentos han sido validados por expertos especialistas en metodología y en materia penal, evaluándolo en base a las variables de estudio.

Validación de Expertos

NOMBRES Y APELLIDOS	**CARGO**	**EXPERIENCIA**
Camayo Tovar Freddy	Abogado Juez de Paz Letrado Penal	7 AÑOS 7 MESES
Linares Perez, Fiorella	Juez de Investigación Preparatoria	5 AÑOS
Del Villar Canchari, Fernndo	Abogado	3 AÑOS

3.8 Método de análisis de la información:

En la presente investigación una vez recopilada la información se aplicará la triangulación de datos, a fin de que a través de las fuentes de información y estrategias se logre llegar a una información consolidada.

Asimismo, la estructura que se va a utilizar es la elaboración de la entrevista con preguntas a fin de obtener información, luego se va a proceder a codificar la data y finalmente se examinará la información recabada contrastándola desde las diversas opiniones y apreciaciones.

Bernal (2010) señala que el método inductivo usa el razonamiento para llegar a las conclusiones.

MÉTODO INDUCTIVO

En la investigación se va a realizar un estudio independiente de cada variable y así de esa manera se pueda obtener conclusiones que serán postuladas como leyes, principios o fundamentos.

Bernal (2010) señala que el método histórico es la manera de investigar y elucidar los fenómenos culturales, que radica en verificar las similitudes de estos fenómenos y sacar conclusiones sobre sus orígenes.

MÉTODO HISTORICO

En la investigación se procedió a examinar los datos históricos existentes a fin de poder verificar su evolución y compararlos con los actuales y así de esta manera determinar las posibles respuestas al problema planteado.

Bernal (2010) señala que el método analítico es la descomposición del objeto de análisis para examinarla de manera individual.

MÉTODO ANALÍTICO

En la presente investigación se procedió a examinar la información recopilada de manera independiente por cada una de las variables del problema.

Estupiñan (2021) citando a García señala que el método exegético es la interpretación de la norma basado en su propio texto.

MÉTODO EXEGETICO

En la presente investigación se procedió a analizar la norma jurídica que tipifica el delito y contrastarla con las actividades ilícitas que realizan los ciberdelincuentes mediante el uso de los sistemas tecnológicos.

3.9 Aspectos éticos:

Ayma (2020) citando a Lipman señala que toda investigación debe promover respeto a la propiedad y derechos de los sujetos.

En la presente investigación se consideró la norma internacional APA 7, la normatividad nacional, la guía de investigación de la Universidad y el turnitin.

Asimismo, se va a considerar el consentimiento de los participantes, la autenticidad y credibilidad de la información, cumpliendo así con los criterios de credibilidad, transferibilidad y confortabilidad.

IV. RESULTADOS Y DISCUSIÓN.

Según Hernández y Mendoza (2018) indica que los resultados se presentan como una narrativa general de análisis obtenido de lo señalado por los entrevistados y de las del investigador propiamente, asimismo señala que de la discusión se llega a las conclusiones y recomendaciones respecto de los objetivos planteados en relación al resultado con el estudio previo.

4.1 Resultados de las entrevistas y análisis documental

Objetivo General: Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022 se ha formulado la Pregunta 01: ¿Explique Ud. si el delito de Fraude Informático regula la responsabilidad penal de las entidades financieras?

Jueces: Abogada Ocares (2023) se observa que, dentro de su tipificación, no se menciona nada respecto de la responsabilidad penal de las entidades financieras. Una de las razones por la cual, se podría pensar, que no tienen responsabilidad penal, en los delitos de fraude informático, es porque tal vez su finalidad, no es la de cometer un ilícito penal, sino brindar un servicio, a fin de obtener a través de ello una utilidad; sin embargo, ello no lo exime de las responsabilidades civiles o administrativas, de no aplicar correctamente las regulaciones establecidas en los reglamentos de cumplimiento, y evitar riesgos que puedan poner en peligro a los usuarios de su servicio; **Mg. Castañeda (2023)** señala que si en la medida que se aplique en concordancia con el artículo 27 del Código Penal (el actuar por otro)**, Abogado La Rosa (2023)** indica que el delito de fraude informático no prevé de manera expresa sobre la responsabilidad penal de las entidades financieras, lo que sí es abordado en la 10° disposición complementaria final de dicha ley y el Código Procesal Penal. **Fiscales: Abogado Paucar (2023)** indica que no, se encuentra contemplado en la Ley N° 30096;

Abogado Portillo (2023) señala que el delito de fraude informático del artículo 8 de la Ley no contempla de forma expresa responsabilidad penal solo consecuencias en mérito a la cooperación y el cumplimiento de información, de forma posterior; **Abogada López (2023)** indica que el delito de fraude informático no regula la responsabilidad penal de las entidades financieras, porque son ellas muchas veces sujetos pasivos de éste delito, quienes se ven afectadas en su imagen, puesto que crea desconfianza entre sus clientes. **Abogados: Abogado Durand (2023)** indica que el delito de fraude informático regula la acción y la responsabilidad penal del sujeto activo que comete el delito, y las entidades financieras con responsabilidad civil, y en casos específicos lo regula su ley especial que los sanciona por no cumplir con el deber de protección de sus productos, en materia contencioso administrativa; **Abogada Purizaca (2023)** señala que el delito de fraude informático actualmente regulado en una ley penal especial no contempla de forma expresa la responsabilidad penal de las entidades financieras. Si bien existen pronunciamientos del ente regulador (SBS) sobre la falta de diligencia en operaciones bancarias, dicha regulación no alcanza el ámbito penal; **Abogada Huiza (2023)** señala que la Ley N° 30096, conocida como la Ley de Delitos Informáticos no regula específicamente la responsabilidad penal de las entidades financieras de manera exclusiva, sin embargo las entidades financieras pueden ser consideradas responsables penalmente por su participación en casos de fraude informático en virtud de otras disposiciones legales y principios generales del derecho penal. La responsabilidad penal de las entidades financieras puede basarse en teorías como la responsabilidad por el actuar de sus empleados en el curso de su actividad, la responsabilidad por omisión en la implementación de medidas de seguridad o la responsabilidad por el beneficio obtenido a través del fraude.

Pregunta 02: ¿Explique Ud. Si el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiera?

Jueces: Abogada Ocares (2023) señala que el delito de fraude informático, influye, en los sistemas de seguridad financiera, porque establecen una forma de garantía para la prevención, contra aquellas personas que vulneren las medidas de seguridad, establecidas por los entes financieros dentro de sus sistemas de seguridad,

a fin de proteger el sistema de pagos y la estabilidad financiera de los intereses de sus propios usuarios; **Mg. Castañeda (2023)** opina que si las entidades del sistema funcionario utilizan sistemas informáticos, las conductas típicas del fraude informático también pueden aplicarse a dichos sistemas**, Abogado La Rosa (2023)** señala que la norma también incide en los sistemas de seguridad financiera, lo dispuesto en la 4° Disposición final y complementaria de la Ley N° 26702, en cuanto al informe técnico de la SBS ni bien se formule denuncia penal contra alguna entidad del área. **Fiscales: Abogado Paucar (2023)** indica que si, tanto a nivel interno como externo, incluso existe un reglamento de la SBS sobre ciberseguridad; **Abogado Portillo (2023)** señala que si, efectivamente el delito de fraude informático en los verbos rectores implica de por si un atentado a la seguridad o al sistema bancario como tal, por ende repercute en las políticas de prevención y seguridad; **Abogada López (2023)** indica que los ciber delincuentes muchas veces logran ingresar a los sistemas financieros de las empresas, en especial del sistema bancario, burlando los sistemas de seguridad, por lo que definitivamente repercute en los sistemas de seguridad financiera. **Abogados: Abogado Durand (2023)** indica que a su entender si repercute por cuanto ante un delito informático responden con multas impuestas de encontrarse responsabilidad**, Abogada Purizaca (2023)** señala que el alcance del delito de fraude informático sí repercute en los sistemas de seguridad financiera, dado que muchas de estas modalidades se realizan mediante la alteración o clonación de datos personales mediante medios informáticos. Así, los ciberdelincuentes logran vulnerar los sistemas de seguridad de los bancos para disponer del dinero de terceros; **Abogada Huiza (2023)** considera que el tratamiento del delito de fraude informático si puede tener repercusiones significativas en los sistemas de seguridad financiera, toda vez que el fraude informático puede afectar la integridad, confidencialidad y disponibilidad de la información financiera, así como comprometer la seguridad de los sistemas y transacciones electrónicas, más aun teniendo en cuenta que en el ámbito financiero, la confianza y la seguridad son fundamentales para el buen funcionamiento de los mercados y la protección de los derechos e intereses de los usuarios.

Pregunta 03: ¿Señale Ud. si el delito de Fraude Informático regula responsabilidad penal por la falta de implementación de sistemas de seguridad financiera?

Jueces: Abogada Ocares (2023) señala que Actualmente, el delito de fraude informático no regula la responsabilidad penal por falta de implementación de sistemas de seguridad en sus actividades financieras, para ellos existen otras normas que le son aplicables, de acuerdo a la materia y que podrían ser materia o pasibles de las consecuencias jurídicas penales establecidas en el art. 105° del Código penal, el cual podría ser modificado para darles el alcance a las entidades financieras en este rubro de ilícitos penales; **Mg. Castañeda (2023)** opina que Si se tiene en cuenta el artículo 8 de la Ley de Delitos Informáticos no hay responsabilidad penal por ello**, Abogado La Rosa (2023)** en su tenor no, pero en aplicación de las glosadas normas de la Ley de delitos informáticos y de la Ley General de la SBS y sus afines si se expresa determinadas pautas para investigar, probar y sancionar a las empresas financieras en ese rubro. **Fiscales: Abogado Paucar (2023)** indica que no actualmente no lo regula; **Abogado Portillo (2023)** señala que no contiene expresamente responsabilidad por falta de implementación, o ausencia de las mismas; **Abogada López (2023)** indica que no regula responsabilidad penal contra de las empresas del sistema bancario, por la falta de implementación de sistemas de seguridad financiera. **Abogados: Abogado Durand (2023)** indica que efectivamente que sí, conforme lo establecido en las disposiciones complementarias finales, disposición DEIMA de la Ley N° 30096, sobre regulación e imposición de multas por la superintendencia de Banca y Seguros y AFP; **Abogada Purizaca (2023)** señala que actualmente solo se encuentra regulada la responsabilidad administrativa por falta de implementación de los mecanismos necesarios para la seguridad financiera (o Compliance); sin embargo, existe la responsabilidad penal de la persona jurídica cuando hubiera participado en la comisión de un delito en beneficio de la misma empresa, para lo cual la se aplican las consecuencias accesorias; **Abogada Huiza (2023)** indica que el delito de Fraude Informático en el Perú no regula específicamente la responsabilidad penal por falta de implementación de sistemas de seguridad financiera sino se centra principalmente en la manipulación o alteración ilícita de datos electrónicos con el fin de obtener un

beneficio económico o causar perjuicios a terceros. Sin embargo, en el contexto de las entidades financieras y la implementación de sistemas de seguridad, existen otras disposiciones legales y regulaciones que establecen obligaciones y responsabilidades para proteger la integridad y confidencialidad de la información financiera.

Objetivo Especifico 01: Evaluar si el delito de fraude informática regula responsabilidad penal de la entidad financiera en relación a los sistemas de seguridad financiero del distrito fiscal Lima Centro 2022

Pregunta 04: ¿Cree Ud. que es posible determinar responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático?

Jueces: Abogada Ocares (2023) señala que Actualmente en el sistema penal peruano, rige el principio "*societas delinquere non potest",* mediante este principio no se regula o aplica, al menos actualmente una responsabilidad penal, para las personas jurídicas; sin embargo como ya se mencionó anteriormente es posible determinar las consecuencias accesorias y aplicables reguladas por el art. 205° del código penal; **Mg. Castañeda (2023)** opina que típicamente es posible la responsabilidad penal de dichas entidades. El problema es su prueba. La posibilidad de investigar o analizar sus sistemas informáticos está cerrada a terceros. Normalmente es la propia entidad financiera la que se supone hace esa evaluación; **Abogado La Rosa (2023)** señala que bajo las normas aludidas y en aplicación de la Ley N° 30424 puede establecerse según los hechos concretos y las pruebas, la responsabilidad administrativa de las entidades financieras según el caso, el programa de cumplimiento normativo o compliance program busca también prevenir y detectar tal delito. **Fiscales: Abogado Paucar (2023)** indica que existiría responsabilidad por delito de acceso ilícito con circunstancia agravante de móvil económico; **Abogado Portillo (2023)** señala que estima que si es posible establecer consecuencias por responsabilidad de entidades financieras, si se comprueba fallas en las políticas de protección, sistemas de alerta,

seguridad u otros que resguardan operaciones no reconocidas**;** **Abogada Lopez (2023)** indica que difícilmente se puede determinar responsabilidad penal de las entidades financieras por el robo de datos, por el contrario, resultan perjudicados. **Abogados: Abogado Durand (2023)** indica que hasta ahora por su experiencia más han sido sancionadas con multas por encontrarse responsables; **Abogada Purizaca (2023)** señalan que existen avances importantes en relación a la responsabilidad administrativa y penal de la persona jurídica, dado que la realidad nos demuestra que para muchas operaciones financieras los bancos no agilizan todos los mecanismos de verificación que demuestren que dicha operación fue segura. Por el contrario, incluso en muchas ocasiones se ha advertido que dentro de los mismos bancos existen trabajadores que extraen datos personales del usuario; **Abogada Huiza (2023)** señala que es posible determinar la responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático en el Perú, siempre y cuando se cumplan ciertos requisitos legales establecidos en la Ley N° 30096. En el caso de las entidades financieras, si se demuestra que han participado activamente en el robo de datos o han facilitado intencionalmente dicha conducta delictiva, pueden ser consideradas responsables penalmente. Esto puede ocurrir si, por ejemplo, un empleado de la entidad financiera está involucrado directamente en el robo de datos o si la entidad financiera no ha implementado las medidas de seguridad adecuadas para proteger la información de sus clientes y ha permitido la vulneración de los sistemas.

Pregunta 05: ¿Puede Ud. indicar de acuerdo a su experiencia qué tipo de responsabilidad se ha logrado identificar en el delito de fraude informático respecto a las entidades financieras?

Abogada Ocares (2023) señala que en este tipo de delitos complejos, en su determinación, por las actividades que realiza, y la multiplicidad de sujetos que intervienen en ello, generalmente se vulneran intereses colectivos, relacionados con los propios sistemas de seguridad de las entidades financieras, pues las empresas de éste tipo, mantienen una serie complejidades dentro de su distribución de funciones, y

siendo ello así, se advierte, generalmente que son agrupaciones, que con un rol especifico, para cada uno de sus individuos - partícipes, afectan intereses colectivos, como por ejemplo, afectación en el tráfico de información, o de bienes jurídicos relacionados con caudales, o patrimonios personales e incluso hasta el propio comercio electrónico**, Mg. Castañeda (2023)** opina que no recuerdo algún caso donde la entidad financiera haya respondido penalmente por fraude informático. En general, se le trata solo como tercero civil responsable; **abogado La Rosa (2023)** señala que se halla una responsabilidad penal de sus agentes y una responsabilidad administrativa de las entidades bancarias de ser el caso, les alude a ambos una responsabilidad civil. **Fiscales: Abogado Paucar (2023)** indica que se ha tomado conocimiento que en algunos casos se ha determinado responsabilidad administrativa ante salas de Indecopi; **Abogado Portillo (2023)** señala que no se ha podido establecer casos de responsabilidad a la fecha, al menos del conocimiento del suscrito; **Abogada López (2023)** indica que el tipo de responsabilidad que le correspondería a las entidades financieras sería la de responsabilidad civil, es decir, sería un tercero civilmente responsable. **Abogados: Abogado Durand (2023)** indica que cuando existe un tema de delitos informáticos por clonación de tarjetas o por tono de dinero de tarjetas, no solo se ha recurrido a la denuncia penal, sino se ha hecho la denuncia administrativa lográndose imposición de multas, al encontrarse responsabilidad de la entidad financiera por falta de implementación en su sistema de seguridad**; Abogada Purizaca (2023)** señala que en su experiencia no he tenido la oportunidad de conocer casos penales sobre responsabilidad penal de entidades del sistema financiero por delitos informáticos; **Abogada Huiza (2023)** señala que en el delito de fraude informático respecto a las entidades financieras en el Perú, se ha logrado identificar responsabilidad penal por participación directa en el delito o por facilitar intencionalmente su comisión. Asimismo, se ha establecido responsabilidad por omisión cuando la entidad financiera no implementa medidas de seguridad adecuadas para prevenir el fraude informático. Además, las entidades financieras pueden enfrentar sanciones administrativas y responsabilidad civil por los daños y perjuicios causados a los afectados.

Pregunta 06: ¿Considera Ud. que las entidades financieras tienen identificados los riesgos de los sistemas de seguridad financiero?

Jueces: Abogada Ocares (2023) señala que considera que si se tienen identificados, las distintas formas que afectan la seguridad financiera, por ello implementan, sistemas de seguridad informática, para los casos que ya se conocen como el ***pharming, phishing,*** del cual se desprende el ***"smishing***", que es otra modalidad de robar información y dinero a través de mensajes de texto; entonces podemos deducir que siempre se están creando nuevas modalidades de fraude informático, por lo que es responsabilidad de las entidades financieras ir a la par, con una actualización permanente de sus sistemas de seguridad a fin de identificar estas nuevas formas de fraude y neutralizar su ejecución**, Mg. Castañeda (2023)** considera que sí; **Abogado La Rosa (2023)** señala que frente a la creciente delincuencia cibernética, amplia y diversificada, los riesgos deben ser asumidos por el sistema de seguridad financiera con mayor especialidad y logística. Están en proceso. **Fiscales: Abogado Paucar (2023)** indica que aún no se ha regulado, ni reglamentado un sistema de prevención; **Abogado Portillo (2023)** señala que estima que sí bien las empresas bancarias tienen sistemas de seguridad, no existen políticas adecuadas de cuidado y prevención, máxime si por el propio descuido o desorden interno se bajan estándares de seguridad para ocasionar mayores ganancias; **Abogada López (2023)** indica que cree que sí, porque las entidades financieras conocen los riesgos que corren, de que son vulnerables a que sus sistemas puedan ser interferidos por delincuentes cibernautas. **Abogados: Abogado Durand (2023)** indica que si tienen identificados sus riesgos, sin embargo a pesar de sus esfuerzos muchas veces son el personal que labora en dichas entidades bancarias los que están implicados en dichos delitos y en otros casos es falta de previsión; **Abogada Purizaca (2023)** señala que es probable que algunas entidades financieras del sistema financiero tengan identificados los riesgos de los sistemas de seguridad financiero mediante capacitaciones y exigencias de la SBS; **Abogada Huiza (2023)** señala que las entidades financieras en el Perú están conscientes de los riesgos asociados a los sistemas de seguridad financiera. Estas entidades suelen tener identificados los

riesgos y están comprometidas con la implementación de medidas adecuadas para mitigarlos. Las entidades financieras están sujetas a regulaciones y supervisión por parte de entidades como la Superintendencia de Banca, Seguros y AFP (SBS) para asegurar que se cumplan los estándares de seguridad y protección de datos. Sin embargo, es importante reconocer que los riesgos pueden evolucionar constantemente y requerir actualizaciones continuas en las medidas de seguridad.

Objetivo Especifico 02: Identificar los riesgos de los sistemas de seguridad financiero que incrementan las denuncias en el distrito fiscal Lima Centro 2022

Pregunta 07: ¿Cree Ud. que las entidades financieras utilizan sistemas de seguridad adecuados de control y seguimiento para evitar vulneraciones a la base de datos de sus usuarios?

Jueces: Abogada Ocares (2023) señala que de lo poco que se conoce, puesto que es información muy reservada, los sistemas de seguridad informático de los sistemas financieros, tratan de apaciguar, o dar frente a este problema actual, a fin de que sus usuarios no se vean afectados**, Mg. Castañeda (2023)** considera que no pues la frecuencia de la comisión de estos delitos en sistemas informáticos de entidades financieras es frecuente; **Abogado La Rosa (2023)** señala que es evidente la insuficiencia de los medios con que cuenta el sistema de seguridad para el control y seguimiento de esas acciones ilegales, las bases de datos de los usuarios son posibles de hackear para sustracción y disposición, en algunos casos debe evitarse.

Fiscales: Abogado Paucar (2023) indica que dichos sistemas de seguridad deben mejorarse; **Abogado Portillo (2023)** señala que estima que si existen dichas políticas de o sistemas de control, pero que las mismas tienen diferencias marcadas dentro de cada empresa del sistema financiero; **Abogada López (2023)** considera que sí, sin embargo, esos sistemas de seguridad tienen que ir de acorde al avance tecnológico, puesto que los delincuentes ciber náuticos adoptan cada vez más nuevas

formas de vulnerar los sistemas informáticos. **Abogados: Abogado Durand (2023)** indica que al parecer no, por cuanto muchas veces los mismos trabajadores son los que pasan los datos de los usuarios a los criminales; **Abogada Purizaca (2023)** señala que es probable que algunas entidades financieras tengan implementados sistemas de seguridad como el Compliance y certificaciones internacionales para fines relacionados; **Abogada Huiza (2023)** indica que si bien implementan medidas de seguridad tecnológicas, como firewalls, encriptación y sistemas de detección de intrusos, así como políticas y procedimientos internos para prevenir y responder a las vulneraciones de seguridad. Sin embargo, es importante destacar que la efectividad de estos sistemas puede depender de factores como la evolución de las amenazas cibernéticas y la capacidad de adaptación de las entidades financieras para mantenerse al día con las mejores prácticas de seguridad, por lo que considera que las entidades financieras no utilizan sistemas de seguridad adecuados.

Pregunta 08: ¿Considera Ud. que los sistemas de seguridad informático establecidos en la norma nacional e internacional son suficientes para salvaguardar la base de datos de las entidades financieras?

Jueces: Abogada Ocares (2023) señala que siempre están en constante desarrollo, y se rigen por la ley de la materia, tanto nacional como internacional, que pueden ser estandarizadas a través de la ISO 27001 u otras normas internacionales**, Mg. Castañeda (2023)** considera que deberían mejorarse; **Abogado La Rosa (2023)** señala que en materia informática los avances son exponenciales, y ante un medio de seguridad surgen nuevos dispositivos invasivos del sistema, por ello por ahora es mensurando tal avances ilícitos y generar nuevos y mejores controles. **Fiscales: Abogado Paucar (2023)** indica que debe implementarse un sistema de prevención con mayor articulación entre los operadores y el sector privado; **Abogado Portillo (2023)** señala que estima que deben existir mayores pautas o requerimientos de control a las entidades; **Abogada Lopez (2023)** indica que no, son suficientes porque estas deben ir cambiando de acorde a los avances y modalidades nuevas que los delincuentes cibernautas utilizan para vulnerar los sistemas informáticos. **Abogados:**

Abogado Durand (2023) indica que mientras más avance en la tecnología, más avanza la criminalidad, sin embargo en latino américa existe más incidencia de delitos informáticos y en Perú es donde más se han incrementado los casos, causando perjuicio económico a los usuarios y las entidades bancarias que tienen que devolver el dinero que se han retirado de las cuentas y también pagar multas por no haber cumplido con las medidas de seguridad establecidas; **Abogada Purizaca (2023)** señala que si bien existen sistemas de seguridad internacional y nacional, la practica denota que cada vez existen nuevas modalidades de vulneración de los sistemas de seguridad; por lo que los mecanismos necesitan ser adecuados y mejorados constantemente; **Abogada Huiza (2023)** considera que no, puesto que como se ha venido advirtiendo en los medios de comunicación y en las denuncias efectuadas tanto a nivel nacional como mundial los delitos informáticos han venido aumentando a lo largo del tiempo.

Pregunta 09: ¿Cree Ud. la vulneración de los sistemas de seguridad financiera son solo de responsabilidad del hacker o también les alcanzaría responsabilidad a las entidades bancarias?

Abogada Ocares (2023), señala que nuestro sistema penal peruano, establece responsabilidad penal, para quienes realicen actuaciones en contra de aquellos intereses protegidos dentro de un sistema establecido. Pero definitivamente alcanza responsabilidad a las entidades bancarias, en su condición de personas jurídicas cuyo quehacer es la prestación de un servicio al ciudadano**, Mg. Castañeda (2023)** opina que cree que hay responsabilidad de las entidades financieras; **Abogado La Rosa (2023)** señala que el hacker podría ser responsable penal a título de autor, mientras que las entidades financieras podrían ser responsables administrativas en este delito, sin perjuicio de la responsabilidad por daños y perjuicios. **Fiscales: Abogado Paucar (2023)** indica que la vulneración de los sistemas de seguridad puede darse tanto a nivel interno como externo; **Abogado Portillo (2023);** señala que estimo que si no existe el debido cuidado si debería considerarse responsabilidad de las empresas del sistema financiero; **Abogada López (2023)** indica que a las entidades financieras les compete mejor sus sistemas de seguridad financiera, utilizando la tecnología y la

ciencia, para evitar que sus clientes sean víctimas de la clonación de sus datos, y el robo de su dinero. **Abogados: Abogado Durand (2023)** indica que es algo discutible, por cuanto cada caso es específico no existe un patrón, en algunos podría alcanzar responsabilidad por los cuáles son sancionados con multas en casos administrativos, en algunos otros son víctimas de los hackers con millonarias pérdidas; **Abogada Purizaca (2023)** señala que existen acciones que deberían estar a cargo de las entidades bancarias tales como a anulación inmediata de operaciones no identificadas por el usuario, activación inmediata de mecanismos de verificación de la identidad del usuario, filtros de seguridad, determinación de tiempos para resolución de quejas y reclamos por fraude informático y hasta devolución de aportes por operaciones no autorizadas por usuarios donde no se haya demostrado que la entidad bancaria haya activado todos los mecanismos de seguridad y actuado con diligencia; **Abogada Huiza (2023)** indica que la responsabilidad por la vulneración de los sistemas de seguridad financiera en el Perú puede recaer tanto en los hackers como en las entidades bancarias, dependiendo de las circunstancias específicas del caso. En los hackers por su accionar directo al acceder de forma ilícita a información financiera y causar perjuicio a terceros y en las entidades financieras por incumplimiento de deber de implementación de medidas de seguridad o negligencia en el mantenimiento y actualización de sistemas

Pregunta 10:¿Cómo se puede evitar el delito de fraude informático?

Jueces: Abogada Ocares (2023), señala que a través de la implementación de mayores sistemas de seguridad en consonancia con las normas internacionales estandarizadas como las ISOS, también se puede evitar este tipo de delitos a través de una coordinación interinstitucional entre el Estado y la actividad financiera privada, en beneficio de la colectividad**, Mg. Castañeda (2023)** estima que los titulares de los sistemas informáticos, como las entidades financieras, deben poseer mejores sistemas de seguridad y, en su defecto, cubrir esas falencias con seguros que garanticen a los terceros usuarios cualquier daño ocasionado por este tipo de delitos; **Abogado La Rosa (2023)** señala que mejorando los mecanismos de prevención y control de las

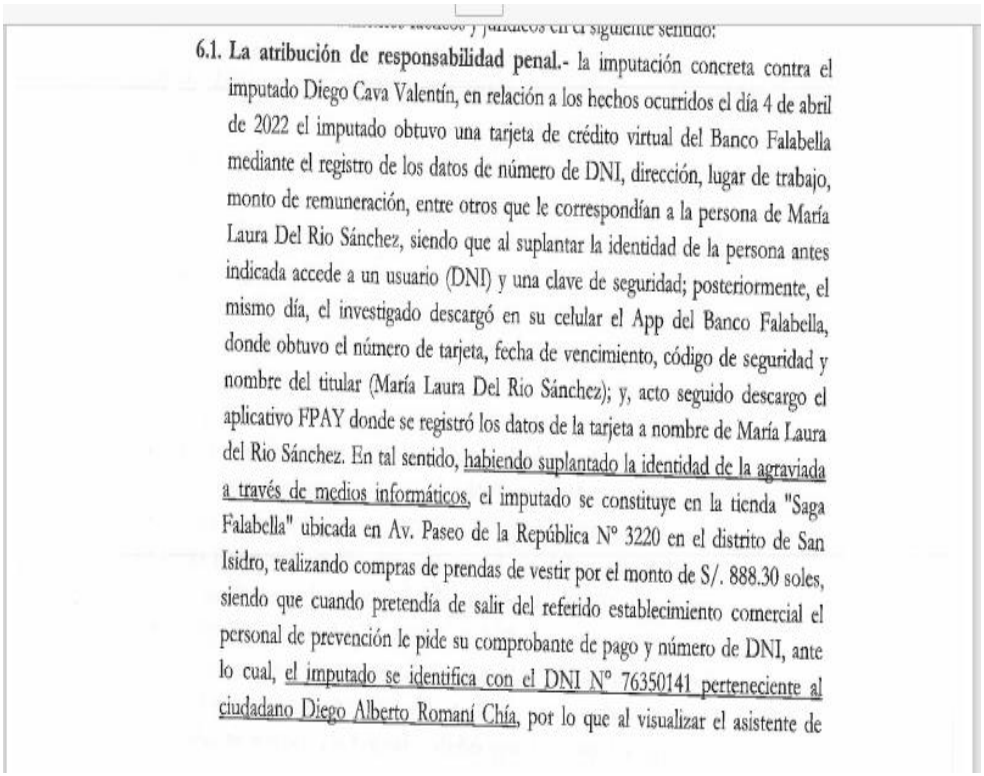
actividades riesgosas en el sistema financiero, especializando unidades técnicas como la DIVIAT – PNP y las fiscalías especializadas, educando al usuario en seguridad financiera. **Fiscales: Abogado Paucar (2023)** indica que se requiere de un plan nacional contra los delitos informáticos, dentro del mismo se debe implementar un sistema de prevención y una entidad que fiscalice y supervise su cumplimiento; **Abogado Portillo (2023)** señala que se debe aumentar las políticas de prevención y protección, mayores controles para la solicitud de cuentas y líneas telefónicas, otorgamiento de información real y oportuna de las empresas para el cumplimiento de la información y el registro de las IP, doblefactor de verificación y exigencia de control biométrico; **Abogada López (2023)** considera que compete al sector empresarial y financiero crear nuevas formas de protección de los datos de los usuarios del sistema financiero, utilizando técnicas de última generación para protección de datos. **Abogados: Abogado Durand (2023)** indica que una de las maneras es mayor difusión de este tipo de delitos a fin de que los usuarios no caigan en errores que permitan este tipo de delitos y en cuanto a las entidades bancarias mayor implementación con sus sistemas de seguridad; **Abogada Purizaca (2023)** señala que mediante la implementación de suficientes programas de cumplimiento normativo, certificaciones internacionales, supervisión y auditoria constante, implementación de procesos ágiles para la atención de quejas y reclamos por delitos informáticos, etc.; **Abogada Huiza (2023)** señala que los usuarios deben utilizar sistemas de seguridad adecuados y las entidades deben mantener actualizados los sistemas operativos y aplicaciones para evitar vulnerabilidades, se debe capacitar a los usuarios y entidades sobre mejores prácticas en seguridad cibernética, así como implementar políticas y procedimientos en materia de seguridad de la información, asimismo deben llevar a cabo auditorías de seguridad informática, mantenerse actualizado en las normas y cumplir con los estándares establecidos por los órganos regulatorios competentes, contar con planes de contingencia y de respuesta frente a incidentes de vulneración de seguridad y realizar monitoreo y detección de actividades sospechosas.

Según Arias (2022) señala que el análisis documental viene hacer la revisión de los documentos con la finalidad de obtener datos para la presentación de resultados.

Análisis documental: Relacionado al objetivo general: Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022

Expediente N° 02207-2022-1-1826-JR-PE-24

Sentencia Anticipada



fácticos en el siguiente sentido:

6.1. La atribución de responsabilidad penal.- la imputación concreta contra el imputado Diego Cava Valentín, en relación a los hechos ocurridos el día 4 de abril de 2022 el imputado obtuvo una tarjeta de crédito virtual del Banco Falabella mediante el registro de los datos de número de DNI, dirección, lugar de trabajo, monto de remuneración, entre otros que le correspondían a la persona de María Laura Del Rio Sánchez, siendo que al suplantar la identidad de la persona antes indicada accede a un usuario (DNI) y una clave de seguridad; posteriormente, el mismo día, el investigado descargó en su celular el App del Banco Falabella, donde obtuvo el número de tarjeta, fecha de vencimiento, código de seguridad y nombre del titular (María Laura Del Rio Sánchez); y, acto seguido descargo el aplicativo FPAY donde se registró los datos de la tarjeta a nombre de María Laura del Rio Sánchez. En tal sentido, habiendo suplantado la identidad de la agraviada a través de medios informáticos, el imputado se constituye en la tienda "Saga Falabella" ubicada en Av. Paseo de la República N° 3220 en el distrito de San Isidro, realizando compras de prendas de vestir por el monto de S/. 888.30 soles, siendo que cuando pretendía de salir del referido establecimiento comercial el personal de prevención le pide su comprobante de pago y número de DNI, ante lo cual, el imputado se identifica con el DNI N° 76350141 perteneciente al ciudadano Diego Alberto Romaní Chía, por lo que al visualizar el asistente de

Del análisis a la sentencia se aprecia en el considerando sexto, numeral 6.1 que el imputado logra obtener una tarjeta de crédito virtual del Banco Falabella mediante la suplantación a través de los medios informáticos de la persona de Laura del Río Sánchez, de la cual registra sus datos personales y otros, recibiendo así un usuario y clave, con el cual ingreso a través de la app del Banco Falabella y posteriormente realiza compras de prendas de vestir y otros, sin embargo al momento que pretende comprar un celular es que es descubierto y aprehendido. Dicho documento se relaciona con el objetivo general, toda vez que se sanciona a una persona por la vulneración de los sistemas de seguridad a fin de obtener un provecho patrimonial.

Expediente: 00382-2023-0-1815-JR-PE-02

Sentencia de Terminación Anticipada

SEXTO: Hechos imputados

En el presente caso se imputa a la persona de Edgar Guillermo Santa Cruz Ferreyra: *"que de manera deliberada e ilegítimamente realizo la utilización de tarjetas de la Línea 1 del Metro Lima, que se detallan:*

N.°	*Número de tarjeta*
1	*12269187*
2	*12269174*
3	*13053752*
4	*12269186*
5	*12269172*
6	*12269188*
7	*12269184*
8	*12269169*
9	*12269170*
10	*12269185*

Las cuales son anómalas en su funcionamiento, *pues estas presentan datos adulterados, siendo que las 10 tarjetas se encontraban con estado EMITIDO, pero pese a ello, estas la primera recarga era de S/ 0.10 céntimos (monto no proporcional a las recargas efectuadas en el sistema de las tarjetas), aunado a ello presentaban saldos adulterados tipo 1 (menor a S/. 100 soles) y datos adulterados, además tenían en exceso la cantidad de pases permitidos en el torniquete del tren en una sola estación; adicional a ello, las tarjetas en el sistema figuraban con saldos de recarga sin que la misma se hayan realizado, figurando en tipo de transacción como ÚSO; finalmente se advierte que estas presentaban saldo, pero que este no fue recargado en los sistemas del Metro de Lima (ello según lo que se advierte de los vauchers de consulta en la administración de la estación*

En la presente Sentencia se analiza en el sexto considerando detalla que al imputado se le encontró usando tarjetas de la línea 1 del metro de Lima con datos y saldos adulterados, pues éstas no fueron recargadas en los sistemas del metro de Lima, obteniendo así un beneficio económico. Dicho accionar ilícito guarda relación con el objetivo, en tanto que al haberse acreditado la manipulación de los sistemas de seguridad se configuró el delito de fraude informático motivo por el cual fue sentenciado.

Relacionado al Objetivo Especifico 01: Evaluar si el delito de fraude informática regula responsabilidad penal de la entidad financiera en relación a los sistemas de

seguridad financiero del distrito fiscal Lima Centro 2022 – Resolución Final N° 2014-2016-/CC1.

45. Al respecto, el Banco se ha limitado a señalar **-sin presentar prueba que lo sustente-** que la segunda transacción (S/ 2 150,00) al dirigirse a una cuenta que se encontraba

9 Ver la Resolución Final N° 1311-2014/CC1 del 13 de noviembre de 2014.

10 Ver por ejemplo, la página web del BBVA Banco Continental S.A. la cual describe a la tarjeta de coordenadas como una herramienta que "contiene una serie de datos numéricos dispuestos en forma de coordenadas, por cada operación o ingreso que realices se te solicitará UNA COORDENADA en forma aleatoria para la autorización cuando el sistema te lo solicite". En: <<https://www.bbvacontinental.pe/meta/seguridad/>>.

11 Ver por ejemplo, la página web de Banco Internacional del Perú S.A.A. - Interbank. la cual señala respecto a la cave dinámica SMS lo siguiente: La Clave Dinámica SMS funciona únicamente para hacer operaciones a terceros desde la Banca por Internet. Para poder solicitar tu Clave Dinámica SMS deberás estar afiliado al servicio de Banca Celular ya que ahí llegarán estas claves por mensajes de texto. En <<http://www.interbank.com.pe/banca-celular-sms>>.

registrada como favorita por la denunciante no necesitaba el ingreso de la clave digital token para validar la misma; por lo tanto, vulneró los mecanismos de seguridad establecidos por el ordenamiento jurídico vigente al momento de los hechos al permitir indebidamente la mencionada transferencia.

46. A mayor abundamiento, este Colegido considera pertinente señalar que el mecanismo de seguridad impuesto por la norma tiene como finalidad evitar el fraude cibernético como, por ejemplo, el "Phishing" método utilizado por terceras personas para la obtención de datos e información sensible de las tarjetas de crédito, débito, clave *token*, clave de coordenadas o clave SMS, entre otros, de los consumidores, con el fin de realizar operaciones a través de internet.

47. En ese sentido, a vista de este Colegiado, el ingreso de las referidas claves como mecanismo de seguridad, cobra mayor relevancia para la realización de cada una de las transacciones a través de Banca electrónica, en tanto protege al cliente que con la información sensible obtenida se realicen consecutivas operaciones.

48. Por todo lo expuesto, esta Comisión considera que corresponde confirmar la Resolución Final N° 870-2015/PS2 que declaró fundada la denuncia en el extremo referido a la transacción no reconocida por el monto de S/ 2 150,00, en tanto el Banco permitió indebidamente la realización de la mencionada operación.

49. Asimismo, corresponde revocar la Resolución Final N° 870-2015/PS2, que declaró fundada la denuncia contra el Banco en el extremo referido a la transacción no reconocida por el monto de S/ 4 600,00; y reformándola, declararla infundada, en tanto quedó acreditado que la entidad financiera cumplió con observar los mecanismos de seguridad respectivos para la realización de dicha transacción.

Del análisis realizado a la Resolución N° 2014-2016/CC1 de fecha 28 de setiembre de 2016 se desprende de los considerandos 45 a 49 se señala que el mecanismo de seguridad establecido en la norma evita el fraude cibernético, por lo

tanto el ingreso de las claves como mecanismo de seguridad es indispensable para la realización de las transacciones a través de la banca electrónica y como tal se protege al cliente, por lo que al indicar el banco que no se requería de la clave token para validar la operación de transferencia de la cuenta del denunciante, ello da lugar a que se permita que se realice la transferencia, vulnerando así los mecanismos de seguridad señalados en la norma, por consiguiente le acarrea responsabilidad a la institución bancaria; en ese sentido se puede advertir que el delito de fraude informático si repercute en los sistemas de seguridad, toda vez que sanciona con responsabilidad a las entidades financieras por la vulneración de los sistemas de seguridad de la base de datos reservada y confidencial de los clientes, por la falta de medidas de seguridad al momento de las transferencias.

Objetivo Especifico 02: Identificar los riesgos de los sistemas de seguridad financiero que incrementan las denuncias en el distrito fiscal Lima Centro 2022 – RN. N° 206-2019

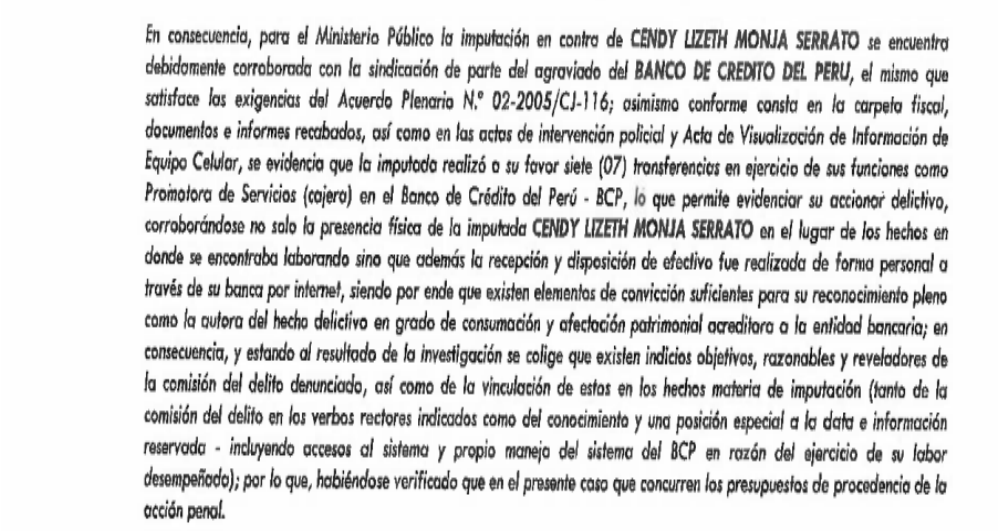
2.11. Además, debe tenerse en cuenta que el delito materia de imputación es el de AID, relacionado a la comisión de delitos de contenido patrimonial y de alta complejidad mediante el uso de la tecnología informática, puesto que según los hechos atribuidos los procesados lograron obtener el número de las tarjetas bancarias a través de la creación de una página web que emulaba una verdadera, técnica conocida como "Phishing" o también denominada "Phishing bancario" mediante la cual se simula la página web de una entidad bancaria para lograr la obtención del número de tarjetas y claves de seguridad, es por tanto la actuación de una asociación de cibercriminales.

2.12. En el caso en concreto, existió la aceptación de cargos del encausado, y el monto fijado por el Colegiado Superior, desconociendo la pretensión del procurador habilitado para solicitar la reparación civil no guarda relación directa con la dimensión de la afectación: por tanto, sobre la base de este criterio y teniendo en cuenta que la procuraduría propuso su pretensión a tiempo, el monto de reparación civil debe ser incrementado, en consonancia con el acuerdo plenario referido en el uno punto siete del SN, aunque no a la dimensión solicitada por la parte legitimada, resultando adecuada la suma de veinte mil soles[4].

2.13. Además, debe tenerse en cuenta que es línea pacifica en la jurisprudencia de esta Instancia Suprema la imposición de reparación civil en los delitos de peligro, como se recoge en el Recurso de Nulidad N.º 1895-2016-Callao, del treinta de mayo de dos mil diecisiete, en cuyo fundamento tres punto cuatro se reconoce que existen daños a la sociedad que no pueden ser viables de cuantificar, por lo que cabe de que la reparación se determine objetivamente en consideración a "la gravedad del delito", su trascendencia y de tal forma que no resulte un monto ínfimo.

Sentencia de Nulidad que señala en los considerandos 2.11 al 2.13 que los procesados lograron obtener el número de las tarjetas bancarias y claves de seguridad mediante la creación de una página web que simulaba una real de una entidad bancaria.

Expediente: 05384-2022-2-1826-JR-PE-22



En consecuencia, para el Ministerio Público la imputación en contra de **CENDY LIZETH MONJA SERRATO** *se encuentra debidamente corroborada con la sindicación de parte del agraviado del* **BANCO DE CREDITO DEL PERU**, *el mismo que satisface las exigencias del Acuerdo Plenario N.° 02-2005/CJ-116; asimismo conforme consta en la carpeta fiscal, documentos e informes recabados, así como en las actas de intervención policial y Acta de Visualización de Información de Equipo Celular, se evidencia que la imputada realizó a su favor siete (07) transferencias en ejercicio de sus funciones como Promotora de Servicios (cajera) en el Banco de Crédito del Perú - BCP, lo que permite evidenciar su accionar delictivo, corroborándose no solo la presencia física de la imputada* **CENDY LIZETH MONJA SERRATO** *en el lugar de los hechos en donde se encontraba laborando sino que además la recepción y disposición de efectivo fue realizada de forma personal a través de su banca por internet, siendo por ende que existen elementos de convicción suficientes para su reconocimiento pleno como la autora del hecho delictivo en grado de consumación y afectación patrimonial acreditara a la entidad bancaria; en consecuencia, y estando al resultado de la investigación se colige que existen indicios objetivos, razonables y reveladores de la comisión del delito denunciado, así como de la vinculación de estos en los hechos materia de imputación (tanto de la comisión del delito en los verbos rectores indicados como del conocimiento y una posición especial a la data e información reservada - incluyendo accesos al sistema y propio manejo del sistema del BCP en razón del ejercicio de su labor desempeñado); por lo que, habiéndose verificado que en el presente caso que concurren los presupuestos de procedencia de la acción penal.*

De la Sentencia se verifica que en el numeral 1.5, literal b) segundo párrafo, el Juez señala que la imputada en ejercicio de sus funciones realizó la recepción y disposición de efectivo de manera personal a través de su banca por internet, ello en virtud a su especial posición de trabajadora del banco con acceso a la data e información reservada. En ese sentido, se puede advertir que los riesgos también se dan también por parte de los propios trabajadores de las entidades financieras, quienes, contando debido a su propio cargo con los accesos a la información reservada de los clientes, logran manipular los sistemas de seguridad y obtener un provecho patrimonial en perjuicio de los usuarios y de la propia entidad bancaria.

4.2 Discusión

4.2.1 ***Objetivo general:*** *Analizar de qué manera el tratamiento del* ***delito de fraude informático*** *repercute en* ***los sistemas de seguridad financiero*** *que incrementa las denuncias, distrito fiscal Lima Centro 2022.*

Del análisis de las entrevistas a los jueces, fiscales y abogados se puede determinar que si bien el tratamiento del delito de Fraude Informático, no regula expresamente la responsabilidad penal de la persona jurídica, sin embargo si causa efecto en la debida implementación de sistemas de seguridad de la data informática por parte de las entidades financieras, toda vez que de no ser así, son pasibles de ser sancionadas conforme a lo establecido en el artículo 105 del Código Penal y las demás normas administrativas y/o civil. De otro lado, se puede señalar que solo un juez y un fiscal han coincidido que las entidades financieras podrían tener responsabilidad penal en los casos del actuar por otro, por omisión de implementación de medidas de seguridad o por beneficio obtenido por medio del fraude.

Saltos et. al (2021) señala que la utilización de las actuales tecnologías facilita la producción de perjuicios imprudentes en los sistemas informáticos, accesos ilícitos, ataques cibernéticos, puesto que en la actualidad se puede cometer un delito por medio de las tecnologías de la información.

Además, respecto al análisis documental se puede decir que, si repercute el delito de fraude informático en los sistemas de seguridad financiero, toda vez que conforme la Resolución Final N° 2014-2016-/CC1 se advierte que debido a la falta de diligencia en la idoneidad de los sistemas de seguridad para la utilización de un servicio a través de un aplicativo utilizado en una plataforma de internet le acarrea responsabilidad y puede ser pasible de sanción la entidad financiera, toda vez que al brindar dicho servicio tiene la obligación de implementar el mecanismo de seguridad impuesto por la norma, lo cual evita el fraude informático. Asimismo, ello también se ve evidenciado en la Sentencia Anticipada del Expediente: 02207-2022-1-1826-JR-PE-24, en la que el Juez sanciona con una pena privativa de libertad suspendida, al imputado por haber obtenido una tarjeta de crédito virtual a nombre de una tercera persona utilizando para ello sus datos personales y a través de la plataforma de internet (FPAY) logra realizar compras, pues dicho accionar ilícito fue realizado a través de la vulneración de los sistemas de seguridad de la información reservada, por lo tanto la conducta descrita en el delito de fraude informático si produce efectos jurídicos, en tanto que ello permite que las entidades financieras cumplan con implementar un debido sistema de seguridad, monitoreo y prevención de riesgos, a fin

de que no incurran en responsabilidad y se evite la intrusión de terceras personas en su base de datos reservados de sus clientes.

El objeto de la acción del delito informático viene hacer la comunicación electrónica que no es otra cosa que la transmisión de datos a través de la red informática e incluso el acceso a la data almacenada en el sistema, lo cual es tutelado a través de la norma penal.

Cherniavskyi, Babanina, Viktoria, Mykytchyk y Mostepaniuk (2021) concluyen que para combatir las amenazas cibernéticas es necesario garantizar la seguridad de la información, y para ello es necesario trabajar en el desarrollo de herramientas efectivas que eviten las vulneraciones.

Nieto et. Al (2023) en su artículo concluye que la pandemia ha dado lugar el uso de los medios tecnológicos por medio de la red de internet, lo cual ha generado que sea aprovechada por los ciberdelincuentes, quiénes a través de correos electrónicos (phishing) logran acceder a la información de la víctima a fin de beneficiarse económicamente, por ello señala que es necesario que se capacite a los usuarios a fin de evitar riesgos y vulneraciones a sus sistemas informáticos.

Fernandez (2018) en su artículo son útiles las TIC para combatir la ciberdelincuencia concluye que la utilización de las tecnologías de información y debida coordinación entre las dependencias policiales ha dado lugar a que se pueda disuadir a los ciber delincuentes que cometen delitos informáticos.

Vinelli (2021) señala que el convenio de Budapest ya cuenta con más de veinte años desde su firma, y que ante la aparición constante de distintas modalidades de delitos informáticos es necesario que se elabore una nueva normativa internacional. Asimismo señala que considera que el delito de fraude informático viene hacer una modalidad del delito de estafa.

Ahora bien, a mi criterio de acuerdo al análisis documental puede señalarse que el delito de fraude informático si repercute en los sistemas de seguridad financiera, es decir que causa un efecto de prevención, toda vez que da lugar a la reducción de las vulneraciones del sistema de seguridad de la información, porque en cada proceso penal que se investiga conforme a la conducta desplegada por el autor del delito se describe el tipo de afectación del sistema de seguridad de la información, lo cual

conlleva a que las entidades financieras busquen que contar con un mejor sistema de seguridad o en la medida posible prevengan las vulneraciones a dichos sistemas, así como implementen medidas de prevención de riesgos y monitoreo constante en el correcto funcionamiento de su parque informático que brinda la seguridad informática de la base de datos almacenadas en su sistema, a fin de evitar un uso no autorizado por parte de terceras personas de la información almacenadas en un sistema de data informática.

Dicho resultado de la repercusión del delito de fraude informático es igual a la teoría sustentada por Aboso (2015) quien señala que la actual norma pone un alto a las conductas delictivas cometidas a través de la red informática, sin embargo agrega que en adelante es necesario que se reglamente otras formas de crímenes de ciber delincuencia, asimismo Anguita (2018) señala que a pesar de que se ha tratado de mitigar el incremento de los delitos informáticos en la Unión Europea, aún existen varios obstáculos que superar, entre otros la utilización del sistema de internet que es a nivel mundial y la capacitación adecuada del personal judicial y policial y Alcíbar et. al (2018) en su artículo concluyen que es necesario que los fiscales y policías se especialicen en técnicas de investigación de los ciberdelitos; de otra parte López (2022) señala que las entidades bancarias no cuentan con instrumentos de ciberseguridad, ni tampoco conocen como actuar ante los avances tecnológicos, además que la voluntad de proteger su data es mínima, lo cual es ratificado por el documento Resolución Final N° 2014-2016-/CC1 y la Sentencia Anticipada del Expediente: 02207-2022-1-1826-JR-PE-24.

Objetivo Especifico 01: Evaluar si el delito de fraude informática regula responsabilidad penal de la entidad financiera en relación a los sistemas de seguridad financiero del distrito fiscal Lima Centro 2022.

De las entrevistas a los jueces, fiscales y abogados estos señalan que el delito de fraude informático no establece responsabilidad penal a las entidades financieras sino solo se ha podido establecer responsabilidad administrativa o civil, sin embargo, solo hay un fiscal y un abogado que ha indicado que si se puede establecer

responsabilidad penal en las entidades financieras en el caso de que se evidencia fallas en la política de seguridad y si se demuestra la participación o facilitación en la conducta delictiva.

El delito informático se configura con la manipulación del sistema informático a fin de transferir fondos de una tercera persona a una cuenta propia o de otra persona, obteniendo así un beneficio económico.

El delito informático es realizado por una serie de personas con reparto de roles, de las cuales en muchos casos es difícil de identificar y ubicar, que pueden incluso trascender trasnacionalmente.

Imputación penal a la empresa, es la atribución de un delito a una persona jurídica ya sea por heteroresponsbilidad, autorresponsabilidad o mixta, en tanto que resultan insuficientes las sanciones aplicadas a los sujetos que la representan o el uso de sanciones administrativas y/o reparatorias. (Bramont-Arias, 2021)

Compliance viene hacer el cumplimiento de las leyes financieras, administrativas y comerciales a fin de evitar la comisión de eventos delictivos, siendo pasibles de ser sancionados penalmente por la falta de implementación de los mismos. (Bernate, 2018)

Carrión (2020) señala que la Ley N° 30424 no cambia el societas delinquere non potest, sino continua pues no se vulneran el principio penal de la *culpabilidad* ni el de acción u omisión que es innato a la persona natural.

Castro & Díaz-Rincón (2020) señala que la comisión de un delito evidencia que el ente colectivo transgrede su deber, es decir la relación de la obligación que genera el delito penal, lo cual vulnera bienes jurídicos protegidos y que debe ser regulado en la norma penal como posición definitiva de la punibilidad de la pena de las personas jurídicas, ello a fin de brindar seguridad jurídica a la ciudadanía. Agrega además que el dolo y la imprudencia deben ser normativizados como requisitos de la punibilidad.

Villavicencio (2014) señala que en el Perú no se puede comprender como sujeto activo a la persona jurídica debido al principio societas delinquere non potest, pero se cuenta con normas en el Código Penal sobre sanciones accesorias como es

el Artículo 105 y el actuar por otro artículo 27 y las normas adjetivas del Código Procesal Penal.

En nuestro país no se encuentra regulado la responsabilidad penal de las personas jurídicas, ni las penas para éstas, toda vez que no existe un concepto penal respecto a la persona jurídica o un modelo de imputación objetiva penal, pues cada vez con el avance tecnológico es más necesario la creación de un derecho penal empresarial, con lo cual se incremente el reproche y eficacia del derecho penal.

Ahora bien, en cuanto al análisis documental lo señalado por la mayoría de jueces, fiscales y abogados se condice con lo resuelto en la Resolución Final N° 2014-2016-/CC1 en la cual se sanciona administrativamente a una entidad financiera por la falta de adecuada implementación de sistema de seguridad en las transacciones electrónicas.

Asimismo, dicho resultado de la falta de regulación en el delito de fraude informático de responsabilidad penal de las entidades financieras, coincide con la teoría sustentada por Abanto (2015) quien sostiene que si la norma penal, no lo establece expresamente, no se puede atribuir una responsabilidad penal a la persona jurídica, lo cual también coincide con Vásquez (2022) quien señala que es necesario implementar alternativas de tipificación de conductas delictivas, asimismo Ochoa (2021) señala que las normativas no son suficientes, lo que motiva que las empresas hagan uso de sus bases de datos sin control, por ello es necesario que se regule la protección de datos y Carrera (2021) señala que la falta de conocimiento, capacidad operativa, carga procesal y falta de aplicación normativa genera que no se logre identificar al autor del delito e ineficacia en la investigación del delito.

Por mi parte puedo señalar que de las respuestas de los entrevistados y de los documentos analizados se aprecia que a nivel fiscal y judicial no se realiza una evaluación adecuada de la imputación objetiva, pues en su mayoría de los casos se resuelve teniendo en cuenta la teoría de Gunther Jakobs, es decir orientada a conductas neutrales (Reyna, 2022). Asimismo no se efectúa una aplicación sistemática de las normas en el análisis de los hechos del accionar ilícito investigado, pues solo se evalúa la conducta típica realizada por el autor del delito, sin verificarse si le alcanza responsabilidad penal, administrativa o civil en la persona jurídica que brinda el

servicio, ello debido a una falta de cumplimiento de las normativas relacionadas a la seguridad de la información de los usuarios o por interés propio del representante de la entidad bancaria, puesto que existen normativas que obligan a las entidades financieras a contar con sistemas de seguridad adecuados y programas de prevención de riesgos y ante la falta de implementación son pasibles de ser sancionadas. A mi criterio si se realiza una adecuada investigación podría determinarse el tipo de responsabilidad penal en que estaría inmersa la persona jurídica, toda vez que el riesgo tecnológico es compartido entre el banco y el usuario. Asimismo cabe mencionar que en el Perú solo se ha regulado mediante la Ley N° 30424 y sus modificatorias, la responsabilidad administrativa de las personas jurídicas a través de un proceso penal por los delitos cohecho, lavado de activos y financiamiento del terrorismo, motivo por el cual en los casos investigados no se analiza la responsabilidad penal de las entidades financieras, lo cual da lugar a que se deje de lado la posibilidad de identificar si la conducta típica del delito de fraude informático fue realizada por una falla de parte de la entidad financiera o de parte del representante legal de la entidad financiera pues este viene hacer una persona natural, a cargo de su dirección, así como es el responsable de la infracción de deberes organizativos, y quien debe responder por el delito cometido; asimismo conforme a las sentencias analizadas se aprecia que no se llega a investigar adecuadamente sino solo se investiga la conducta del sujeto activo que en muchos casos acepta el delito y logra una sentencia con un beneficio quedando el proceso concluido, y de esta manera no se logra ir más allá, a fin de evidenciar si el representante de la persona jurídica observó el cumplimiento de las normas y como tal contaba con una adecuada prevención de riesgos, ello en la medida que existe una conexión entre el representante y la persona jurídica y éste no previno el delito por defecto o falla estructural organizativo o de control.

Asimismo, se puede señalar que las entidades bancarias si pueden ser pasibles de responsabilidad penal, pero a través de sus representantes, toda vez que los mismos actúan en representación de la persona jurídica y puede participar de esa manera en la comisión de un delito en beneficio de la entidad bancaria, ya sea porque no cumplió con las normas establecidas para la implementación de sistemas de

seguridad, la falta de idoneidad de los bienes y servicios que se ofrece a los consumidores sobre transferencia a través de los canales electrónicos. Así como se debe tener en cuenta las regulaciones existentes en otros países como en el caso del país de Chile que si existe la Ley N° 20.393 que regula la responsabilidad penal de las personas jurídicas, por defecto organizacional, sin embargo, doctrinariamente se ha aplicado en base a las reglas de compliance y en España con la Ley Orgánica 5/2010 modificada por la LO 1/2015 que sanciona por delitos realizados por sus representantes legales o por la comisión del delito de un sujeto bajo la autoridad del representante legal. (Bedecarratz, 2020), lo cual también es señalado por Fernández (2019) quien precisa que la activación de la conexión se da cuando el delito ha sido realizado por cuenta de la persona jurídica a través de la persona natural en favor directo o indirecto del ente colectivo.

Objetivo Especifico 02: Identificar los riesgos de los sistemas de seguridad financiero que incrementan las denuncias en el distrito fiscal Lima Centro 2022

Por lo tanto, de las entrevistas y documentos analizados las entidades financieras no tienen identificados los riesgos de los sistemas de seguridad financiero, toda vez que conforme a las respuestas de los jueces, fiscales y abogados si bien cuentan las entidades financieras cuentan con sistemas de seguridad, estas no son suficientes y adecuadas para mitigar la vulneración de la seguridad informática de la base de datos de los usuarios, ello en virtud a los avances tecnológicos, la insuficiencia del marco normativo respecto a la salvaguarda de la protección de datos y la falta de cumplimiento de la norma por parte de las entidades bancarias sobre implementación y aplicación de los sistemas de seguridad de la información. Resultado que coincide con la postura de Mansilla (2020) quien señala que el Perú no cuenta con un reglamento que regule la gestión de riesgos digitales, motivo por el cual se requiere un programa de cumplimiento de ciberseguridad y lo cual es ratificado por el documento Sentencia por Terminación Anticipada Expediente N° 05384-2022-2-1826-JR-PE-22 en donde se sanciona con una condena a la trabajadora de una entidad bancaria que realizó transferencias de dinero desde las cuentas bancarias que maneja la institución

a su propia cuenta, utilizando las claves de acceso que se le confiaron, con lo cual se denota que no existía un programa de prevención de riesgos en los sistemas de seguridad financiero a fin de poder detectar este tipo de conductas ilícitas y evitar un perjuicio patrimonial al usuario, asimismo ello también coincide con el documento RN. N° 206-2019, en el que se condena a una persona que usó una página web similar a la real de una entidad bancaria, para obtener el número de tarjeta bancaria y clave de un usuario, con lo cual se evidencia las deficiencias que existen en los sistemas de seguridad de la información de las entidades bancarias. De otro parte De Maglie (2005) señala que en los Estados Unidos las sentencias se basan en un enfoque retributivo, preventivo y disuasorio, lo cual debe ser aplicado también en nuestro país a fin de evitar impunidades y falta de cumplimiento de deberes por parte de las entidades financieras.

V. CONCLUSIONES

1. Se puede concluir de las entrevistas y el análisis documental que el delito de fraude informático si repercute en los sistemas de seguridad, toda vez que guarda una relación directa con la criminalidad financiera, así como se ha podido verificar que en nuestro país se sanciona al sujeto activo que vulnera los sistemas de seguridad por la manipulación de programas de seguridad informática a fin de obtener la data reservada de los usuarios de una entidad financiera y de esta manera beneficiarse económicamente así mismo o a favor de terceros, accionar ilícito que también puede haberse realizado con conocimiento de la propia institución financiera (a fin de beneficiarla) o sin el consentimiento de ésta, toda vez que dicha conducta se encuentra tipificada en el artículo 8 de la Ley N.° 30096, sin embargo respecto a los sistemas de seguridad financiera existe un vacío legal, pues no existe una normativa que regule específicamente sanción penal alguna por la inadecuada implementación de las mismas.

2. Se concluye que la norma no establece responsabilidad penal de las entidades bancarias, sino solo se sanciona con responsabilidad administrativa o civil, debido a la falta de conocimiento de las normas conexas del delito de fraude informático por parte de la policía nacional, fiscales y jueces, así como la insuficiente normativa que regule adecuadamente sobre los casos en que puede incurrir en responsabilidad penal las entidades bancarias, es decir existen vacíos de punibilidad. Cabe señalar que la norma solo regula sanciones administrativas y civiles, las misma que a la fecha son insuficientes y no producen un verdadero reproche y política de prevención de delitos hacia los usuarios. Asimismo, en el Perú solo se ha normado a través de la Ley N° 30424 responsabilidad administrativa de las personas jurídicas a través de un proceso penal por delitos de cohecho, lavado de activos y financiamiento de terrorismo, lo cual da lugar a que no se llegue a determinar en sí la responsabilidad penal de la persona jurídica que puede darse por falla propia de la persona jurídica o

por el representante legal de dicha entidad a cargo de su dirección en beneficio propio o de terceros.

3. Se concluye que las entidades financieras no tienen del todo, debidamente identificados los riesgos de sus sistemas de seguridad de la información, en tanto que si bien existe normativa administrativa que regula los requisitos que debe cumplir las entidades bancarias sobre sistemas de seguridad informática y de protección de datos, también es cierto que estos no se encuentran actualizados conforme al avance tecnológico que utilizan los sujetos activos del delito, así como no existe una entidad que realice el control de prevención de riesgos que las entidades bancarias deberían utilizar obligatoriamente a fin de evitar vulneraciones a sus sistemas informáticos donde almacenan la data reservada de los usuarios. Existen vacíos normativos respecto a la debida implementación de la gestión de riesgos digitales bajo un programa de cumplimiento de ciberseguridad, ello a fin de evitar posibles vulneraciones a los sistemas de seguridad de información de las entidades financieras.

VI. RECOMENDACIONES

1. Se recomienda que el Ministerio Publico en coordinación con la Policía Nacional, el Poder Judicial y el Ministerio de Justicia y Derechos Humanos realicen capacitaciones al personal integrante de cada institución sobre la normatividad aplicable a los delitos informáticos, especialmente de Fraude Informático tanto nacional como internacional, a fin de que puedan resolver con un mejor análisis sistemático de las normas.
2. Se recomienda que los fiscales del Ministerio Público realicen propuestas y modificaciones legislativas de las normas relativas a la responsabilidad penal de las entidades financieras por el delito de Fraude Informático y de la implementación de sistemas de seguridad informática y de protección de datos.
3. Se recomienda que el Ministerio Público proponga la creación de un organismo que realice el control y monitoreo de la implementación de gestión de riesgos en las entidades financieras a fin de evitar la vulneración continua y permanente de los sistemas de seguridad financiero y de la protección de datos.

REFERENCIA

Abanto, M. (2015) Dogmática Penal de Derecho Penal Económico y Política Criminal, Responsabilidad penal de los entes colectivos: Estado actual y reflexiones preliminares. Tomo I, Segunda edición, Gaceta Jurídica.

Aboso, G. (2015) Dogmática Penal de Derecho Penal Económico y Política Criminal, La nueva regulación de los llamados “delitos informáticos” en el Código Penal Argentino: Un estudio comparado. Tomo I, Segunda edición, Gaceta Jurídica.

Acosta, G. & Benavides, M. & García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. Revista Venezolana de Gerencia, 25(89),351-368. https://www.redalyc.org/articulo.oa?id=29062641023

Alcívar C., Blanc G., y Calderón J. (2018). Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidad. http://www.revistaespacios.com/a18v39n42/a18v39n42p15.pdf. Obtenido de http://www.revistaespacios.com/a18v39n42/a18v39n42p15.pd

Anguita, J. (2018). Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea. Revista de Estudios en Seguridad Internacional, Vol.4, No. 1,pp. 107-126. ISSN: 2444-6157. DOI: http://dx.doi.org/10.18847/1.7.7

Apolinario, D. (2022). Propuesta de creación de Centros de Respuesta a Incidentes de Seguridad Informática como Estrategia de Cyberseguridad para medios de pagos digitales. Tesis de grado, Universidad de Guayaquil, Lima.

Arias, M. y Giraldo, C. (2011). El rigor científico en la investigación cualitativa, Revista Redalyc, https://bit.ly/3h35I1B

Ayma, H. (2020). Delitos Informáticos y su relación con el proceso de investigación preliminar en el distrito fiscal de Lima Norte año 2019. Tesis de grado, Universidad Alas Peruanas, Lima.

Bedecarratz, F. (2020). Defecto de organización y reglas de comportamiento en la imputación de las personas jurídicas. En: https://www.scielo.cl/pdf/politcrim/v15n30/0718-3399-politcrim-15-30- 694.pd

Bernate, F. (2018). El compliance y la responsabilidad penal de las personas jurídicas en Colombia. Revista Jurídica Mario Alario D´Filippo, Colombia. En: https://doi.org/10.32997/2256-2796-vol.10-num.20-2018-2146

Bernal, C., (2010). Metodología de la Investigación para administración, economía, humanidades y ciencias sociales. (3° ed.). Bogotá: Pearson Educación.

Bramont-Arias, L. (2021). ¿La empresa como sujeto de derecho penal empresarial? En: https://repositorio.pucp.edu.pe/index/handle/123456789/182677

Bunge, M. La Ciencia su Método y su Filosofía. 1a. Ed. Buenos Aires: Siglo Veinte, 1960.

Cámara, S. (2020). La Cibercriminología y el perfil del ciberdelincuente. Derecho y Cambio Social, ISSN-e 2224-4131, Nº. 60, págs. 470-512.

Carrera, I. (2022). Deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021. Tesis de grado, Universidad César Vallejo, Lima.

Carrión, J. (2018). ¿Responsabilidad penal o administrativa de la persona jurídica? Algunos alcances a partir del Decreto Legislativo N°30424. En: https://revistas.urp.edu.pe/index.php/Inkarri/article/view/3693 Castro, J. y S. Díaz-Rincón (2020). Responsabilidad penal de las personas jurídica

Castro, J. y S. Díaz-Rincón (2020). Responsabilidad penal de las personas jurídicas en Colombia. En: https://webcache.googleusercontent.com/search?q=cache:90t-h4t7bZIJ:https://revistas.unisimon.edu.co/index.php/tejsociales/article/download/4748/4957&cd=1&hl=es-419&ct=clnk&gl=pe

Cevallos, Y., et al (2020) La interpretación extensiva y la analogía en los delitos de estafa con documento bancario. https://www.recimundo.com/index.php/es/article/view/774/1208

Cisneros, R. (2022). Factores de identificación del imputado de fraude informático en un despacho de la fiscalía de ciberdelincuencia, año 2021. Tesis de grado, Universidad César Vallejo, Lima.

Condori, R. (2020). Implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio distrito fiscal de Lima Norte 2020. Tesis de grado, Universidad César Vallejo, Lima.

Cherniavskyi, Babanina, Viktoria, Mykytchyk y Mostepaniuk (2021). Measures to combat cybercrime: analysis of international and Ukrainian experience. Recuperado de: https://doi.org/10.46398/cuestpol.3969.06

Choque, S. (2021). El uso de las TIC's y la comisión del delito de estafa en el distrito Judicial de Tacna, 2021. Tesis de grado, Universidad César Vallejo, Lima.

Cruz, J. (2021). Trabajo de Investigación para obtener el grado académico de Magíster en Gobierno y Políticas Públicas. Tesis de grado, Pontificia Universidad Católica del Perú, Lima.

De la Espirella y Gómez (2020), Metodología de investigación y lectura crítica, teoría fundamentada, http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0034-74502020000200127

De Maglie, C. (2005). Models of Corporate Criminal Liability in Comparative Law. En:https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1213&context=law_globalstudies

Ezequiel, L. (2019). Los delitos informáticos en el Código Penal Italiano- Computer crimes in the Italian Criminal Law. Obtenido de http://www.scielo.org.mx/pdf/dgedj/v5n14/2448-5136-dgedj-5-14-127.pd

Fernández, J. (2019). Responsabilidad penal de las personas jurídicas. El contenido de las obligaciones de supervisión, organización, vigilancia y control referidas en el art. 31 bis 1). b) del Código Penal Español. Revista Electrónica de Ciencia Penal y Criminología. En: http://criminet.ugr.es/recpc/21/recpc21- 03.pdf

Fernández, W., Vargas, C. (2018). Does ICT Curb Cybercrimes? The Association between Cybercrime Charges and the Police Station Technological Apparatus. https://doi.org/10.26512/lstr.v10i2.21492. https://www.aulavirtualusmp.pe/ojs/index.php/VJ/article/download/1718/172 6

Gioia, C. (2019). Metodología de análisis forense informático para la obtención de evidencia digital en base de datos. Tesis de grado, Universidad Nacional de la Matanza, Argentina.

Hernández, J. (2020). La responsabilidad de las entidades financieras por fraudes electrónicos. Tesis de grado, Universidad Pontificia Bolivariana.

Hernández, R. & Mendoza, C. (2018). Metodología de investigación. Las rutas cuantitativa, cualitativa y mixta. Mexico: Mc Graw Hill Education.

La ley N° 30096 (2013) ley de delitos Informáticos, https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

Lopez, J. y Rodriguez, M. (2022). La ciberseguridad en el diseño de productos financieros. Tesis de grado, Universidad Externado de Colombia, Colombia.

Mansilla, D. (2020). Implementación de Programas de cumplimiento en ciberseguridad como una práctica de buen gobierno corporativo en las entidades que forman parte del sistema financiero peruano. Tesis de grado, Pontificia Universidad Católica del Perú, Lima.

Mamani, M. (2022). Modelo de Sistema de gestión de la seguridad de la información en base a la norma ISO 27001 para entidades públicas. Tesis de grado, Universidad Mayor de San Andrés, Bolivia.

Mayer, L. & Oliver, G. (2020). El delito de fraude informático: concepto y delimitación. *Rev. chil. derecho tecnol.* [online]. 2020, vol.9, n.1, [citado 2023.05.07], pp.151-184. ISSN 0719-2584. https://www.scielo.cl/scielo.php?pid=S0719-25842020000100151&script=sci_abstract

Montalvo, C. (2022). Estándar de seguridad para la protección de datos de tarjetas de pago en las entidades financieras, Lima 2021. Tesis de grado, Universidad César Vallejo, Lima.

Ministerio de Justicia y Derechos Humanos (2022). Ciberdelincuencia, reporte de Información estadística y recomendaciones para la prevención, [citado el 2023.05.07],https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf

Nieto, G. et al (2023). El correo electrónico, como medio de intrusión del Phishing y fraude informático. Revista de Climatología, Vol.23, (2023): 1138-1148 ISSN 1578-8768. DOI: 10.59427/rcli/2023/v23cs.1138-1148

Novoa, D. (2022). Injusto penal de sistemas y datos informáticos en la transgresión del derecho a la intimidad en un juzgado unipersonal, 2022. Tesis de grado, Universidad César Vallejo, Lima.

Picoy (2020). Analfabetismo Digital en el Perú, [citado el 2023.05.07], https://sites.google.com/site/sistemasdeinformacionanto/APORTTES-ANTONIO-PICOY/analfabetismo-digital-en-per%C3%BA

Quispe, S. (2020). Factores que determinan el archivo de investigaciones por delito de Fraude informático en el Distrito Fiscal de la Libertad año 2019. Tesis de grado, Universidad César Vallejo, Lima.

Reyna, L. (2022) Código Penal del Bicentenario. Estudios de Derecho Penal Actual. Tomo II, Primera edición, Gaceta Jurídica.

Rodríguez, C. (2018). Metodología de clasificación de delitos informáticos en redes sociales su tipificación según las leyes del Ecuador, determinación de vacíos

legales y el proceso para propuesta de ley. Tesis de grado, Universidad Internacional Sek, Quito.

Roibón, M. (2019). La estafa informática en el Código Penal Argentino, Revista Pensamiento Penal, Argentina, recuperado de https://bit.ly/3jbQgTu

Romano, D. (2019). Análisis criminológicos de los ataques DDoS: una propuesta de Legge ferenda. Tesis de grado de doctor, Universidad Alcalá, España.

Saltos, M., Robalino, J., & Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. Revista Conrado, 17(78), 343-351.

Vara 2010, https://www.administracion.usmp.edu.pe/investigacion/files/7-PASOS-PARA-UNA-TESIS-EXITOSA-Desde-la-idea-inicial-hasta-la-sustentaci%C3%B3n.pdf

Vargas, W. (2022). Necesidad de tipificar la estafa básica en la Ley de Delitos Informáticos para reducir la impunidad en el Perú. Tesis de grado, Universidad César Vallejo, Lima.

Vasquez, A. (2022). Necesidad de incorporación de nuevas figuras delictivas informáticas en el Código Penal, 2021. Tesis de grado, Universidad César Vallejo, Lima.

Vásquez, L. (2021). La importancia de un estándar legal de prevención de los delitos cibernéticos que atentan contra la niñez y adolescencia. Tesis de grado, Universidad de los Hemisferios, Ecuador.

Vences, O. (2019). Penalización de los delitos informáticos. Tesis de grado, Universidad Autónoma del Estado de Morelos, México.

Villavicencio, F. (2014). Delitos Informáticos, Revista IUS ET VERITAS, N° 49, (2014): 284-304 ISSN 1995-2929. En: https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Vinelli Vereau, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. Ius Et Praxis, (53), 95-110. https://doi.org/10.26439/iusetpraxis2021.n053.4995

Wadha Abdullah, A; Somaya Al-Maadeed; Abdulghani Alii, A. y Muhammad Khuraam K. (2020). Comprehensive Review of Cybercrime Detection Techniques, IEEE Access, https://wlv.openrepository.com/bitstream/handle/2436/623411/Sadiq_Comprehensive_Review_of_Cybercrime_2020.pdf?sequence=6&isAllowed=y

Liao, Yl., Tsai, C. (2006). Análisis de las características de los delitos informáticos en Taiwán. En: Chen, H., Wang, FY., Yang, C.C., Zeng, D., Chau, M., Chang, K. (eds) Intelligence and Security Informatics. WISI 2006. Lecture Notes in Computer Science, vol 3917. Springer, Berlín, Heidelberg. https://doi.org/10.1007/11734628_6

Zevallos, O. (2020). Delitos informáticos: ¿Cuáles son los principales fraudes informáticos que se pueden cometer a través del E-Commerce?, Ius 360, https://ius360.com/delitos-informaticos-cuales-son-los-principales-fraudes-informaticos-que-se-pueden-cometer-a-traves-del-e-commerce-oscar-zevallos-prado/

ANEXOS

MATRIZ DE CATEGORIZACIÓN: Fraude Informático en los Sistemas de Seguridad Financiero, Distrito Fiscal de Lima Centro 2022

PROBLEMAS	OBJETIVOS	SUPUESTO	CATEGORÍA	SUBCATEGORÍA
¿De qué manera el tratamiento del delito de Fraude Informático repercute en los sistemas de seguridad financiero que incrementa las denuncias del distrito fiscal Lima Centro 2022?	Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022	El fraude informático en los sistemas de seguridad financiero incrementa denuncias, del distrito fiscal de Lima Centro 2022.	Fraude Informático.	Robo de datos Alterar o dar mal uso a sistemas o software
¿De qué manera el robo de datos informáticos disminuye con la utilización adecuada de la información de la base de datos de las entidades financieras del distrito fiscal Lima Centro 2022?	Evaluar si el delito de fraude informática regula responsabilidad penal de la entidad financiera en relación a los sistemas de seguridad financiero del distrito fiscal Lima Centro 2022	Le alcanza responsabilidad penal a la entidad financiera por delito de fraude informático del distrito fiscal de Lima Centro 2022.	Sistemas de Seguridad Financiero.	Utilización adecuada de información
¿Cómo la alteración de sistemas o software implican responsabilidad de la entidad financiera debido a la falta de respeto de los accesos de la información establecidos del distrito fiscal Lima Centro 2022?	Identificar los riesgos de los sistemas de seguridad financiero que incrementan las denuncias en el distrito fiscal Lima Centro 2022	Los riesgos en los sistemas de seguridad financiero inciden en el incremento de denuncias del distrito fiscal de Lima Centro 2022.	Sistema de Seguridad Financiero	Respeto de los accesos de la información establecidos.

PROGRAMA ACADÉMICO DE MAESTRIA EN DERECHO PENAL Y PROCESAL PENAL

CARTA DE PRESENTACIÓN

Lima, 05 de junio de 2023

Señorita Magister

Fiorella Linares Pérez

Lima – Perú
Presente**. -**

Asunto : Validación de instrumento, por criterio de experto

De mi especial consideración:

Es grato dirigirme a Usted, para expresarle un saludo cordial e informarle que como parte del desarrollo de la tesis del Programa Académico de Maestría en Derecho Penal y Procesal Penal, estoy desarrollando el avance de mi tesis titulada: "Fraude Informático en los Sistemas de Seguridad Financiero, Distrito Fiscal de Lima Centro 2022", motivo por el cual elabore una matriz de categorización, construcción del instrumento y certificado de validación.

Por lo expuesto, con la finalidad de darle rigor científico necesario, se requiere la validación de dichos instrumentos a través de la evaluación de Juicio de Expertos. Es por ello, que me permito solicitarle su participación como magister, apelando a su trayectoria como profesional y reconocimiento académico.

Agradeciendo por anticipado su colaboración y aporte me despido de usted, no sin antes expresarle los sentimientos de consideración y estima personal.

Atentamente:

……..

Brenda Lisset Rosas Marroqui

DNI:22309091

PD. Se adjunta:

- Matriz de categorización
- Instrumentos de recolección de la información
- Ficha de validación de instrumento

MATRIZ DE CATEGORIZACIÓN DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Problema de investigación	**Categoría**	**Subcategorías**	**Indicadores**	**Ítems de la guía de entrevista aplicada dirigida a especialistas en derecho penal y procesal penal**
¿De qué manera el tratamiento del delito de Fraude Informático repercute en los sistemas de seguridad financiero que incrementa las denuncias del distrito fiscal Lima Centro 2022?	Fraude Informático.	Robo de datos Alterar o dar mal uso a sistemas o software	Información o base datos	4,14
			La falta de prevención sobre el control, supervisión y vigilancia de los sistemas de seguridad	9
			Ser responsable por la responsabilidad de otro, por no controlar, supervisar o vigilar	1,2,3,10,11, 13
¿De qué manera el robo de datos informáticos disminuye con la utilización adecuada de la información de la base de datos de las entidades financieras del distrito fiscal Lima Centro 2022?	Sistemas de Seguridad Financiero.	Utilización adecuada de información	Aparatos electrónicos	8
			Dispositivos digitales	4
			Vulnerabilidad de los sistemas informáticos	7,8
			Inadecuada Implementación	12
			Base de datos	4,6

¿Cómo la alteración de sistemas o software implican responsabilidad de la entidad financiera debido a la falta de respeto de los accesos de la información establecidos del distrito fiscal Lima Centro 2022?	Sistemas de Seguridad Financiero.	Respeto de los accesos de la información establecidos	Claves de acceso	11
			Información	8,9
			Responsables	1,2,4,13
			Sistema operativo	14

GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Entrevistado (a): ……

Edad: …… años Sexo: ……Fecha: ……

Objetivo general: Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022

1. ¿Considera Ud. que el delito de Fraude Informático regula responsabilidad objetiva para las entidades financieras?

……..

2. ¿Considera Ud. que los elementos de convicción acopiados en las investigaciones por delito de fraude informático llegan a acreditar responsabilidad penal de las entidades financieras?

……..

3. ¿Considera Ud. que el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero?

……..

4. ¿Cree Ud. que es posible determinar responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático.?

……..

5. ¿Considera Ud. que las entidades financieras tienen identificados los riesgos de los sistemas de seguridad financiero?

……..

6. ¿De qué manera el robo de datos repercute en los sistemas de seguridad financiero?

……

7. ¿Cree Ud. que las entidades financieras utilizan sistemas de seguridad adecuados a fin de evitar vulneraciones a la base de datos de sus usuarios?

……

8. ¿Cree Ud. que las entidades financieras utilizan procedimientos adecuados

para asegurar que la información sea utilizada adecuadamente?

……

9. ¿Cree Ud. que las entidades financieras realizan un control y seguimiento a los sistemas de seguridad de la información implementadas a fin de evitar vulneraciones?

……

10. ¿Considera Ud. que las entidades financieras cuentan con medidas preventivas a fin de salvaguardar la confidencialidad de su base de datos?

……

11. ¿Considera Ud. que la falta de cuidado y prevención sobre los riesgos de ataques por parte de las entidades financieras genera una responsabilidad penal?

……

12. ¿Considera Ud. que los sistemas de seguridad informático establecidos en la norma nacional e internacional son suficientes para salvaguardar la base de datos de las entidades financieras?

……

13. ¿Puede Ud. indicar de acuerdo a su experiencia qué tipo de responsabilidad se ha logrado identificar en el delito de fraude informático respecto a las entidades financieras?

……

14. ¿Cree Ud. que el robo de datos y la alteración o mal uso de los sistemas de software son solo de responsabilidad del hacker o también les alcanzaría responsabilidad a las entidades financieras?

……

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Nº	Formulación del ítem	Pertinencia[1]		Relevancia[2]		Claridad[3]		Observaciones	Sugerencias
		si	no	si	no	si	no		
1	¿Considera Ud. Que el delito de Fraude Informático regula responsabilidad objetiva para las entidades financieras?	X		X		X			
2	¿ Considera Ud. que los elementos de convicción acopiados en las investigaciones por delito de fraude informático llegan a acreditar responsabilidad penal de las entidades financieras?	X		X		X			
3	¿Considera Ud. que el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero?	X		X		X			
4	¿ Cree Ud. que es posible determinar responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático?	X		X		X			
5	¿ Considera Ud. que las entidades financieras tienen identificados los riesgos de los sistemas de seguridad financiero?	X		X		X			
6	¿ De qué manera el robo de datos repercute en los sistemas de seguridad financiero?	X		X		X			
7	¿ Cree Ud. que las entidades financieras utilizan sistemas de seguridad adecuados a fin de evitar vulneraciones a la base de datos de sus usuarios?	X		X		X			
8	¿ Cree Ud. que las entidades financieras utilizan procedimientos adecuados para asegurar que la información sea utilizada adecuadamente?	X		X		X			
9	¿ Cree Ud. que las entidades financieras realizan un control y seguimiento a los sistemas de seguridad de la información implementadas a fin de evitar vulneraciones?	X		X		X			
10	¿ Considera Ud. que las entidades financieras cuentan con medidas preventivas a fin de salvaguardar la confidencialidad de su base de datos?	X		X		X			
11	¿Considera Ud. que la falta de cuidado y prevención sobre los riesgos de ataques por parte de las entidades financieras genera una responsabilidad penal?	x		x		x			

12	¿Considera Ud. que los sistemas de seguridad informático establecidos en la norma nacional e internacional son suficientes para salvaguardar la base de datos de las entidades financieras?	X		X		X			
13	¿Puede Ud. indicar de acuerdo a su experiencia qué tipo de tipo responsabilidad se ha logrado identificar en el delito de fraude informático respecto a las entidades financieras?	X		X		X			
14	¿Cree Ud. que el robo de datos y la alteración o mal uso de los sistemas de software son solo de responsabilidad del hacker o también les alcanzaría responsabilidad a las entidades financieras?	X		X		X			

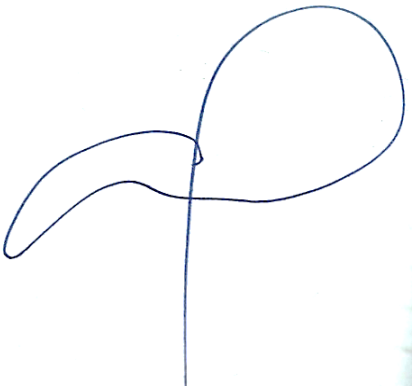
OPINIÓN DE APLICABILIDAD DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE LA RESPOSNABILIDAD PENAL DE LA PERSONA JURÍDICA, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Observaciones (precisar si hay suficiencia):

……

Opinión de aplicabilidad:

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

Nombres y Apellidos	Linares Pérez, Fiorella	DNI N°	42988692
Dirección domiciliaria	Los Olivos	Teléfono / Celular	993 952 151
Título profesional/ Especialidad	Abogado – Juez de Investigación Preparatoria	Firma	
Grado Académico	Magister con mención en Derecho Penal y Procesal Penal		
Metodólogo/ temático	Temático	Lugar y fecha	Lima, 05 de Junio 2023

[1] **Pertinencia:** El ítem corresponde al concepto teórico formulado.

[2] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo.

[3] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para evaluar la categoría

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: Linares Perez, Fiorella
1.2. Cargo e institución donde labora: Corte Superior de Justicia de Lima Norte
1.3. Nombre del instrumento motivo de evaluación: Guía de Entrevista
1.4. Autores de Instrumento: Rosas Marroqui, Brenda Lisset

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	Está formulado con lenguaje comprensible.												X	
2. OBJETIVIDAD	Está adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Está 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	Está 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

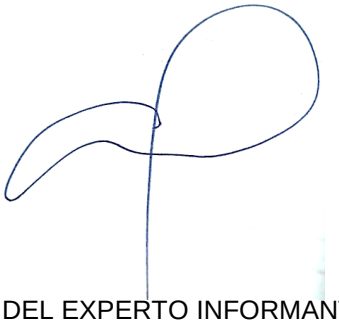
- El Instrumento cumple con los requisitos para su aplicación
- El Instrumento no cumple con los requisitos para su aplicación

95%	

IV. PROMEDIO DE VALORACIÓN:

95%

Lima, 05 de Junio de 2023.



FIRMA DEL EXPERTO INFORMANTE

DNI No 42988692 Telf.: 993 952 151

MATRIZ DE CATEGORIZACIÓN: Fraude Informático en los Sistemas de Seguridad Financiero, Distrito Fiscal de Lima Centro 2022

PROBLEMAS	OBJETIVOS	SUPUESTO	CATEGORÍA	SUBCATEGORÍA
¿De qué manera el tratamiento del delito de Fraude Informático repercute en los sistemas de seguridad financiero que incrementa las denuncias del distrito fiscal Lima Centro 2022?	Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022	El fraude informático en los sistemas de seguridad financiero incrementa denuncias, del distrito fiscal de Lima Centro 2022.	Fraude Informático.	Robo de datos Alterar o dar mal uso a sistemas o software
¿De qué manera el robo de datos informáticos disminuye con la utilización adecuada de la información de la base de datos de las entidades financieras del distrito fiscal Lima Centro 2022?	Evaluar si el delito de fraude informática regula responsabilidad penal de la entidad financiera en relación a los sistemas de seguridad financiero del distrito fiscal Lima Centro 2022	Le alcanza responsabilidad penal a la entidad financiera por delito de fraude informático del distrito fiscal de Lima Centro 2022.	Sistemas de Seguridad Financiero.	Utilización adecuada de información
¿Cómo la alteración de sistemas o software implican responsabilidad de la entidad financiera debido a la falta de respeto de los accesos de la información establecidos del distrito fiscal Lima Centro 2022?	Identificar los riesgos de los sistemas de seguridad financiero que incrementan las denuncias en el distrito fiscal Lima Centro 2022	Los riesgos en los sistemas de seguridad financiero inciden en el incremento de denuncias del distrito fiscal de Lima Centro 2022.	Sistema de Seguridad Financiero	Respeto de los accesos de la informaciÓn establecidos.

PROGRAMA ACADÉMICO DE MAESTRIA EN DERECHO PENAL Y PROCESAL PENAL

CARTA DE PRESENTACIÓN

Lima, 05 de junio de 2023

Señor Doctor

Freddy Andrés Camayo Tovar

Lima – Perú
Presente**. -**

Asunto : Validación de instrumento, por criterio de experto

De mi especial consideración:

Es grato dirigirme a Usted, para expresarle un saludo cordial e informarle que como parte del desarrollo de la tesis del Programa Académico de Maestría en Derecho Penal y Procesal Penal, estoy desarrollando el avance de mi tesis titulada: "Fraude Informático en los Sistemas de Seguridad Financiero, Distrito Fiscal de Lima Centro 2022", motivo por el cual elabore una matriz de categorización, construcción del instrumento y certificado de validación.

Por lo expuesto, con la finalidad de darle rigor científico necesario, se requiere la validación de dichos instrumentos a través de la evaluación de Juicio de Expertos. Es por ello, que me permito solicitarle su participación como magister, apelando su trayectoria y reconocimiento como juez y profesional.

Agradeciendo por anticipado su colaboración y aporte me despido de usted, no sin antes expresarle los sentimientos de consideración y estima personal.

Atentamente:

……..

Brenda Lisset Rosas Marroqui

DNI:22309091

PD. Se adjunta:

- Matriz de categorización
- Instrumentos de recolección de la información
- Ficha de validación de instrumento

MATRIZ DE CATEGORIZACIÓN DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Problema de investigación	**Categoría**	**Subcategorías**	**Indicadores**	**Ítems de la guía de entrevista aplicada dirigida a especialistas en derecho penal y procesal penal**
¿De qué manera el tratamiento del delito de Fraude Informático repercute en los sistemas de seguridad financiero que incrementa las denuncias del distrito fiscal Lima Centro 2022?	Fraude Informático.	Robo de datos Alterar o dar mal uso a sistemas o software	Información o base datos	4,14
			La falta de prevención sobre el control, supervisión y vigilancia de los sistemas de seguridad	9
			Ser responsable por la responsabilidad de otro, por no controlar, supervisar o vigilar	1,2,3,10,11,13
¿De qué manera el robo de datos informáticos disminuye con la utilización adecuada de la información de la base de datos de las entidades financieras del distrito fiscal Lima Centro 2022?	Sistemas de Seguridad Financiero.	Utilización adecuada de información	Aparatos electrónicos	8
			Dispositivos digitales	4
			Vulnerabilidad de los sistemas informáticos	7,8
			Inadecuada Implementación	12
			Base de datos	4,6

¿Cómo la alteración de sistemas o software implican responsabilidad de la entidad financiera debido a la falta de respeto de los accesos de la información establecidos del distrito fiscal Lima Centro 2022?	Sistemas de Seguridad Financiero.	Respeto de los accesos de la información establecidos	Claves de acceso	11	
			Información	8,9	
			Responsables	1,2,4,13	
			Sistema operativo	14	

GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Entrevistado (a): ……

Edad: …… años Sexo: ……Fecha: ……

Objetivo general: Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022

1. ¿Considera Ud. que el delito de Fraude Informático regula responsabilidad objetiva para las entidades financieras?

……..

2. ¿Considera Ud. que los elementos de convicción acopiados en las investigaciones por delito de fraude informático llegan a acreditar responsabilidad penal de las entidades financieras?

……..

3. ¿Considera Ud. que el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero?

……..

4. ¿Cree Ud. que es posible determinar responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático.?

……..

5. ¿ Considera Ud. que las entidades financieras tienen identificados los riesgos de los sistemas de seguridad financiero?

……..

6. ¿De qué manera el robo de datos repercute en los sistemas de seguridad financiero?

……

7. ¿Cree Ud. que las entidades financieras utilizan sistemas de seguridad adecuados a fin de evitar vulneraciones a la base de datos de sus usuarios?

……

8. ¿Cree Ud. que las entidades financieras utilizan procedimientos adecuados

para asegurar que la información sea utilizada adecuadamente?

……

9. ¿Cree Ud. que las entidades financieras realizan un control y seguimiento a los sistemas de seguridad de la información implementadas a fin de evitar vulneraciones?

……

10. ¿Considera Ud. que las entidades financieras cuentan con medidas preventivas a fin de salvaguardar la confidencialidad de su base de datos?

……

11. ¿Considera Ud. que la falta de cuidado y prevención sobre los riesgos de ataques por parte de las entidades financieras genera una responsabilidad penal?

……

12. ¿Considera Ud. que los sistemas de seguridad informático establecidos en la norma nacional e internacional son suficientes para salvaguardar la base de datos de las entidades financieras?

……

13. ¿Puede Ud. indicar de acuerdo a su experiencia qué tipo de tipo responsabilidad se ha logrado identificar en el delito de fraude informático respecto a las entidades financieras?

……

14. ¿Cree Ud. que el robo de datos y la alteración o mal uso de los sistemas de software son solo de responsabilidad del hacker o también les alcanzaría responsabilidad a las entidades financieras?

……

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Nº	Formulación del ítem	Pertinencia[1]		Relevancia[2]		Claridad[3]		Observaciones	Sugerencias
		si	no	si	no	si	no		
1	¿Considera Ud. Que el delito de Fraude Informático regula responsabilidad objetiva para las entidades financieras?	X		X		X			
2	¿ Considera Ud. que los elementos de convicción acopiados en las investigaciones por delito de fraude informático llegan a acreditar responsabilidad penal de las entidades financieras?	X		X		X			
3	¿Considera Ud. que el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero?	X		X		X			
4	¿ Cree Ud. que es posible determinar responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático?	X		X		X			
5	¿ Considera Ud. que las entidades financieras tienen identificados los riesgos de los sistemas de seguridad financiero?	X		X		X			
6	¿ De qué manera el robo de datos repercute en los sistemas de seguridad financiero?	X		X		X			
7	¿ Cree Ud. que las entidades financieras utilizan sistemas de seguridad adecuados a fin de evitar vulneraciones a la base de datos de sus usuarios?	X		X		X			
8	¿ Cree Ud. que las entidades financieras utilizan procedimientos adecuados para asegurar que la información sea utilizada adecuadamente?	X		X		X			
9	¿ Cree Ud. que las entidades financieras realizan un control y seguimiento a los sistemas de seguridad de la información implementadas a fin de evitar vulneraciones?	X		X		X			
10	¿ Considera Ud. que las entidades financieras cuentan con medidas preventivas a fin de salvaguardar la confidencialidad de su base de datos?	X		X		X			
11	¿Considera Ud. que la falta de cuidado y prevención sobre los riesgos de ataques por parte de las entidades financieras genera una responsabilidad penal?	X		X		X			

12	¿Considera Ud. que los sistemas de seguridad informático establecidos en la norma nacional e internacional son suficientes para salvaguardar la base de datos de las entidades financieras?	X		X		X			
13	¿Puede Ud. indicar de acuerdo a su experiencia qué tipo de tipo responsabilidad se ha logrado identificar en el delito de fraude informático respecto a las entidades financieras?	X		X		X			
14	¿Cree Ud. que el robo de datos y la alteración o mal uso de los sistemas de software son solo de responsabilidad del hacker o también les alcanzaría responsabilidad a las entidades financieras?	X		X		X			

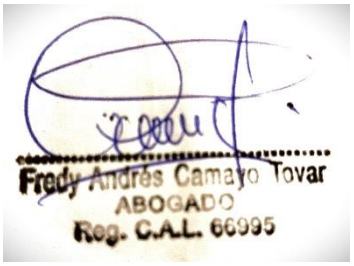
OPINIÓN DE APLICABILIDAD DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE LA RESPOSNABILIDAD PENAL DE LA PERSONA JURÍDICA, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Observaciones (precisar si hay suficiencia):

……

Opinión de aplicabilidad:

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

Nombres y Apellidos	Camayo Tovar Freddy Andrés	DNI N°	44171882
Dirección domiciliaria	Av. Argentina N° 1653	Teléfono / Celular	963309155
Título profesional/ Especialidad	Abogado - Penal	Firma	
Grado Académico	Magister con mención en Derecho Penal		
Metodólogo/ temático	Temático	Lugar y fecha	05 Junio 2023

[1] **Pertinencia:** El ítem corresponde al concepto teórico formulado.

[2] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo.

[3] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para evaluar la categoría

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.5. Apellidos y Nombres: Camayo Tovar, Freddy Andrés
1.6. Cargo e institución donde labora: Corte Superior de Justicia del Callao
1.7. Nombre del instrumento motivo de evaluación: Guía de Entrevista
1.8. Autores de Instrumento: Rosas Marroqui, Brenda Lisset

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	Está formulado con lenguaje comprensible.												x	
2. OBJETIVIDAD	Está adecuado a las leyes y principios científicos.												x	
3. ACTUALIDAD	Está 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	Está 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

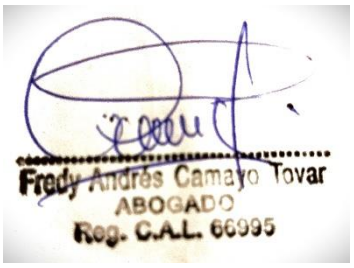
- El Instrumento cumple con los requisitos para su aplicación
- El Instrumento no cumple con los requisitos para su aplicación

95%	

IV. PROMEDIO DE VALORACIÓN:

95%

Lima, 05 de Junio de 2023.



FIRMA DEL EXPERTO INFORMANTE

DNI No 44171882 Telf.: 963309155

MATRIZ DE CATEGORIZACIÓN: Fraude Informático en los Sistemas de Seguridad Financiero, Distrito Fiscal de Lima Centro 2022

PROBLEMAS	OBJETIVOS	SUPUESTO	CATEGORÍA	SUBCATEGORÍA
¿De qué manera el tratamiento del delito de Fraude Informático repercute en los sistemas de seguridad financiero que incrementa las denuncias del distrito fiscal Lima Centro 2022?	Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022	El fraude informático en los sistemas de seguridad financiero incrementa denuncias, del distrito fiscal de Lima Centro 2022.	Fraude Informático.	Robo de datos Alterar o dar mal uso a sistemas o software
¿De qué manera el robo de datos informáticos disminuye con la utilización adecuada de la información de la base de datos de las entidades financieras del distrito fiscal Lima Centro 2022?	Evaluar si el delito de fraude informática regula responsabilidad penal de la entidad financiera en relación a los sistemas de seguridad financiero del distrito fiscal Lima Centro 2022	Le alcanza responsabilidad penal a la entidad financiera por delito de fraude informático del distrito fiscal de Lima Centro 2022.	Sistemas de Seguridad Financiero.	Utilización adecuada de información
¿Cómo la alteración de sistemas o software implican responsabilidad de la entidad financiera debido a la falta de respeto de los accesos de la información establecidos del distrito fiscal Lima Centro 2022?	Identificar los riesgos de los sistemas de seguridad financiero que incrementan las denuncias en el distrito fiscal Lima Centro 2022	Los riesgos en los sistemas de seguridad financiero inciden en el incremento de denuncias del distrito fiscal de Lima Centro 2022.	Sistema de Seguridad Financiero	Respeto de los accesos de la informaciÓn establecidos.

PROGRAMA ACADÉMICO DE MAESTRIA EN DERECHO PENAL Y PROCESAL PENAL

CARTA DE PRESENTACIÓN

Lima, 05 de Junio de 2023

Señor Magister:

Del Villar Canchari, Fernando

Lima – Perú
Presente**. -**

Asunto : Validación de instrumento, por criterio de experto

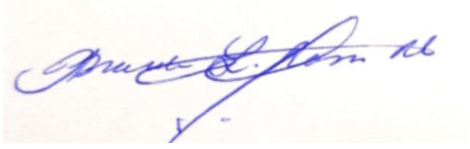
De mi especial consideración:

Es grato dirigirme a Usted, para expresarle un saludo cordial e informarle que como parte del desarrollo de la tesis del Programa Académico de Maestría en Derecho Penal y Procesal Penal, estoy desarrollando el avance de mi tesis titulada: "Fraude Informático en los Sistemas de Seguridad Financiero, Distrito Fiscal de Lima Centro 2022", motivo por el cual elabore una matriz de categorización, construcción del instrumento y certificado de validación.

Por lo expuesto, con la finalidad de darle rigor científico necesario, se requiere la validación de dichos instrumentos a través de la evaluación de Juicio de Expertos. Es por ello, que me permito solicitarle su participación como abogada en ejercicio, apelando su trayectoria y reconocimiento como profesional.

Agradeciendo por anticipado su colaboración y aporte me despido de usted, no sin antes expresarle los sentimientos de consideración y estima personal.

Atentamente:



……..

Brenda Lisset Rosas Marroqui

DNI:22309091

PD. Se adjunta:

- Matriz de categorización
- Instrumentos de recolección de la información
- Ficha de validación de instrumento

MATRIZ DE CATEGORIZACIÓN DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Problema de investigación	**Categoría**	**Subcategorías**	**Indicadores**	**Ítems de la guía de entrevista aplicada dirigida a especialistas en derecho penal y procesal penal**
¿De qué manera el tratamiento del delito de Fraude Informático repercute en los sistemas de seguridad financiero que incrementa las denuncias del distrito fiscal Lima Centro 2022?	Fraude Informático.	Robo de datos Alterar o dar mal uso a sistemas o software	Información o base datos	4,14
			La falta de prevención sobre el control, supervisión y vigilancia de los sistemas de seguridad	9
			Ser responsable por la responsabilidad de otro, por no controlar, supervisar o vigilar	1,2,3,10,11,13
¿De qué manera el robo de datos informáticos disminuye con la utilización adecuada de la información de la base de datos de las entidades financieras del distrito fiscal Lima Centro 2022?	Sistemas de Seguridad Financiero.	Utilización adecuada de información	Aparatos electrónicos	8
			Dispositivos digitales	4
			Vulnerabilidad de los sistemas informáticos	7,8
			Inadecuada Implementación	12
			Base de datos	4,6

¿Cómo la alteración de sistemas o software implican responsabilidad de la entidad financiera debido a la falta de respeto de los accesos de la información establecidos del distrito fiscal Lima Centro 2022?	Sistemas de Seguridad Financiero.	Respeto de los accesos de la información establecidos	Claves de acceso	11	
			Información	8,9	
			Responsables	1,2,4,13	
			Sistema operativo	14	

GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Entrevistado (a): ……

Edad: …… años Sexo: ……Fecha: ……

Objetivo general: Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022

1. ¿Considera Ud. que el delito de Fraude Informático regula responsabilidad objetiva para las entidades financieras?

……..

2. ¿Considera Ud. que los elementos de convicción acopiados en las investigaciones por delito de fraude informático llegan a acreditar responsabilidad penal de las entidades financieras?

……..

3. ¿Considera Ud. que el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero?

……..

4. ¿Cree Ud. que es posible determinar responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático??

……..

5. ¿Considera Ud. que las entidades financieras tienen identificados los riesgos de los sistemas de seguridad financiero?

……..

6. ¿De qué manera el robo de datos repercute en los sistemas de seguridad financiero?

……

7. ¿Cree Ud. que las entidades financieras utilizan sistemas de seguridad adecuados a fin de evitar vulneraciones a la base de datos de sus usuarios?

……

8. ¿Cree Ud. que las entidades financieras utilizan procedimientos adecuados para asegurar que la información sea utilizada adecuadamente?

……

9. ¿Cree Ud. que las entidades financieras realizan un control y seguimiento a los sistemas de seguridad de la información implementadas a fin de evitar vulneraciones?

……

10. ¿Considera Ud. que las entidades financieras cuentan con medidas preventivas a fin de salvaguardar la confidencialidad de su base de datos?

……

11. ¿Considera Ud. que la falta de cuidado y prevención sobre los riesgos de ataques por parte de las entidades financieras genera una responsabilidad penal?

……

12. ¿Considera Ud. que los sistemas de seguridad informático establecidos en la norma nacional e internacional son suficientes para salvaguardar la base de datos de las entidades financieras?

……

13. ¿Puede Ud. indicar de acuerdo a su experiencia qué tipo de tipo responsabilidad se ha logrado identificar en el delito de fraude informático respecto a las entidades financieras?

……

14. ¿Cree Ud. que el robo de datos y la alteración o mal uso de los sistemas de software son solo de responsabilidad del hacker o también les alcanzaría responsabilidad a las entidades financieras?

……

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Nº	Formulación del ítem	Pertinencia[1]		Relevancia[2]		Claridad[3]		Observaciones	Sugerencias
		si	no	si	no	si	no		
1	¿Considera Ud. Que el delito de Fraude Informático regula responsabilidad objetiva para las entidades financieras?	X		X		X			
2	¿ Considera Ud. que los elementos de convicción acopiados en las investigaciones por delito de fraude informático llegan a acreditar responsabilidad penal de las entidades financieras?	X		X		X			
3	¿Considera Ud. que el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero?	X		X		X			
4	¿ Cree Ud. que es posible determinar responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático?	X		X		X			
5	¿ Considera Ud. que las entidades financieras tienen identificados los riesgos de los sistemas de seguridad financiero?	X		X		X			
6	¿ De qué manera el robo de datos repercute en los sistemas de seguridad financiero?	X		X		X			
7	¿ Cree Ud. que las entidades financieras utilizan sistemas de seguridad adecuados a fin de evitar vulneraciones a la base de datos de sus usuarios?	X		X		X			
8	¿ Cree Ud. que las entidades financieras utilizan procedimientos adecuados para asegurar que la información sea utilizada adecuadamente?	X		X		X			
9	¿ Cree Ud. que las entidades financieras realizan un control y seguimiento a los sistemas de seguridad de la información implementadas a fin de evitar vulneraciones?	X		X		X			
10	¿ Considera Ud. que las entidades financieras cuentan con medidas preventivas a fin de salvaguardar la confidencialidad de su base de datos?	X		X		X			
11	¿Considera Ud. que la falta de cuidado y prevención sobre los riesgos de ataques por parte de las entidades financieras genera una responsabilidad penal?	X		X		X			

12	¿Considera Ud. que los sistemas de seguridad informático establecidos en la norma nacional e internacional son suficientes para salvaguardar la base de datos de las entidades financieras?	X		X		X			
13	¿Puede Ud. indicar de acuerdo a su experiencia qué tipo de tipo responsabilidad se ha logrado identificar en el delito de fraude informático respecto a las entidades financieras?	X		X		X			
14	¿Cree Ud. que el robo de datos y la alteración o mal uso de los sistemas de software son solo de responsabilidad del hacker o también les alcanzaría responsabilidad a las entidades financieras?	X		X		X			

OPINIÓN DE APLICABILIDAD DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE LA RESPOSNABILIDAD PENAL DE LA PERSONA JURÍDICA, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Observaciones (precisar si hay suficiencia):

……

Opinión de aplicabilidad:

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

Nombres y Apellidos	Fernando del Villar Canchari	DNI N°	20052658
Dirección domiciliaria	Calle Los Tilos Mz F1 Lote 42 Urb. El Alamo Comas – Lima - Lima	Teléfono / Celular	912590113
Título profesional/ Especialidad	Abogado -	Firma	
Grado Académico	Magister en Derecho Penal y Procesal Penal		
Metodólogo/ temático	temático	Lugar y fecha	05 Junio 2023

[1] **Pertinencia:** El ítem corresponde al concepto teórico formulado.

[2] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo.

[3] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para evaluar la categoría

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.9. Apellidos y Nombres: Del Villar Canchari, Fernando
1.10. Cargo e institución donde labora: Colegio de Abogados de Lima
1.11. Nombre del instrumento motivo de evaluación: Guía de Entrevista
1.12. Autores de Instrumento: Rosas Marrroqui, Brenda Lisset

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	Está formulado con lenguaje comprensible.												x	
2. OBJETIVIDAD	Está adecuado a las leyes y principios científicos.												x	
3. ACTUALIDAD	Está 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	Está 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
- El Instrumento no cumple con los requisitos para su aplicación

95%	

IV. PROMEDIO DE VALORACIÓN:

95%

Lima, 05 de Junio de 2023.

Mg. Fernando Del Villar Canchari

Reg CAL N° 87263

DNI 20052658

Móvil 912590113

GUÍA DE ENTREVISTA SEMIESTRUCTURADAS OBRE FRAUDE INFORMÁTICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Entrevistado(a):

Lourdes Nelly Ocares Ochoa

……

Edad:63……..años Sexo:…Femenino…….Fecha: 15 Junio 2023……

Objetivo general: Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias,distrito fiscal Lima Centro 2022

1. **¿Explique Ud. si el delito de Fraude Informático regula la responsabilidad penal de las entidades financieras?**

La Ley N° 30096, sobre delitos informáticos, que fue promulgada el 22 de octubre de 2013, y modificada por Ley N° 30171, se observa que dentro de su tipificación, no se menciona nada respecto de la responsabilidad penal de las entidades financieras. Una de las razones por la cual, se podría pensar, que no tienen responsabilidad penal, en los delitos de fraude informático, es porque tal vez su finalidad, no es la de cometer un ilícito penal, sino brindar un servicio, a fin de obtener a traves de ello una utilidad; sin embargo, ello no lo exime de las responsabilidades civiles o administrativas, de no aplicar correctamente las regulaciones establecidas en los reglamentos de cumplimiento, y evitar riesgos que puedan poner en peligro a los usuarios de su servicio.

2. ¿Explique Ud. Si el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiera?

El delito de fraude informático, influye, en los sistemas de seguridad financiera, porque establecen una forma de garantía para la prevención, contra aquellas personas que vulneren las medidas de seguridad, establecidas por los entes financieros dentro de sus sistemas de seguridad, a fin de proteger el sistema de pagos y la estabilidad financiera de los intereses de sus propios usuarios.

3. ¿Señale Ud. si el delito de Fraude Informático regula responsabilidad penal por la falta de implementación de sistemas de seguridad financiera?

Firma Digital
Firmado digitalmente por OCARES OCHOA Lourdes Nelly FAU 20550734223 soft
Motivo: Soy el autor del documento
Fecha: 22.07.2023 15:57:12 -05:00

Actualmente, el delito de fraude informático no regula la responsabilidad penal por falta de implementación de sistemas de seguridad en sus actividades financieras, para ellos existen otras normas que le son aplicables, de acuerdo a la materia y que podrían ser materia o pasibles de las consecuencias jurídicas penales establecidas en el art. 105° del Código penal, el cual podría ser modificado para darles el alcance a las entidades financieras en este rubro de ilícitos penales.

4. ¿Cree Ud. que es posible determinar responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático?

Actualmente en el sistema penal peruano, rige el principio "*societas delinquere non potest*", mediante este principio no se regula o aplica, al menos actualmente una responsabilidad penal, para las personas jurídicas; sin embargo como ya se mencionó anteriormente es posible determinar las consecuencias accesorias y aplicables reguladas por el art. 205° del código penal.

5. ¿Puede Ud. indicar de acuerdo a su experiencia qué tipo de responsabilidad se ha logrado identificar en el delito de fraude informático respecto a las entidades financieras?

En este tipo de delitos complejos, en su determinación, por las actividades que realiza, y la multiplicidad de sujetos que intervienen en ello, generalmente se vulneran intereses colectivos, relacionados con los propios sistemas de seguridad de las entidades financieras, pues las empresas de éste tipo, mantienen una serie complejidades dentro de su distribución de funciones, y siendo ello así, se advierte, generalmente que son agrupaciones, que con un rol especifico, para cada uno de sus individuos - partícipes, afectan intereses colectivos, como por ejemplo, afectación en el tráfico de información, o de bienes jurídicos relacionados con caudales, o patrimonios personales e incluso hasta el propio comercio electrónico.

6. ¿Considera Ud. que las entidades financieras tienen identificados los riesgos de los sistemas de seguridad financiero?

Considero que si se tienen identificados, las distintas formas que afectan la seguridad financiera, por ello implementan, sistemas de seguridad informatica, para los casos que ya se conocen como el ***pharming, phishing,*** del cual se desprende el ***"smishing***", que es otra modalidad de robar información y dinero a través de mensajes de texto; entonces podemos deducir que siempre se están

creando nuevas modalidades de fraude informático, por lo que es responsabilidad de las entidades financieras ir a la par, con una actualización permanente de sus sistemas de seguridad a fin de identificar estas nuevas formas de fraude y neutralizar su ejecución.

7. ¿Cree Ud. que las entidades financieras utilizan sistemas de seguridad adecuados de control y seguimiento para evitar vulneraciones a la base de datos de sus usuarios?

De lo poco que se conoce, puesto que es información muy reservada, los sistemas de seguridad informático de los sistemas financieros, tratan de apaciguar, o dar frente a este problema actual, a fin de que sus usuarios no se vean afectados.

8. ¿Considera Ud. que los sistemas de seguridad informático establecidos en la norma nacional e internacional son suficientes para salvaguardar la base de datos de las entidades financieras?

Siempre están en constante desarrollo, y se rigen por la ley de la materia, tanto nacional como internacional, que pueden ser estandarizadas a través de la ISO 27001 u otras normas internacionales.

9. ¿Cree Ud. la vulneración de los sistemas de seguridad financiera son solo de responsabilidad del hacker o también les alcanzaría responsabilidad a las entidades bancarias?

Nuestro sistema penal peruano, establece responsabilidad penal, para quienes realicen actuaciones en contra de aquellos intereses protegidos dentro de un sistema establecido. Pero definitivamente alcanza responsabilidad a las entidades bancarias, en su condición de personas jurídicas cuyo quehacer es la prestación de un servicio al ciudadano.

10. ¿Cómo se puede evitar el delito de fraude informático?

A través de la implementación de mayores sistemas de seguridad en consonancia con las normas internacionales estandarizadas como las ISOS, también se puede evitar este tipo de delitos a través de una coordinación interinstitucional entre el Estado y la actividad financiera privada, en beneficio de la colectividad.

Nombre del entrevistado	**Sello y firma**
Lourdes Nelly Ocares Ochoa	**Juez Superior 2da Sala Penal Transitoria C.S.J. Lima Norte**

Firma Digital

Firmado digitalmente por OCARES OCHOA Lourdes Nelly FAU 20550734223 soft
Motivo: Soy el autor del documento
Fecha: 22.07.2023 15:59:06 -05:00

GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Entrevistado (a): Miguel Ricardo Castañeda Moya

.....

Edad: .....54... años Sexo: ...Masculino....Fecha: .....21.06.2023...

Objetivo general: Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022

1. ¿Explique Ud. si el delito de Fraude Informático regula la responsabilidad penal de las entidades financieras?

Si en la medida que se aplique en concordancia con el artículo 27 del Código Penal (el actuar por otro).

2. ¿Explique Ud. Si el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiera

Si las entidades del sistema funcionario utilizan sistemas informáticos, las conductas típicas del fraude informático también pueden aplicarse a dichos sistemas.

3. ¿Señale Ud. si el delito de Fraude Informático regula responsabilidad penal por la falta de implementación de sistemas de seguridad financiera?

Si se tiene en cuenta el artículo 8 de la Ley de Delitos Informáticos no hay responsabilidad penal por ello.

4. ¿Cree Ud. que es posible determinar responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático.?

Típicamente es posible la responsabilidad penal de dichas entidades. El problema es su prueba. La posibilidad de investigar o analizar sus sistemas informáticos está cerrada a terceros. Normalmente es la propia entidad financiera la que se supone hace esa evaluación.

5. ¿Puede Ud. indicar de acuerdo a su experiencia qué tipo de responsabilidad se ha logrado identificar en el delito de fraude informático respecto a las entidades financieras?

No recuerdo algún caso donde la entidad financiera haya respondido penalmente por fraude informático. En general, se le trata solo como tercero civil responsable.

6. ¿Considera Ud. que las entidades financieras tienen identificados los riesgos de los sistemas de seguridad financiero?

Considero que sí.

7. ¿Cree Ud. que las entidades financieras utilizan sistemas de seguridad adecuados de control y seguimiento para evitar vulneraciones a la base de datos de sus usuarios?

Considero que no pues la frecuencia de la comisión de estos delitos en sistemas informáticos de entidades financieras es frecuente.

8. ¿Considera Ud. que los sistemas de seguridad informático establecidos en la norma nacional e internacional son suficientes para salvaguardar la base de datos de las entidades financieras?

Considero que deberían mejorarse.

9. ¿Cree Ud. la vulneración de los sistemas de seguridad financiera son solo de responsabilidad del hacker o también les alcanzaría responsabilidad a las entidades bancarias?

Creo que hay responsabilidad de las entidades financieras.

10. ¿Cómo se puede evitar el delito de fraude informático?
Estimo que los titulares de los sistemas informáticos, como las entidades financieras, deben poseer mejores sistemas de seguridad y, en su defecto, cubrir esas falencias con seguros que garanticen a los terceros usuarios cualquier daño ocasionado por este tipo de delitos.

Nombre del entrevistado	Sello y firma
Miguel Ricardo Castañeda Moya	PODER JUDICIAL DEL PERU MIGUEL RICARDO CASTAÑEDA MOYA PRESIDENTE 1° SALA PENAL DE APELACIONES PERMANENTE CORTE SUPERIOR DE JUSTICIA DEL CALLAO

GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Entrevistado (a):

LUIS ANTONIO LA ROSA PAREDES

Edad: ..... años Sexo: Masculino Fecha: 05/07/2023.

Objetivo general: Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022

1. ¿Explique Ud. si el delito de Fraude Informático regula la responsabilidad penal de las entidades financieras?

El delito de fraude informático no prevé de manera expresa sobre la responsabilidad penal de las entidades financieras, lo que sí es abordado en la 10° disposición complementaria final de dicha ley y el Código Procesal Penal.....

2. ¿Explique Ud. Si el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiera?

La norma también incide en los sistemas de seguridad financiera, lo dispuesto en la 4° Disposición final y complementaria de la Ley N° 26702, en cuanto al informe técnico de la SBS ni bien se formule denuncia penal contra alguna entidad del área.

3. ¿Señale Ud. si el delito de Fraude Informático regula responsabilidad penal por la falta de implementación de sistemas de seguridad financiera?

En su tenor no, pero en aplicación de las glosadas normas de la Ley de delitos informáticos y de la Ley General de la SBS y sus afines si se expresa determinadas pautas para investigar, probar y sancionar a las empresas financieras en ese rubro.....

4. ¿Cree Ud. que es posible determinar responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático.?

Que bajo las normas aludidas y en aplicación de la Ley N° 30424 puede establecerse según los hechos concretos y las pruebas, la responsabilidad administrativa de las entidades financieras según el caso, el programa de cumplimiento normativo o compliance program busca también prevenir y detectar tal delito.....

5. ¿Puede Ud. indicar de acuerdo a su experiencia qué tipo de responsabilidad se ha logrado identificar en el delito de fraude informático respecto

a las entidades financieras?

Se halla una responsabilidad penal de sus agentes y una responsabilidad administrativa de las entidades bancarias de ser el caso, les alude a ambos una responsabilidad civil.....

6. ¿Considera Ud. que las entidades financieras tienen identificados los riesgos de los sistemas de seguridad financiero?

Que, frente a la creciente delincuencia cibernética, amplia y diversificada, los riesgos deben ser asumidos por el sistema de seguridad financiera con mayor especialidad y logística. Están en proceso. .....

7. ¿Cree Ud. que las entidades financieras utilizan sistemas de seguridad adecuados de control y seguimiento para evitar vulneraciones a la base de datos de sus usuarios?

Es evidente la insuficiencia de los medios con que cuenta el sistema de seguridad para el control y seguimiento de esas acciones ilegales, las bases de datos de los usuarios son posibles de hackear para sustracción y disposición, en algunos casos debe evitarse.....

8. ¿Considera Ud. que los sistemas de seguridad informático establecidos en la norma nacional e internacional son suficientes para salvaguardar la base de datos de las entidades financieras?

En materia informática los avances son exponenciales, y ante un medio de seguridad surgen nuevos dispositivos invasivos del sistema, por ello por ahora es mensurando tal avances ilícitos y generar nuevos y mejores controles.....

9. ¿Cree Ud. la vulneración de los sistemas de seguridad financiera son solo de responsabilidad del hacker o también les alcanzaría responsabilidad a las entidades bancarias?

El hacker podría ser responsable penal a título de autor, mientras que las entidades financieras podrían ser responsables administrativas en este delito, sin perjuicio de la responsabilidad por daños y perjuicios.....

10. ¿Cómo se puede evitar el delito de fraude informático?

Se podría evitar mejorando los mecanismos de prevención y control de las actividades riesgosas en el sistema financiero, especializando unidades técnicas como la DIVIAT – PNP y las fiscalías especializadas, educando al usuario en seguridad financiera.....

Nombre del entrevistado	Sello y firma
LUIS ANTONIO LA ROSA PAREDES	JUEZ SUPERIOR

GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Entrevistado (a):

Maritza Del Pilar Lopez Rojas

Edad: 62 años Sexo: F e m e n i n o .Fecha: 16 de Junio del 2023

Objetivo general: Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022

1.¿Explique Ud. si el delito de Fraude Informático regula la responsabilidad penal de las entidades financieras?

El delito de fraude informático no regula la responsabilidad penal de las entidades financieras, porque son ellas muchas veces sujetos pasivos de éste delito, quienes se ven afectadas en su imagen, puesto que crea desconfianza entre sus clientes.

2.¿Explique Ud. Si el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiera?

Los ciber delincuentes muchas veces logran ingresar a los sistemas financieros de las empresas, en especial del sistema bancario, burlando los sistemas de seguridad, por lo que definitivamente repercute en los sistemas de seguridad financiera.

3. ¿Señale Ud. si el delito de Fraude Informático regula responsabilidad penal por la falta de implementación de sistemas de seguridad financiera?

No regula responsabilidad penal contra de las empresas del sistema bancario, por la falta de implementación del sistemas de seguridad financiera.

4.¿Cree Ud. que es posible determinar responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático.?

dificilmente se puede determinar responsabilidad penal de las entidades financieras por el robo de datos, por el contrario resultan perjudicados

5.¿Puede Ud. indicar de acuerdo a su experiencia qué tipo de responsabilidad se ha logrado identificar en el delito de fraude informático respecto a las entidades financieras?

El tipo de responsabilidad que le correspondería a las entidades financieras sería la de responsabilidad civil, es decir, sería un tercero civilmente responsable.

6. ¿Considera Ud. que las entidades financieras tienen identificados los riesgos de los sistemas de seguridad financiero?

Creo que si, porque las entidades financieras conocen los riesgos que corren, de que son vulnerables a que sus sistemas puedan ser interferidos por delincuentes cibernautas.

7.¿Cree Ud. que las entidades financieras utilizan sistemas de seguridad adecuados de control y seguimiento para evitar vulneraciones a la base de datos de sus usuarios?

Considero que sí, sin embargo esos sistemas de seguridad tienen que ir de acorde al avance tecnológico, puesto que los delincuentes ciber náuticos adoptan cada vez más nuevas formas de vulnerar los sistemas informáticos.

8.¿Considera Ud. que los sistemas de seguridad informático establecidos en la norma nacional e internacional son suficientes para salvaguardar la base de datos de las entidades financieras?

No, son suficientes porque estas deben ir cambiando de acorde a los avances y modalidades nuevas que los delincuentes cibernautas utilizan para vulnerar los sistemas informáticos .

9.¿Cree Ud. la vulneración de los sistemas de seguridad financiera son solo de responsabilidad del hacker o también les alcanzaría responsabilidad a las entidades bancarias?

A las entidades financieras les compete mejor sus sistemas de seguridad financiera, utilizando la tecnología y la ciencia, para evitar que sus clientes sean víctimas de la clonación de sus datos, y el robo de su dinero.

10.¿Cómo se puede evitar el delito de fraude informático?
Compete al sector empresarial y financiero crear nuevas formas de protección de los datos de los usuarios del sistema financiero, utilizando técnicas de última generación para protección de datos.

Nombre del entrevistado	**Sello y firma**
Maritza Del Pilar Lopez Rojas	MARITZA DEL PILAR LOPEZ ROJAS Fiscal Provincial Penal 2da. Fiscalía Provincial Penal Corporativa de Ventanilla

GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Entrevistado (a):

.....Dr. Jonathan Cirilo Portillo Vela .....

Edad: 35 años Sexo: .....M..... Fecha: 03/07/2023

Objetivo general: Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022

1. ¿Explique Ud. si el delito de Fraude Informático regula la responsabilidad penal de las entidades financieras?

.....

El delito de fraude informático del artículo 8 de la ley no contempla de forma expresa responsabilidad penal solo consecuencias en mérito a la cooperación y el cumplimiento de información, de forma posterior.

.....

2. ¿Explique Ud. Si el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiera?

.....

Si, efectivamente el delito de fraude informático en los verbos rectores implica de por si un atentado a la seguridad o al sistema bancario como tal, por ende repercute en las políticas de prevención y seguridad

.....

3. ¿Señale Ud. si el delito de Fraude Informático regula responsabilidad penal por la falta de implementación de sistemas de seguridad financiera?

.....

No contiene expresamente responsabilidad por falta de implementación, o ausencia de las mismas.

.....

4. ¿Cree Ud. que es posible determinar responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude

informático.?

.....

Estimo que si es posible establecer consecuencias por responsabilidad de entidades financieras si para el caso concreto se comprueba fallas en las políticas de protección, sistemas de alerta, seguridad u otros que resguarden operaciones no reconocidas.

.....

5. ¿Puede Ud. indicar de acuerdo a su experiencia qué tipo de responsabilidad se ha logrado identificar en el delito de fraude informático respecto a las entidades financieras?

.....

No se ha podido establecer casos de responsabilidad a la fecha, al menos del conocimiento del suscrito

.....

6. ¿Considera Ud. que las entidades financieras tienen identificados los riesgos de los sistemas de seguridad financiero?

.....

Estimo que si bien las empresas bancarias tienen sistemas de seguridad, no existen políticas adecuadas de cuidado y prevención, máxime si por el propio descuido o desorden interno se bajan estándares de seguridad para ocasionar mayores ganancias.

.....

7. ¿Cree Ud. que las entidades financieras utilizan sistemas de seguridad adecuados de control y seguimiento para evitar vulneraciones a la base de datos de sus usuarios?

.....

Estimo que si existen dichas políticas o sistemas de control, pero que las mismas tienen diferencias marcadas dentro de cada empresa del sistema financiero,

.....

8. ¿Considera Ud. que los sistemas de seguridad informático establecidos en la norma nacional e internacional son suficientes para salvaguardar la base de datos de las entidades financieras?

.....

.....

Estimo que deben existir mayores pautas o requerimientos de control a las entidades.

.....

9. ¿Cree Ud. la vulneración de los sistemas de seguridad financiera son solo de responsabilidad del hacker o también les alcanzaría responsabilidad a las entidades bancarias?

.....

Estimo que si no existe el debido cuidado si debería considerarse responsabilidad de las empresas del sistema financiero.

.....

10. ¿Cómo se puede evitar el delito de fraude informático?

.....

Aumento de las políticas de prevención y protección, mayores controles para la solicitud de cuentas y líneas telefónicas, otorgamiento de información real y oportuna de las empresas para el cumplimiento de la información y el registro de las IP, doble factor de verificación y exigencia de control biometrico

.....

Nombre del entrevistado	**Sello y firma**
Jonathan Cirilo Portillo Vela	JONATHAN CIRILO PORTILLO VELA Fiscal Provincial 2° Despacho Provincial de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro

GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Entrevistado (a):

Marcial Eloy Paucar Chappa

Edad: 40 años Sexo: masculino Fecha: 21/06/2023

Objetivo general: Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022

1. ¿Explique Ud. si el delito de Fraude Informático regula la responsabilidad penal de las entidades financieras?

No, actualmente no se encuentra contemplado en la Ley Nº 30096.

2. ¿Explique Ud. Si el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiera?

Sí, tanto a nivel interno como externo, Incluso existe un reglamento de la SBS sobre ciberseguridad.

3. ¿Señale Ud. si el delito de Fraude Informático regula responsabilidad penal por la falta de implementación de sistemas de seguridad financiera?

No, actualmente no regula.

4. ¿Cree Ud. que es posible determinar responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático.?

Existiría responsabilidad por delito de acceso ilícito con circunstancia agravante de móvil económico.

5. ¿Puede Ud. indicar de acuerdo a su experiencia qué tipo de responsabilidad se ha logrado identificar en el delito de fraude informático respecto a las entidades financieras?

Se ha tomado conocimiento que en algunos casos se ha determinado responsabilidad administrative ante Salas de Indecopi.

6. ¿Considera Ud. que las entidades financieras tienen identificados los riesgos de los sistemas de seguridad financiero?

Aún no se ha regulado ni reglamentado un sistema de prevención.

7. ¿Cree Ud. que las entidades financieras utilizan sistemas de seguridad adecuados de control y seguimiento para evitar vulneraciones a la base de datos de sus usuarios?

Dichos sistemas de seguridad deben mejorarse.

8. ¿Considera Ud. que los sistemas de seguridad informático establecidos en la norma nacional e internacional son suficientes para salvaguardar la base de datos de las entidades financieras?

Debe implementarse un sistema de prevención con mayor articulación entre los operadores y el sector privado.

9. ¿Cree Ud. la vulneración de los sistemas de seguridad financiera son solo de responsabilidad del hacker o también les alcanzaría responsabilidad a las entidades bancarias?

La vulneración de los sistemas de seguridad puede darse tanto a nivel interno como externo.

10. ¿Cómo se puede evitar el delito de fraude informático?

Se requiere un Plan Nacional contra los delitos informáticos, dentro del mismo se debe implementar un sistema de prevención y una entidad que fiscalice y supervise su cumplimiento.

Nombre del entrevistado	**Sello y firma**
MARCIAL ELOY PAUCAR CHAPPA	MARCIAL ELOY PAUCAR CHAPPA FISCAL PROVINCIAL PENAL TITULAR DE LIMA 1° DESPACHO PROVINCIAL DE LA FISCALÍA CORPORATIVA ESPECIALIZADA EN CIBERDELINCUENCIA DE LIMA CENTRO

GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Entrevistado (a): Miguel Ángel Durand Ramírez .....

Edad: 59 años. Sexo: Masculino Fecha: 14/04/1964.

Objetivo general: Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022

1. **¿Explique Ud. si el delito de Fraude Informático regula la responsabilidad penal de las entidades financieras?**

   El delito de Fraude Informático regula la acción y la responsabilidad penal del sujeto activo que comete el delito, y las entidades financieras con responsabilidad civil, y en casos específicos lo regula su ley especial, que los sanciona por no cumplir con el deber de protección de sus productos, en materia contenciosa administrativa.

2. **¿Explique Ud. Si el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiera?**

   A mi entender, si repercute por cuanto ante un delito informáticos responden con multas impuestas de encontrase responsabilidad.

3. **¿Señale Ud. si el delito de Fraude Informático regula responsabilidad penal por la falta de implementación de sistemas de seguridad financiera?**

   Efectivamente que sí, conforme a lo establecido en las disposiciones complementarias Finales, disposición DECIMA de la Ley N° 30096, sobre Regulación e imposición de multas por la Superintendencia de Banca, Seguros y AFP.

4. **¿Cree Ud. que es posible determinar responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático.?**

   Hasta ahora por mi experiencia más he vistos que sean sancionadas con multas al encontrase responsables.

5. **¿Puede Ud. indicar de acuerdo a su experiencia qué tipo de responsabilidad se ha logrado identificar en el delito de fraude informático respecto a las entidades financieras?**

   Cuando existe un tema de delitos informáticos por clonación de tarjetas o por robo de dinero a través de tarjetas, no solo se ha recurrido a la denuncia penal sino también se ha hecho la denuncia administrativa a INDECOPI, donde luego de realizado el trámite administrativo respectivo se ha logrado la imposición de multas, al encontrarse responsabilidad de la entidad financiera por falta de implementación en su sistema de seguridad.

6. **¿Considera Ud. que las entidades financieras tienen identificados los riesgos de los sistemas de seguridad financiero?**

   Si tienen identificados sus riesgos, sin embargo, a pesar de sus esfuerzos, muchas veces son el personal que labora en dichas entidades bancarias son los que están implicados en dichos delitos y en otros casos falta de previsión.

7. **¿Cree Ud. que las entidades financieras utilizan sistemas de seguridad adecuados de control y seguimiento para evitar vulneraciones a la base de datos de sus usuarios?**

   Al parecer no, por cuanto muchas veces los mismos trabajadores son los que pasan los datos de los usuarios a los criminales.

8. **¿Considera Ud. que los sistemas de seguridad informático establecidos en la norma nacional e internacional son suficientes para salvaguardar la base de datos de las entidades financieras?**

   Mientras más avance hay en la tecnología, mas avanza la criminalidad también, sin embargo, estos últimos cinco años en latino américa más incidencia de delitos informáticos, y en Perú especialmente donde mayormente se han incrementados los casos, causando un perjuicio económico no solo de los consumidores agraviados, sino también de las entidades bancarias, por cuanto tienen que devolver el dinero sacado de las cuentas por los hacker sino también por las multas impuestas al encontrárseles responsables al no haber cumplido con las medidas de seguridad establecidas.

9. **¿Cree Ud. la vulneración de los sistemas de seguridad financiera son solo de responsabilidad del hacker o también les alcanzaría**

responsabilidad a las entidades bancarias?

Es algo discutible, por cuanto cada caso es especifico no existe un patrón, cada caso es diferente, en algunos si podría alcanzarle responsabilidad por los cuales son sancionados con Multas en casos administrativos, en algunos otros son víctimas de los hackers, con millonarias pérdidas.

10. **¿Cómo se puede evitar el delito de fraude informático?** Una de las maneras es mayor difusión de este tipo de delitos a fin de que los usuarios no caigan en errores que puedan permitir este tipo de delitos y en cuanto a las entidades bancarias mayor implementación con sus sistemas de seguridad.

Nombre del entrevistado	Sello y firma
Miguel Ángel Durand Ramírez	MIGUEL A. DURAND RAMÍREZ ABOGADO Reg. CAL N° 19050

GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Entrevistado (a):

.....Abg.ANDREA DAYSI HUIZA CHAUCA

Edad: 28..... años Sexo: .....FEMENINO.....

.....Fecha:30/06/2023 .....

Objetivo general: Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022

1. ¿Explique Ud. si el delito de Fraude Informático regula la responsabilidad penal de las entidades financieras?

Al respecto debo indicar que el delito de Fraude Informático está regulado por la Ley N° 30096, conocida como la Ley de Delitos Informáticos. Esta ley establece los delitos informáticos y las penas correspondientes, pero no regula específicamente la responsabilidad penal de las entidades financieras de manera exclusiva.

Sin embargo, en el Perú, las entidades financieras pueden ser consideradas responsables penalmente por su participación en casos de fraude informático en virtud de otras disposiciones legales y principios generales del derecho penal. La responsabilidad penal de las entidades financieras puede basarse en teorías como la responsabilidad por el actuar de sus empleados en el curso de su actividad, la responsabilidad por omisión en la implementación de medidas de seguridad o la responsabilidad por el beneficio obtenido a través del fraude.

Es importante destacar que la responsabilidad penal de las entidades financieras dependerá de las circunstancias específicas del caso y de la interpretación de las leyes y regulaciones aplicables por parte de los tribunales peruanos. Además, existen normativas y regulaciones específicas que rigen el ámbito financiero y establecen obligaciones y responsabilidades para las entidades financieras en relación con la prevención y detección de delitos financieros, como el lavado de activos y el financiamiento del terrorismo.

2. ¿Explique Ud. Si el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiera?

Considero que el tratamiento del delito de fraude informático si puede tener repercusiones significativas en los sistemas de seguridad financiera, toda vez que el

fraude informático puede afectar la integridad, confidencialidad y disponibilidad de la información financiera, así como comprometer la seguridad de los sistemas y transacciones electrónicas, más aun teniendo en cuenta que en el ámbito financiero, la confianza y la seguridad son fundamentales para el buen funcionamiento de los mercados y la protección de los derechos e intereses de los usuarios.

.....

3. ¿Señale Ud. si el delito de Fraude Informático regula responsabilidad penal por la falta de implementación de sistemas de seguridad financiera?

Respecto a la interrogante planteada se debo indicar que el delito de Fraude Informático en el Perú no regula específicamente la responsabilidad penal por falta de implementación de sistemas de seguridad financiera. El delito de Fraude Informático se centra principalmente en la manipulación o alteración ilícita de datos electrónicos con el fin de obtener un beneficio económico o causar perjuicios a terceros. Sin embargo, en el contexto de las entidades financieras y la implementación de sistemas de seguridad, existen otras disposiciones legales y regulaciones que establecen obligaciones y responsabilidades para proteger la integridad y confidencialidad de la información financiera.

.....

4. ¿Cree Ud. que es posible determinar responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático.?

Sobre el particular puedo decir que es posible determinar la responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático en el Perú, siempre y cuando se cumplan ciertos requisitos legales. En el Perú, el delito de fraude informático está regulado por la Ley N°30096, que establece diversas conductas delictivas relacionadas con el uso indebido de sistemas y datos informáticos. Entre estas conductas, se encuentra el robo de datos, que implica la apropiación o sustracción ilícita de información electrónica almacenada o transmitida a través de sistemas informáticos.

En el caso de las entidades financieras, si se demuestra que han participado activamente en el robo de datos o han facilitado intencionalmente dicha conducta delictiva, pueden ser consideradas responsables penalmente. Esto puede ocurrir si, por ejemplo, un empleado de la entidad financiera está involucrado directamente en el robo de datos o si la entidad financiera no ha implementado las medidas de seguridad adecuadas para proteger la información de sus clientes y ha permitido la vulneración de los sistemas.

.....

5. ¿Puede Ud. indicar de acuerdo a su experiencia qué tipo de responsabilidad se ha logrado identificar en el delito de fraude informático respecto a las entidades financieras?

En el delito de fraude informático respecto a las entidades financieras en el Perú, se ha logrado identificar responsabilidad penal por participación directa en el delito o por facilitar intencionalmente su comisión. Asimismo, se ha establecido responsabilidad por omisión cuando la entidad financiera no implementa medidas de seguridad adecuadas para prevenir el fraude informático. Además, las entidades financieras pueden enfrentar sanciones administrativas y responsabilidad civil por los daños y perjuicios causados a los afectados.

.....

6. ¿Considera Ud. que las entidades financieras tienen identificados los riesgos de los sistemas de seguridad financiero?

Puedo decirte que las entidades financieras en el Perú están conscientes de los riesgos asociados a los sistemas de seguridad financiera. Estas entidades suelen tener identificados los riesgos y están comprometidas con la implementación de medidas adecuadas para mitigarlos. Las entidades financieras están sujetas a regulaciones y supervisión por parte de entidades como la Superintendencia de Banca, Seguros y AFP (SBS) para asegurar que se cumplan los estándares de seguridad y protección de datos. Sin embargo, es importante reconocer que los riesgos pueden evolucionar constantemente y requerir actualizaciones continuas en las medidas de seguridad.

.....

7. ¿Cree Ud. que las entidades financieras utilizan sistemas de seguridad adecuados de control y seguimiento para evitar vulneraciones a la base de datos de sus usuarios?

Debo indicar que si bien implementan medidas de seguridad tecnológicas, como firewalls, encriptación y sistemas de detección de intrusos, así como políticas y procedimientos internos para prevenir y responder a las vulneraciones de seguridad. Sin embargo, es importante destacar que la efectividad de estos sistemas puede depender de factores como la evolución de las amenazas cibernéticas y la capacidad de adaptación de las entidades financieras para mantenerse al día con las mejores prácticas de seguridad, por lo que consider que las entidades financieras no utilizan sistemas de seguridad adecuados.

.....

8. ¿Considera Ud. que los sistemas de seguridad informático

establecidos en la norma nacional e internacional son suficientes para salvaguardar la base de datos de las entidades financieras?

Considero que no, puesto que como se ha venido advirtiendo en los medios de comunicación y en las denuncias efectuadas tanto a nivel nacional como mundial los delitos informáticos han venido aumentando a lo largo del tiempo.....

.....

9. ¿Cree Ud. la vulneración de los sistemas de seguridad financiera son solo de responsabilidad del hacker o también les alcanzaría responsabilidad a las entidades bancarias?

Debo indicar que la responsabilidad por la vulneración de los sistemas de seguridad financiera en el Perú puede recaer tanto en los hackers como en las entidades bancarias, dependiendo de las circunstancias específicas del caso.

Los hackers que llevan a cabo la vulneración de los sistemas con el propósito de acceder de forma ilícita a información financiera y causar perjuicio a terceros, son los responsables directos de sus acciones y pueden ser sujetos a responsabilidad penal por sus actos delictivos.

Por otro lado, las entidades bancarias también pueden ser consideradas responsables si se demuestra que han incumplido con su deber de implementar medidas de seguridad adecuadas para proteger la información financiera de sus clientes. Esto podría ocurrir si se determina que las entidades bancarias no han adoptado las medidas de seguridad tecnológicas necesarias, han sido negligentes en el mantenimiento y actualización de sus sistemas, o han permitido el acceso no autorizado a la información de sus clientes debido a deficiencias en sus procedimientos internos.

Es importante tener en cuenta que las entidades bancarias tienen la responsabilidad legal y ética de salvaguardar la información confidencial de sus clientes y de implementar medidas de seguridad adecuadas para prevenir la vulneración de sus sistemas. Sin embargo, la determinación de la responsabilidad específica en cada caso dependerá de las pruebas presentadas y de la interpretación de las leyes y regulaciones aplicables.

.....

10. ¿Cómo se puede evitar el delito de fraude informático?

a) Implementar medidas de seguridad adecuadas: Las entidades y usuarios deben utilizar sistemas de seguridad robustos, como firewalls, encriptación de datos, sistemas de detección de intrusos y software de protección contra malware. Asimismo, es importante mantener actualizados los sistemas operativos y aplicaciones para remediar posibles vulnerabilidades.

b) Educar y concientizar a los usuarios: Las entidades y usuarios deben recibir capacitación sobre las mejores prácticas de seguridad cibernética, como el uso de contraseñas seguras, evitar el acceso a sitios web y correos electrónicos sospechosos, y no compartir información confidencial a través de canales no seguros.

c) Establecer políticas y procedimientos internos: Las entidades deben implementar políticas y procedimientos claros en materia de seguridad de la información, incluyendo la gestión de contraseñas, el acceso a datos confidenciales y el manejo de incidentes de seguridad. Estas políticas deben ser comunicadas y cumplidas por todos los empleados.

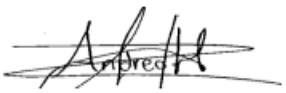
d) Realizar auditorías y pruebas de seguridad: Las entidades deben llevar a cabo auditorías regulares de seguridad informática y realizar pruebas de penetración para identificar posibles vulnerabilidades en los sistemas. Esto permitirá corregir las deficiencias y fortalecer la seguridad.

e) Mantenerse actualizado con las regulaciones y mejores prácticas: Las entidades deben estar al tanto de las regulaciones vigentes en materia de seguridad informática y cumplir con los estándares y directrices establecidos por los organismos regulatorios competentes. Además, es importante seguir las mejores prácticas de seguridad recomendadas por expertos en la industria.

f) Establecer mecanismos de respuesta a incidentes: Las entidades deben tener planes de contingencia y mecanismos de respuesta a incidentes para actuar rápidamente en caso de una vulneración de seguridad. Esto incluye la notificación oportuna a las autoridades competentes y a los usuarios afectados.

g) Monitorear y detectar actividades sospechosas: Las entidades deben implementar sistemas de monitoreo y detección de actividades sospechosas en sus redes y sistemas, con el fin de identificar y responder rápidamente a posibles ataques o intrusiones.

.....

Nombre del entrevistado	**Sello y firma**
ABG. ANDREA DAYSI HUIZA CHAUCA	 CAL N.°83370

GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE FRAUDE INFORMATICO EN LOS SISTEMAS DE SEGURIDAD FINANCIERO, DIRIGIDA A PROFESIONALES ESPECIALISTAS EN DERECHO PENAL Y PROCESAL PENAL

Entrevistado (a):

JUDIT MARIBEL PURIZACA SANCHEZ

Edad: 29 años Sexo: F .....Fecha: 25.06.2023

Objetivo general: Analizar de qué manera el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiero que incrementa las denuncias, distrito fiscal Lima Centro 2022

1. ¿Explique Ud. si el delito de Fraude Informático regula la responsabilidad penal de las entidades financieras?

El delito de fraude informático actualmente regulado en una ley penal especial no contempla de forma expresa la responsabilidad penal de las entidades financieras. Si bien existen pronunciamientos del ente regulador (SBS) sobre la falta de diligencia en operaciones bancarias, dicha regulación no alcanza el ámbito penal.

.....

2. ¿Explique Ud. Si el tratamiento del delito de fraude informático repercute en los sistemas de seguridad financiera?

El alcance del delitos e fraude informático sí repercute en los sistemas de seguridad financiera, dado que muchas de estas modalidades se realizan mediante la alteración o clonación de datos personales mediante medios informáticos. Así, los ciberdelincuentes logran vulnerar los sistemas de seguridad de los bancos para disponer del dinero de terceros.

.....

3. ¿Señale Ud. si el delito de Fraude Informático regula responsabilidad penal por la falta de implementación de sistemas de seguridad financiera?

Actualmente solo se encuentra regulada la responsabilidad administrativa por falta de implementación de los mecanismos necesarios para la seguridad financiera (o Compliance); sin embargo, existe la responsabilidad penal de la persona jurídica cuando hubiera participado en la comisión de un delito en beneficio de la misma empresa, para lo cual la se aplican las consecuencias accesorias.

4. ¿Cree Ud. que es posible determinar responsabilidad penal de las entidades financieras por el robo de datos tipificado en el delito de fraude informático.?

Existen avances importantes en relación a la responsabilidad administrativa y penal de la persona jurídica, dado que la realidad nos demuestra que para muchas operación financieras los bancos no agilizan todos los mecanismos de verificación que demuestren que dicha operación fue segura. Por el contrario, incluso en muchas ocasiones se ha advertido que dentro de los mismos bancos existen trabajadores que extraen datos personales del usuario.

.....

5. ¿Puede Ud. indicar de acuerdo a su experiencia qué tipo de responsabilidad se ha logrado identificar en el delito de fraude informático respecto a las entidades financieras?

En mi experiencia no he tenido la oportunidad de conocer casos penales sobre responsabilidad penal de entidades del sistema financiero por delitos informáticos.

.....

6. ¿Considera Ud. que las entidades financieras tienen identificados los riesgos de los sistemas de seguridad financiero?

Es probable que algunas entidades financieras del sistema financiero tengan identificados los riesgos de los sistemas de seguridad financiero mediante capacitaciones y exigencias de la SBS.

.....

7. ¿Cree Ud. que las entidades financieras utilizan sistemas de seguridad adecuados de control y seguimiento para evitar vulneraciones a la base de datos de sus usuarios?

Es probable que algunas entidades financieras tengan implementados sistemas de seguridad como el Compliance y certificaciones internacionales para fines relacionados.

.....

8. ¿Considera Ud. que los sistemas de seguridad informático establecidos en la norma nacional e internacional son suficientes para salvaguardar la base de datos de las entidades financieras?

Si bien existen sistemas de seguridad internacional y nacional, la practica denota que cada vez existen nuevas modalidades de vulneración de los sistemas de seguridad; por lo que los mecanismos necesitan ser adecuados y mejorados constantemente.

.....

9. ¿Cree Ud. la vulneración de los sistemas de seguridad financiera son solo de responsabilidad del hacker o también les alcanzaría responsabilidad a las entidades bancarias?

Existen acciones que deberían estar a cargo de las entidades bancarias tales como a anulación inmediata de operaciones no identificadas por el usuario, activación inmediata de mecanismos de verificación de la identidad del usuario, filtros de seguridad, determinación de tiempos para resolución de quejas y reclamos por fraude informático y hasta devolución de aportes por operaciones no autorizadas por usuarios donde no se haya demostrado que la entidad bancaria haya activado todos los mecanismos de seguridad y actuado con diligencia.

.....

10. ¿Cómo se puede evitar el delito de fraude informático?

Mediante la implementación de suficientes programas de cumplimiento normativo, certificaciones internacionales, supervisión y auditoria constante, implementación de procesos ágiles para la atención de quejas y reclamos por delitos informáticos, etc.

.....

Nombre del entrevistado	**Sello y firma**
JUDIT MARIBEL PURIZACA SANCHEZ	

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN

3° Despacho Provincial de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro
<3despachociberdelincuencialimacentro@mpfn.gob.pe>

EXP. 2207-2022 SENTENCIA DE TERMINACION ANTICIPADA

2 mensajes

Da Jessica 01.4490-2022

Fiorella Rubi Tipian De la Cruz <ftipian@pj.gob.pe> 20 de junio de 2023, 13:10
Para: 3despachociberdelincuencialimacentro@mpfn.gob.pe, efloresdn@mpfn.gob.pe

PODER JUDICIAL DE LA CORTE SUPERIOR DE JUSTICIA DE LIMA CENTRO

Por encargo del Vigésimo Cuarto Juzgado de Investigación Preparatoria, se le remite la Sentencia de Terminación Anticipada del exp. 2207-2022.

Se le adjunta:
- RESOLUCIÓN TRES

--

PODER JUDICIAL DEL PERÚ

Fiorella Rubi Tipian De la Cruz

Asistente Jurisdiccional - Sede Iquitos

8° al 28° Juzgado de Investigación Preparatoria

Módulo Penal - NCPP

Corte Superior de Justicia de Lima

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN
3° Despacho Provincial de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro
20 JUN 2023
RECIBIDO
HORA: 14:49 FIRMA: FOLIOS: 09

2207.pdf
345K

3° Despacho Provincial de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro <3despachociberdelincuencialimacentro@mpfn.gob.pe> 20 de junio de 2023, 13:15
Para: Fiorella Rubi Tipian De la Cruz <ftipian@pj.gob.pe>

RECIBIDO
[Texto citado oculto]
--

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN

3° DESPACHO PROVINCIAL DE LA FISCALÍA CORPORATIVA ESPECIALIZADA EN CIBERDELINCUENCIA DE LIMA CENTRO.
Doña Catalina 498 - Santiago de Surco.
Teléfono: (01) 625 5555 - Anexo: 2521

Correo: 3despachociberdelincuencialimacentro@mpfn.gob.pe

NOTA: LOS CORREOS REMITIDOS FUERA DEL HORARIO ESTABLECIDO DE LUNES A VIERNES DE 08:00 AM A 16:45 PM, SE CONSIDERAN PARA EL SIGUIENTE DÍA HÁBIL SEGÚN EL ORDEN DE LLEGADA, EN CASO SEA ENVIADO EL VIERNES FUERA DE HORARIO, SE RECIBIRÁN A PARTIR DEL DÍA LUNES SIGUIENTE DE ACUERDO AL ORDEN DE LLEGADA EN LA BANDEJA DE CORREOS.

PODER JUDICIAL
DEL PERÚ

VIGÉSIMO CUARTO JUZGADO DE
INVESTIGACIÓN PREPARATORIA DE LIMA

CORTE SUPERIOR DE JUSTICIA DE LIMA

Expediente:	N° 02207-2022-1-1826-JR-PE-24
Juez:	CRISTÓBAL ANTONIO SOLÍS MONTAÑEZ
Especialista de Causa:	CARLOS JOAO LUPERDI CÁRDENAS
Investigado:	DIEGO CAVA VALENTÍN
Delitos:	CONTRA EL PATRIMONIO – FRAUDE INFORMÁTICO CONTRA LA FE PÚBLICA – FALSEDAD GENÉRICA
Agraviados:	MARÍA LAURA DEL RÍO SÁNCHEZ DIEGO ALBERTO ROMANI CHIA
Requirente:	FISCALÍA CORPORATIVA ESPECIALIZADA EN CIBERDELINCUENCIA DE LIMA CENTRO, TERCER DESPACHO.

SENTENCIA ANTICIPADA

RESOLUCION N° 03
Lima, veintinueve de abril
del año dos mil veintidós.-

De los **ACTUADOS** en el Proceso **Y OÍDO** la fundamentación del Requerimiento de Terminación Anticipada formulado por la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, Tercer Despacho; sustentada oralmente en la audiencia de su propósito, con la asistencia del imputado Diego Cava Valentín y de su abogada defensora; por lo que corresponde emitir el pronunciamiento que la resuelve; y,

SOBRE LOS DATOS PERSONALES DE LA INVESTIGADA:

1) DIEGO CAVA VALENTÍN, sexo masculino, identificado con DNI N° 77536851, fecha de nacimiento: 26 de mayo de 1995, lugar de nacimiento: distrito, provincia y departamento de Lima, edad 26 años, estado civil: soltero grado de instrucción: Secundaria Completa, nombre del padre: Víctor Manuel, nombre de la madre: Jessy Iveth María, y con domicilio real en el Jirón Independencia N° 472 del distrito de Breña, provincia y departamento de Lima.

I. CONSIDERANDOS:

PRIMERO: LA AUTONOMÍA CONSTITUCIONAL DE LA FUNCIÓN DE INVESTIGACIÓN DEL MINISTERIO PÚBLICO.-

El Ministerio Público, es una de las instituciones centrales del Poder Jurisdiccional del Estado que tiene como función principal la "acción judicial en defensa de la legalidad y de los intereses públicos". La Constitución también le reconoce como función "conducir desde su

inicio la investigación del delito" y "ejercitar la acción penal", conforme lo regula en su artículo 159°:

"Artículo 159.- Corresponde al Ministerio Público:

1. *Promover de oficio, o a petición de parte, la acción judicial en defensa de la legalidad y de los intereses públicos tutelados por el Derecho.*
2. *(…)*
3. *(…)*
4. *"Conducir desde su inicio la investigación del delito. Con tal propósito, la Policía Nacional está obligada a cumplir los mandatos del Ministerio Público en el ámbito de su función.*
5. *"Ejercitar la acción penal de oficio o a petición de parte.*

(…)"

El conjunto de estas funciones puede identificarse como funciones fiscales dentro del Estado. Le corresponden al Ministerio Público en forma exclusiva cumplir con dichas funciones dado que ninguna otra institución o poder de Estado tiene. La "defensa de la legalidad y los intereses públicos" está relacionado con la defensa de la sociedad en temas de infracciones sociales o delitos. Para ello la Constitución le otorga la atribución y obligación de "conducir desde un inicio la investigación del delito", incluyéndose todo tipo de delitos (entre particulares y aquellos que involucren a funcionarios públicos). En el mismo sentido la Constitución le otorga al Ministerio Público la atribución y obligación de "ejercer la acción penal de oficio o a petición de parte", lo que significa ser el titular de la acción penal. Ninguna institución u órgano del Poder Legislativo o del Poder Ejecutivo, incluidas las instituciones autónomas del Estado, tiene estas facultades constitucionales.

Para garantizar el ejercicio de estas funciones del Ministerio Público, la Constitución le otorga autonomía institucional (artículo 158° de la Constitución), pero sobre todo reconoce en los miembros del Ministerio Público los mismos derechos, prerrogativas y obligaciones que los miembros del Poder Judicial. Esto significa que los miembros del Ministerio Público participan de la unidad y exclusividad de la función jurisdiccional, prohibiendo a toda autoridad de los otros poderes del Estado (incluidos los congresistas) interferir en sus funciones (artículo 139° de la Constitución). Esta regulación constitucional confirma que la labor del Ministerio Público complementa a la del Poder Judicial, haciendo en ambos el Poder Jurisdiccional del Estado.

SEGUNDO: EL PROCESO ESPECIAL DE TERMINACIÓN ANTICIPADA COMO MECANISMO DE SIMPLIFICACIÓN PROCESAL.-

El Código Procesal Penal (Decreto Legislativo N° 957) ha regulado mecanismos de simplificación procesal con la finalidad de racionalizar eficazmente el trámite de las etapas del proceso penal para los delitos de mínima lesividad, contribuyendo de esta forma con la descongestión del sistema de justicia penal y el sistema penitenciario, respecto de las causas penales cuyos procesados que sin contar con antecedentes penales previos tengan un alto

grado de reinserción social y, se obliguen a reparar el daño ocasionado como consecuencia de su comportamiento ilícito. En razón a las motivaciones expuestas, se han establecido como procedimientos especiales de simplificación procesal: Acusación Directa, Proceso Inmediato, Terminación Anticipada, Conclusión Anticipada y Colaboración Eficaz; en los cuales se ponen de manifiesto los principios procesales de celeridad y economía procesal como una solución eficaz y eficiente para resolver el conflicto penal de los ciudadanos que incurren en conductas ilícitas que afectan bienes jurídicos protegidos por el Estado.

Es oportuno mencionar que en los procedimientos de simplificación procesal resulta de capital importancia **el principio de consenso penal**, por el cual las partes procesales debidamente constituidas en el proceso penal tienen un rol de primacía respecto de sus pretensiones procesales que los habilita a conferenciar, y eventualmente, celebrar acuerdos provisionales sobre los hechos ilícitos materia de investigación, la calificación jurídica y tipicidad de la conducta ilícita y, la pretensión resarcitoria; todo ello con prescindencia de la ley ritual aplicable al proceso común, pero bajo el control jurisdiccional del Juzgador de la Investigación Preparatoria, quien verifica la legalidad de los términos del acuerdo provisional para su posterior homologación judicial.

Sobre la naturaleza jurídica de la Terminación Anticipada debe tenerse en cuenta que: "El proceso especial de terminación anticipada es una institución consensual que permite la solución del conflicto jurídico penal, en forma alternativa y hasta preferente por su rapidez y eficacia a la conclusión tradicional en un juicio público y contradictorio. Es una suerte de transacción previa a la etapa final de juzgamiento que evidentemente contiene concesiones recíprocas, el imputado negocia la admisión de culpabilidad y el Fiscal negocia una reducción de la pena."[1]. Por su parte, los presupuestos normativos de procedencia están regulados en el numeral 6 del artículo 468° del Código Procesal Penal (Decreto Legislativo N° 957) que prescribe: "6. Si el Juez considera que la calificación jurídica del hecho punible y la pena a imponer, de conformidad con lo acordado, son razonables y obran elementos de convicción suficientes, dispondrá en la sentencia la aplicación de la pena indicada, la reparación civil y las consecuencias accesorias que correspondan enunciando en su parte resolutiva que ha habido acuerdo. Rige lo dispuesto en el artículo 398."

TERCERO: LA DOCTRINA LEGAL ESTABLECIDA EN EL ACUERDO PLENARIO N° 5–2009/CJ–116.-

En el desarrollo del V Pleno Jurisdiccional de las Salas Penales Permanente y Transitorias de las Salas Penales Permanente y Transitorias de la Corte Suprema de Justicia de la República, se emitió el Acuerdo Plenario N° 5-2009/CJ-116 de fecha 13 de noviembre de

[1] Taboada Pilco, Giammpol; "El Proceso Especial de Terminación Anticipada en el Nuevo Código Procesal Penal. Especial referencia a su aplicación en el Distrito Judicial de La Libertad.". Recuperado de: https://biblioteca.cejamericas.org/bitstream/handle/2015/4979/Terminacion_anticipada.pdf?sequence=1&isAllowed=y

2009 (Asunto: Proceso de Terminación Anticipada: Aspectos Esenciales); en cuyos fundamentos jurídicos se ha establecido la doctrina legal aplicable al presente caso, la cual se expone a continuación:

> "8°. El proceso de terminación anticipada atraviesa diversas etapas o fases, que va desde la calificación de la solicitud de terminación anticipada –sin que para ello o para la continuación del referido proceso corresponda realizar diligencia preliminar alguna o tomar una declaración al imputado- [fase inicial], hasta la realización de la audiencia respectiva [fase principal] y la consecuente emisión de la decisión resolutoria correspondiente: auto desaprobatorio del acuerdo o sentencia anticipad [fase decisoria]. Es claro, por lo demás, que audiencia preparatoria es privada, cuya justificación estriba en que es consecuencia del carácter de publicidad relativa de la investigación preparatoria y constituye, desde la perspectiva del imputado, uno de los efectos benéficos de este proceso especial, quien apunta a que su caso no se ventile públicamente.
>
> Es condición de la realización de la citada audiencia que la solicitud de terminación anticipada pase el examen judicial de admisibilidad y procedencia. Además, el Juez ha de revisar si el imputado tiene debido conocimiento de los alcances y consecuencia del acuerdo al que puede llegar –es, precisamente, el segundo paso de la audiencia, inmediatamente después de la presentación de los cargos por la Fiscalía-. El consentimiento del imputado, visto el carácter dispositivo de la pretensión o los efectos que entraña, ha de ser libre, voluntario –sin presiones o amenazas-, informado, prestado con el auxilio de un abogado defensor, y con pleno conocimiento de lo que hace o deja de hacer y a lo que se somete una vez que acepta el acuerdo.
>
> 9°. Si es que las partes arriban a un acuerdo –que tiene como presupuesto la afirmación de la responsabilidad penal del imputado y, como condición, la precisión de las consecuencias jurídico penales y civiles correspondientes, en perfecta armonía con el principio de legalidad-, corresponde al Juez en ejercicio de su potestad jurisdiccional llevar a cabo los pertinentes controles acerca de la legalidad del acuerdo y de la razonabilidad de la pena.
>
> 10°. El control de legalidad del acuerdo se expresa en tres planos diferentes:
>
> A. El ámbito de la tipicidad o calificación jurídico penal, en relación a los hechos objeto de la causa y a las circunstancias que rodean al hecho punible.
>
> B. El ámbito de la legalidad de la pena y, en su caso, a su correspondencia con los parámetros, mínimo y máximo, que fluyen del tipo legal aplicado y de las circunstancias modificativas de la responsabilidad –esto es lo que se denomina „pena básica"-. También el juicio de legalidad alcanza al respeto de los ámbitos legalmente definidos de la reparación civil –siendo del caso resaltar que en este extremo prima por completo la disposición sobre el objeto civil- y de las consecuencias accesorias.

C. La exigencia de una suficiente actividad indiciaria. Ello implica que las actuaciones o diligencias de la investigación permitan concluir que existe base suficiente –probabilidad delictiva- (i) de la comisión de los hechos imputados y de su vinculación con el imputado, y (ii) que están presentes todos los presupuestos de la punibilidad y de la perseguibilidad.

11°. El control de la razonabilidad de la pena está centrado en el examen del quantum de la pena y de la reparación civil objeto del acuerdo. El Juez ha de realizar una valoración que evite que se vulnere, por exceso o por defecto, el principio de proporcionalidad, se lesione la finalidad de la pena o se afecte indebidamente los derechos e intereses legítimos de la víctima. Por consiguiente, sólo podrá rechazar el acuerdo si de modo palmario o evidente se estipule una pena o una reparación civil evidentemente desproporcionada o que en el caso de la pena se lesione ostensiblemente el principio preventivo."

CUARTO: LOS FUNDAMENTOS FACTICOS Y LAS DILIGENCIAS REALIZADAS EN LA ETAPA DE INVESTIGACIÓN PREPARATORIA.-

Conforme se verifica del Requerimiento de Terminación Anticipada interpuesto por la Sétima Fiscalía Corporativa Penal Cercado de Lima – Breña – Rímac – Jesús María, Primer Despacho; los fundamentos facticos y los elementos de convicción que fueran sustentados oralmente en la audiencia de su propósito, son los que a continuación se indican:

4.1. La Imputación Fáctica: se atribuye al investigado Alfredo Arturo Vega Javier lo siguiente:

- **Hechos Precedentes.-** El 04 de abril de 2022, el investigado Diego Cava Valentín ingresó a la base de datos llamada SENTINEL, mediante un código de usuario y clave que adquirió de manera ilícita en la Av. Wilson ubicada en el Cercado de Lima por el monto de S/200.00, con la finalidad de obtener información crediticia de una persona en particular. Una vez que logró ingresar a dicha base de datos, colocó números al azar y obtuvo el DNI N° 07761701 de titularidad de María Laura Del Rio Sánchez, quien cumplía con los requisitos para adquirir una tarjeta de crédito virtual del banco Falabella, por lo que, procedió a ingresar a la página de dicha entidad bancaria y registrar los siguientes datos: número de DNI, dirección, lugar de trabajo, monto de remuneración, entre otros; obteniendo un usuario (DNI) y una clave de seguridad. Posteriormente, el mismo día, el investigado descargó en su celular el App del Banco Falabella, donde obtuvo el número de tarjeta, fecha de vencimiento, código de seguridad y nombre del titular (María Laura Del Rio Sánchez); y, acto seguido descargo el aplicativo FPAY donde se registró los datos de la tarjeta a nombre de María Laura del Rio Sánchez.

- **Hechos Concomitantes.-** Ese mismo día, a las 18:00 horas aproximadamente, el investigado Diego Cava Valentín, se constituyó a la tienda "Saga Falabella" ubicada en Av. Paseo de la República N° 3220 en el distrito de San Isidro; dirigiéndose al área de ropa y hogar, cogiendo: 3 medias marca Adidas, 1 pijama, 1 polera, 1 pantalón, 1 buzo y 1 juego de sabanas. Luego se dirigió al área de electro solicitando un celular de marca Xiomi de último modelo, requiriendo a señorita de atención al cliente que le entregue el equipo celular a efectos de realizar el pago en las cajas de autoservicio, empero ésta le indicó la existencia de un procedimiento respecto al pago de celulares, en base al cual se le hacía entrega de un código a fin que cancele el producto y con dicho comprobante recién podían hacerle entrega del celular; sin embargo, el investigado insistió a que realizaría el pago en la caja de autoservicio, pedido al que no accedieron, dicha actitud levantó las sospechas de Milton Núñez Sono, personal a cargo de las cámaras de seguridad de la Tienda seguida los movimiento de Diego Cava Valentín, se dirigió al segundo piso de la tienda donde se encuentran ubicadas las cajas de autoservicio, procediendo a ingresar el DNI 07761701 y registrar todos los productos antes mencionados, obteniendo un código QR que salió en la pantalla del cajero de autoservicio, por lo que, procedió a realizar dicho pago con el uso del aplicativo FPAY desde su celular por el monto de S/. 888.30 soles. Acto seguido, introduce las prendas en las bolsas con el logotipo de Saga Falabella de manera rápida y nerviosa, sin percatarse que no le habla retirado los dispositivo de seguridad de dichos productos, hecho que permitió que el asistente de prevención de la tienda Milton Núñez Sono intervenga de manera inmediata, solicitándole el comprobante de pago para poder ayudarlo, preguntándole si el DNI 07761701 era de él, indicando el investigado que era de su tía, y que ella le había dado la clave y usuario para que realice la compra, a lo que el personal de prevención de la tienda le preguntó si su tía se encontraba en el establecimiento comercial, refiriéndole el investigado que no, por lo que el personal de prevención le solicitó su DNI, identificándose en ese momento con el DNI N° 76350141 perteneciente al ciudadano Diego Alberto Romaní Chía, por lo que al visualizar el asistente de prevención la fotografía del DNI en mención, los rasgos físicos no coincidían (rostro), indicándole al investigado que lo acompañe al área de prevención, y que llame a su tía para que confirme que efectivamente autorizó dicha compra, llamando presuntamente el investigado por teléfono de manera reiterativa sin respuesta alguna. En esa circunstancias estando en el área de Prevención ubicado en el sótano de la tienda Saga Falabella, el asistente de dicha área

reportó el hecho a sus compañeros quienes llamaron a personal de la Policía Nacional del Perú, reportando lo sucedido y le dijeron al investigado que el DNI mostrado no es él, por lo que procedió a sacar de su billetera su DNI en físico con N°77536851, del cual si era titular; luego en el área de prevención verifican a quien le pertenece el DNI N° 07761701 que aparece en la boleta de compra de los productos, el cual pertenecería a María Laura del Rio Sánchez, solicitándose al investigado se comunique con ella, pero éste indicó que se le había agotado la batería de su celular.

- **Hechos Posteriores.-** Personal policial procedió a su detención por haber hecho uso de los datos de la ciudadana María Laura del Rio Sánchez mediante el aplicativo en mención para realizar la compra y usar el DNI de Diego Alberto Romaní Chía para identificarse. Asimismo, la agraviada María Laura del Río Sánchez ha presentado su hoja de reclamación N° 1-123453493548 al Banco Falabella S. A. en donde indica que no reconoce haber contratado ningún producto CMR con número de cuenta 000001393787, ni cuentas con FPAY.

4.2. **Los actos de investigación realizados en la etapa de investigación preparatoria:** sustentados oralmente por la Fiscalía requirente son los que a continuación se indican: a) El acta de Intervención Policial del día 4 de abril del año 2022, en la cual se detalle las formas y circunstancias de su intervención; b) El acta de Intervención N° 91 de fecha 4 de abril del año 2022; c) El Acta de registro personal de incautación de especies, en la cual luego de haberse practicado el registro personal del detenido Diego Cava Valentín, se verifica que se encontraba en posesión de un teléfono celular marca Apple modelo iPhone 8, color negro, un DNI N°76350141 que corresponde a Diego Alberto Romaní Chía, una tarjeta de crédito del banco BCP, una tarjeta de débito del banco Interbank, una billetera Renzo Costa y una licencia de conducir de moto lineal; d) El acta de perennización de prendas de fecha 4 de abril del año 2022, en el cual se deja constancia de las prendas adquiridas de manera ilícita por el investigador Diego Cava Valentín; e) El acta de perennización de celular de fecha 4 de abril del año 2022; f) La ficha de servicio de autentificación e identificación biométrica de Diego Cava Valentín identificado con número de DNI N° 77536851; g) La declaración del presunto agraviado Diego Alberto Romani Chía de fecha 5 de abril del año 2022, quien señala no conocer al investigador Diego acá Valentín y que en el mes de octubre del año 2021 tres personas con armas de fuego le arrebataron su maletín que contenía entre sus pertenencias justamente su documento Nacional de identidad; h) El Acta de Recepción y Lacrado de fecha 6 de abril del año 2022, mediante el cual se

resguarda un CD que contiene tres vídeos de imágenes de las cámaras de vigilancia del establecimiento comercial de la tienda Saga Falabella sede San Isidro en donde se registran en vídeo los movimientos realizados o el desplazamiento realizado por el investigador; i) El acta de des lacrado, visualización de videos y posterior lacrado de fecha 7 de abril del año 2022 en la cual se visualizan los tres vídeos que contenía el CD antes mencionado en relación a los desplazamientos realizados por el investigado; j) La declaración indagatoria de la presunta agraviada María Laura del Río Sánchez de fecha 6 de abril del año 2022, que manifiesta no conocer al investigador Diego Cava Valentín, así como tampoco al presunto agraviado Diego Alberto Romani Chia y refiere que no tiene tarjeta del banco Falabella; k) El acta de des lacrado de visualización de videos y posterior lacrado de fecha 8 de abril del año 2022, en la cual se visualizan los vídeos respecto a las imágenes del área de las cajas automáticas en donde se deja constancia que aparece la persona del investigado Diego Cava Valentín; y, l) La declaración de ampliación del investigador Diego Cava Valentín de fecha 10 de abril del año 2022, donde narra las formas y circunstancias en que se produjo el hecho delictivo y reconoce la comisión del hecho de fraude informático.

QUINTO: LOS FUNDAMENTOS EN CONTRAPOSICIÓN AL REQUERIMIENTO DE TERMINACIÓN ANTICIPADA.-

El Código Procesal Penal de 2004 (Artículos 98° a 106°) regula la institución procesal denominada Actor Civil, quien en resumida cuenta se puede definir como la víctima que ha formalizado su situación jurídica dentro del proceso penal a través de su constitución como actor civil, sin embargo en ausencia de éste, la ley establece que dicha titularidad será ejercida por el representante del Ministerio Público, persecutor del delito y quien se encargará de requerir el pago de la reparación civil correspondiente. Así también, la referida norma procesal establece las facultades[2] del actor civil, entre las que se cuentan: deducir nulidad de actuados, ofrecer medios de investigación y de prueba, participar en los actos de investigación y de prueba, intervenir en el juicio oral, interponer los recursos impugnatorios que la Ley prevé, intervenir -cuando corresponda- en el procedimiento para la imposición de medidas limitativas

[2] Código Procesal Penal (Decreto Legislativo N° 957)
Artículo 104° Facultades del actor civil.-
El actor civil, sin perjuicio de los derechos que se le reconocen al agraviado, está facultado para deducir nulidad de actuados, ofrecer medios de investigación y de prueba, participar en los actos de investigación y de prueba, intervenir en el juicio oral, interponer los recursos impugnatorios que la Ley prevé, intervenir -cuando corresponda- en el procedimiento para la imposición de medidas limitativas de derechos, y formular solicitudes en salvaguarda de su derecho.
Artículo 105° Facultades adicionales del actor civil.-
La actividad del actor civil comprenderá también la colaboración con el esclarecimiento del hecho delictivo y la intervención de su autor o participe, así como acreditar la reparación civil que pretende. No le está permitido pedir sanción.

de derechos, y formular solicitudes en salvaguarda de su derecho; teniendo como facultades adicionales: colaborar con el esclarecimiento del hecho delictivo y acreditar la reparación civil que pretende. No debiendo perderse de vista que la oportunidad para constituirse en Actor Civil es antes de la culminación de la Investigación Preparatoria.

Ahora bien, de los actuados en el presente proceso verifica el Juzgador que respecto al delito informático contra el patrimonio – fraude informático (hecho licito previsto y sancionado en el primer párrafo del artículo 8° de la Ley N° 300096: Ley de los Delitos Informáticos) y, delito contra la fe pública – falsedad genérica (hecho ilícito previsto y sancionado en el artículo 438° del Código Penal); respecto a los cuales, la parte agraviada no se encuentra constituida como Actor Civil, y no obstante haberse cumplido con trasladar el requerimiento de terminación anticipada, esta no ha cumplido con formular oposición al requerimiento del Ministerio Publico y, también se verifica que no han concurrido al desarrollo de la Audiencia de Terminación Anticipada.

SEXTO: EL ACUERDO PROVISIONAL DE TERMINACION ANTICIPADA Y LA EXPRESION DE CONFORMIDAD DE LA INVESTIGADA.-

En Audiencia de Terminación Anticipada el Ministerio Publico representado por la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, Tercer Despacho, sustentó oralmente los fundamentos facticos y jurídicos en el siguiente sentido:

6.1. La atribución de responsabilidad penal.- la imputación concreta contra el imputado Diego Cava Valentín, en relación a los hechos ocurridos el día 4 de abril de 2022 el imputado obtuvo una tarjeta de crédito virtual del Banco Falabella mediante el registro de los datos de número de DNI, dirección, lugar de trabajo, monto de remuneración, entre otros que le correspondían a la persona de María Laura Del Rio Sánchez, siendo que al suplantar la identidad de la persona antes indicada accede a un usuario (DNI) y una clave de seguridad; posteriormente, el mismo día, el investigado descargó en su celular el App del Banco Falabella, donde obtuvo el número de tarjeta, fecha de vencimiento, código de seguridad y nombre del titular (María Laura Del Rio Sánchez); y, acto seguido descargo el aplicativo FPAY donde se registró los datos de la tarjeta a nombre de María Laura del Rio Sánchez. En tal sentido, habiendo suplantado la identidad de la agraviada a través de medios informáticos, el imputado se constituye en la tienda "Saga Falabella" ubicada en Av. Paseo de la República N° 3220 en el distrito de San Isidro, realizando compras de prendas de vestir por el monto de S/. 888.30 soles, siendo que cuando pretendía de salir del referido establecimiento comercial el personal de prevención le pide su comprobante de pago y número de DNI, ante lo cual, el imputado se identifica con el DNI N° 76350141 perteneciente al ciudadano Diego Alberto Romaní Chía, por lo que al visualizar el asistente de

prevención la fotografía del DNI en mención, los rasgos físicos no coincidían (rostro).

6.2. **La calificación jurídica y la tipificación del hecho ilícito.-** la conducta desplegada por el imputado Diego Cava Valentín es en calidad de autor de los delitos:

Ley N° 30096: Ley de Delitos Informáticos, que prescribe:

Delitos Informáticos Contra El Patrimonio

"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. (...)"

Delito contra la Fe Publica – Falsedad Genérica, que prescribe:

"Artículo 438.- El que de cualquier otro modo que no esté especificado en los Capítulos precedentes, comete falsedad simulando, suponiendo, alterando la verdad intencionalmente y con perjuicio de terceros, por palabras, hechos o usurpando nombre, calidad o empleo que no le corresponde, suponiendo viva a una persona fallecida o que no ha existido o viceversa, será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años."

6.3. **Los elementos de convicción.-** son los que se han consignado de forma detallada en el cuarto considerando de la presente resolución.

6.4. **La determinación de la pena y circunstancias modificatorias.-** en atención a los tipos penales atribuidos al imputado se tiene lo siguiente:

Para Delitos Informáticos Contra El Patrimonio – Fraude Informático, se ha previsto la sanción penal de pena privativa de libertad con una pena abstracta no menor de 3 años ni mayor de 8 años; en ese sentido, se debe tener en cuenta que para establecer la pena concreta que le correspondería a Diego Cava Valentín en aplicación del sistema de tercios regulado en el numeral 1 del artículo 45°-A, al verificarse que tiene circunstancias atenuantes por no contar con antecedentes penales y, no se ha verificado circunstancias agravantes genéricas ni específicas; el representante del Ministerio Publico postula su pretensión punitiva en el primer tercio o tercio inferior (3 años a 4 años con 6 meses de pena privativa de libertad y de 60ª 90 días multa); por lo que, le correspondería al imputado Diego Cava Valentín tres (03) años de pena privativa de libertad y el pago de 60 días multa.

Para el delito contra la Fe Publica – Falsedad Genérica, se ha previsto la sanción penal de pena privativa de libertad con una pena abstracta no menor de 2 años ni mayor de 4 años; en ese sentido, se debe tener en cuenta que para establecer la pena concreta que le correspondería a Diego Cava Valentín en aplicación del

sistema de tercios regulado en el numeral 1 del artículo 45°-A, al verificarse que tiene circunstancias atenuantes por no contar con antecedentes penales y, no se ha verificado circunstancias agravantes genéricas ni específicas; el representante del Ministerio Publico postula su pretensión punitiva en el primer tercio o tercio inferior (02 años de pena privativa de libertad); por lo que, le correspondería al imputado Diego Cava Valentín dos (02) años de pena privativa de libertad.

Ahora bien, el Juzgador verifica de lo expuesto en los párrafos que anteceden que la conducta desplegada por el imputado Diego Cava Valentín ha materializado dos hechos punibles que son tipificados por la norma penal como delitos independientes entre sí, por lo que en aplicación de lo estipulado en el artículo 50° del Código Penal, por tratarse de un concurso real de delitos se debe proceder a la sumatoria de las penas, la cual arroja cinco (05) años de pena privativa de libertad y el pago de 60 días multa.

6.5. **La procedibilidad del beneficio premial.-** La procedibilidad del beneficio premial.- el primer párrafo del artículo 471° del Código Procesal Penal regula el beneficio de reducción de la pena en una sexta parte para el imputado que se acoge al proceso especial de Terminación Anticipada, con excepción para los casos en lo que al imputado se le atribuya la comisión de los delitos consignados en el tercer párrafo de la norma adjetiva acotada; en ese sentido, el fiscal requirente propone la aplicación del beneficio premial de reducción de la pena a favor del imputado Diego Cava Valentín, siendo que luego de realizado el cálculo respectivo se tiene que la pena a imponérsele es de cuatro (04) años de pena privativa de libertad y el pago de 50 días multa.

6.6. **La suspensión de la pena e imposición de reglas de conducta.-** el artículo 57° del Código Penal establece los presupuestos normativos para la suspensión de la pena, estos son: i) que la condena a imponerse no sea mayor a 4 años de pena privativa de libertad; ii) la naturaleza, el modo del hecho punible, la conducta procesal y la personalidad del agente que permita inferir que no volverá a cometer nuevo delito; y, iii) que el agente no tenga la condición de reincidente o habitual. En atención a lo normado, el representante del Ministerio Publico propone la suspensión de la ejecución de la pena a favor del imputado Diego Cava Valentín por un periodo de prueba de tres (03) años y con la imposición de reglas de conducta que se indican: a) Comparecer mensualmente al juzgado, personal y obligatoriamente, en forma virtual, para informar y justificar sus actividades, b) Reparar los daños ocasionados por el delito y cumplir con su pago fraccionado, conforme al cronograma establecido para el pago de la reparación civil, en caso de incumplimiento de una cuota, se procederá a solicitar la revocatoria de la pena, y c) No ausentarse de la localidad en la que reside sin conocimiento del Juzgado.

6.7. La pretensión reparatoria e identificación del agraviado.- conforme lo ha consignado el fiscal requirente, la parte agraviada son los ciudadanos María Laura del Río Sánchez y Diego Alberto Romani Chia, quienes no se han constituido en Actor Civil en el presente proceso; no obstante ello, se ha cumplido con trasladar el contenido del requerimiento de terminación anticipada y, citarla a la audiencia de su propósito; siendo así, se verifica que no ha concurrido al desarrollo del referido acto procesal, por lo que la legitimidad de la pretensión reparatoria aun la ostenta el Ministerio Publico, que postula como reparación civil la suma de un mil y 00/100 (S/. 1,000) soles a favor de María Laura del Río Sánchez y, doscientos y 00/100 (S/. 200) a favor de Diego Alberto Romani Chia; lo cual fue objeto de traslado a la defensa técnica del imputado Diego Cava Valentín, quien manifestó su conformidad conforme se registró en audio y video.

SÉTIMO: CONTROL JUDICIAL Y ANÁLISIS DE PROCEDENCIA DEL REQUERIMIENTO DE TERMINACIÓN ANTICIPADA.-

La formalización de la investigación preparatoria planteada por el Ministerio Publico se sustentó sobre la línea de investigación contra Diego Cava Valentín como presunto autor del delito informático contra el patrimonio – fraude informático (hecho licito previsto y sancionado en el primer párrafo del artículo 8° de la Ley N° 300096: Ley de los Delitos Informáticos) y, delito contra la fe pública – falsedad genérica (hecho ilícito previsto y sancionado en el artículo 438° del Código Penal). En ese sentido, respecto al hecho ilícito materia de la investigación preparatoria formalizada se procede a realizar el correspondiente controlo de legalidad en el siguiente sentido:

7.1. Control en el ámbito de la calificación jurídico penal y tipicidad del hecho ilícito.- el relato incriminatorio postulado por el Ministerio Publico se corrobora con los actos de investigación realizados que se han descrito en el cuarto considerando (ítem 4.2) de la presente resolución. En consecuencia, el juzgador verifica que la tesis incriminatoria del Ministerio Publico en su aspecto factico está acreditada con los suficientes elementos de convicción que se han reseñado en el cuarto considerando de la presente resolución; de igual modo la calificación jurídica de la conducta ilícita desplegada por el imputado Diego Cava Valentín ha superado el juicio de tipicidad, al comprobarse que se encuentra regulada como delito informático contra el patrimonio – fraude informático y, delito contra la fe pública – falsedad genérica.

7.2. La exigencia de una suficiente actividad indiciaria.- el juzgador verifica que los actos de la investigación preparatoria formalizada que se han detallado en el cuarto considerando de la presente resolución son pertinentes y útiles para establecer la existencia de indicios reveladores de la comisión de un hecho ilícito; que para efectos del presente caso se configura como delito informático contra

el patrimonio – fraude informático y, delito contra la fe pública – falsedad genérica.

7.3. **El control en el ámbito de la legalidad de la pena.-** habiendo cumplido el representante del Ministerio Publico con oralizar el requerimiento de terminación anticipada, el Juzgador verifica que el imputado Diego Cava Valentín no tiene antecedentes penales y judiciales, configurándose de este modo la existencia solo de circunstancias atenuantes que ameritan aplicar la pena abstracta dentro de los parámetros del tercio inferior: i) Para el delito informático contra el patrimonio – fraude informático tres (03) años de pena privativa de libertad y el pago de 50 días-multa, y ii) Para el delito contra la fe pública – falsedad genérica dos (02) años de pena privativa de libertad; por lo que: al tratarse de un concurso real de delitos procede aplicar la sumatoria de las penas, cuyo resultado es de cinco (05) años de pena privativa de libertad y el pago de 50 días multa. Así también, el juzgador verifica la procedencia de los beneficios premiales de reducción de un sexto por acogerse al proceso especial de terminación anticipada; cuya procedibilidad se ha comprobado de forma suficiente en el ítem 6.5 de la presente resolución. Por lo tanto, la pena que le corresponde imponer al imputado Diego Cava Valentín es de **cuatro (04) años de pena privativa de libertad con el carácter de suspendida, el pago de 50 días multa** y, la imposición de reglas de conducta.

7.4. **El control de razonabilidad de la pena y su aplicación.-** superado el control de legalidad de la pena aplicable y la procedencia de los beneficios de reducción de la pena por acogerse a la terminación anticipada, el Juzgador verifica el cumplimiento de los presupuestos normativos contenidos en el artículo 57° del Código Penal para la suspensión de la pena; debido a que la pena concreta a imponerse es menor a cuatro (04) años de pena privativa de libertad, la naturaleza del hecho ilícito es de mínima lesividad y de carácter patrimonial y, el imputado ha reconocido la autoría del delito que le atribuye el Ministerio Publico y su voluntad de resarcir el daño ocasionado, de igual modo, se ha evidenciado que no tiene la condición de reincidente o habitual; de esta forma se puede inferir válidamente que no volverá a cometer nuevo delito. En cuanto, a la aplicación de la pena será con el carácter de suspendida por un periodo de prueba de tres (03) años y, la imposición de reglas de conducta descritas en el ítem 6.6 de la presente resolución, bajo el apercibimiento de aplicarse lo dispuesto en los artículos 59° y 60° del Código Penal en caso de incumplimiento.

7.5. **El control sobre los alcances y consecuencias del acuerdo provisional.-** conforme lo regulado en el numeral 4 del artículo 468° del Código Procesal Penal, le corresponde al Juez de Investigación Preparatoria "(...) explicar al

procesado los alcances y consecuencias del acuerdo, así como las limitaciones que representa la posibilidad de controvertir su responsabilidad. (...)"; en cumplimiento de la norma adjetiva acotada, el Juzgador en la audiencia de su propósito cumplió con explicar al imputado Diego Cava Valentín las consecuencias y alcances del acuerdo provisional de terminación anticipada celebrado entre el Fiscal de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, Tercer Despacho y su abogado defensor particular, a lo cual expreso su conformidad con la aceptación de los hechos ilícitos que se le imputan, la calificación jurídica, la sanción penal que se le impondrá, las reglas de conducta que deberá cumplir y, el monto del pago de la reparación civil que deberá cumplir con cancelar a los agraviados; a todo lo cual expreso su aceptación conforme queda registrado en audio y video.

OCTAVO: CONCLUSIÓN Y HOMOLOGACIÓN JUDICIAL.-

Finalmente, se ha cumplido con efectuar el control judicial del acuerdo provisional de terminación anticipada, tal como lo estipula la doctrina legal establecida en los fundamentos jurídicos del Acuerdo Plenario N° 5-2009/CJ-116 de fecha 13 de noviembre de 2009 (Asunto: Proceso de Terminación Anticipada: Aspectos Esenciales); verificándose la correcta calificación jurídica y tipificación del hecho ilícito atribuido al imputado Diego Cava Valentín, la suficiencia indiciaria de los elementos de convicción que sustentan el requerimiento, la legalidad de la determinación de la pena, la procedencia de los beneficios premiales de reducción de la pena y, la razonabilidad de la aplicación suspendida de la pena. Por lo tanto, corresponde homologar judicialmente el acuerdo provisional y, declarar la responsabilidad penal de Diego Cava Valentín, en los términos recogidos en el sexto considerando de la presente resolución.

II. DECISIÓN:

Por los fundamentos expuestos y las normas antes glosadas, el señor del Juez del Vigésimo Cuarto Juzgado de Investigación Preparatoria de Lima RESUELVE:

2.1. **APROBAR EL ACUERDO PROVISIONAL** de Terminación Anticipada celebrado entre el Fiscal de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, Tercer Despacho y el abogado de la defensa técnica particular de Diego Cava Valentín.

2.2. **DECLARAR** que **DIEGO CAVA VALENTÍN**, cuyos datos de identificación se consignan en la parte expositiva de la presente sentencia, es **AUTOR** del delito informático contra el patrimonio – fraude informático (hecho licito previsto y sancionado en el primer párrafo del artículo 8° de la Ley N° 300096: Ley de los Delitos Informáticos) y, delito contra la fe pública – falsedad genérica (hecho ilícito previsto y sancionado en el artículo 438° del Código Penal); en

agravio de María Laura del Río Sánchez y Diego Alberto Romani Chia; en consecuencia, le **IMPONGO CUATRO (04) AÑOS DE PENA PRIVATIVA DE LIBERTAD** con el carácter de **SUSPENDIDA** en su ejecución.

2.3. **IMPONER** al sentenciado Alfredo Arturo Vega Javier **LA PENA DE MULTA EQUIVALENTE A CINCUENTA (50) DÍAS MULTA** a razón del veinticinco por ciento de su haber mensual, la misma que deberá ser pagada en el plazo de diez días hábiles.

2.4. **ESTABLECER EL PERIODO DE PRUEBA** por un plazo de **TRES (03) AÑOS**, sujeto a las siguientes reglas de conducta: a) Comparecer mensualmente al juzgado, personal y obligatoriamente, en forma virtual, para informar y justificar sus actividades, b) Reparar los daños ocasionados por el delito y cumplir con su pago fraccionado, conforme al cronograma establecido para el pago de la reparación civil, en caso de incumplimiento de una cuota, se procederá a solicitar la revocatoria de la pena, y c) No ausentarse de la localidad en la que reside sin conocimiento del Juzgado; todo ello, bajo apercibimiento de aplicarse lo establecido en el artículo 59° del Código Penal en caso de incumplimiento, es decir amonestación, prórroga y revocatoria.

2.5. **FIJAR** en la suma de MIL DOSCIENTOS y 00/100 (S/. 1,200), el monto que por concepto de REPARACIÓN CIVIL deberá pagar el sentenciado a favor de los agraviados; a razón de un mil y 00/100 (S/. 1,000) soles a favor María Laura del Río Sánchez y, doscientos y 00/100 (S/. 200) a favor de Diego Alberto Romani Chia.

2.6. **CONSENTIDA** y/o **EJECUTORIADA** que sea la presente resolución: **INSCRÍBASE** en el Registro Nacional de Condenas y **ARCHÍVESE** los actuados en la forma y modo de Ley.

2.7. **NOTIFIQUESE** a las partes procesales.

2517 - 2022 Ita Mercedes

CORTE SUPERIOR DE JUSTICIA LIMA - Sistema de Notificaciones Electronicas SINOE
SEDE IQUITOS
Asistente Judicial (notificaciones):NONALAYA CHACA Gustavo Adolfo FAU 20546303951 soft
Fecha: 04/05/2023 10:39:02,Razón: NOTIFICACIÓN JUDICIAL,D.Judicial: LIMA / ANTICORRUPCION,FIRMA DIGITAL

PODER JUDICIAL DEL PERU
CORTE SUPERIOR DE JUSTICIA
LIMA
Sede Iquitos

CEDULA ELECTRONICA

04/05/2023 10:32:03
Pag 1 de 1
Número de Digitalización
0000069138-2023-ANX-JR-PE

42023076623202205384182613700235 5

NOTIFICACION N°76623-2023-JR-PE

EXPEDIENTE	**05384-2022-2-1826-JR-PE-22**	JUZGADO	22° JUZGADO DE INVESTIGACIÓN PREPARATORIA
JUEZ	DIAZ LEIVA JORGE EDUARDO	ESPECIALISTA LEGAL	LEON GARCIA EDWIN MAURO

IMPUTADO : MONJA SERRATO, CENDY LIZETH
AGRAVIADO : BANCO DE CREDITO DEL PERU ,

DESTINATARIO MINISTERIO PUBLICO-GERENCIA GENERAL

DIRECCION : **Dirección Electrónica - N°127420**

Se adjunta Resolución TRES de fecha 04/05/2023 a Fjs : 12
ANEXANDO LO SIGUIENTE:
NOTIF RESOL N°3 SENTENCIA TA

4 DE MAYO DE 2023

PODER JUDICIAL
DEL PERÚ

CORTE SUPERIOR DE JUSTICIA DE LIMA
VIGÉSIMO SEGUNDO JUZGADO DE INVESTIGACIÓN PREPARATORIA

Av. Iquitos N°198, con Jr. Antonio Raimondi N°297 - La Victoria (SEDE IQUITOS)
Teléfono N° 014101010, Anexo 12363 (Área de Esp. de Causas), Anexo 12396 (Área de Esp. de Audiencia) Anexo 32561 (Despacho)

EXPEDIENTE	**: 05384-2022-2-1826-JR-PE-22**
JUEZ	**: DIAZ LEIVA JORGE EDUARDO**
ESPECIALISTA	**: LEÓN GARCÍA EDWIN MAURO**
IMPUTADO	**: CENDY LIZETH MONJA SERRATO,**
DELITO	**: FRAUDE INFORMÁTICO AGRAVADO**
AGRAVIADO	**: BANCO DE CRÉDITO DEL PERÚ**

SENTENCIA POR TERMINACIÓN ANTICIPADA

RESOLUCIÓN NRO. TRES
Lima, cinco de abril del
Dos mil veintitrés. –

AUTOS, VISTOS Y OIDOS: El Ministerio Público, en audiencia de terminación anticipada indica haber llegado con la investigada **CENDY LIZETH MONJA SERRATO**, a un Acuerdo Provisional, sobre la pena y la reparación civil y llevada la audiencia con todos los sujetos procesales; y, **ATENDIENDO:**

I. PARTE EXPOSITIVA:

1.1. SUJETOS PROCESALES

1.1.1. Parte acusadora: Dr. Jonathan Cirilo Portillo Vela, *Fiscal Provincial del Segundo Despacho de la Fiscalía Provincial Corporativa Especializada en Delitos de Ciberdelincuencia de Lima, con domicilio procesal en Calle Doña Catalina N.° 498, piso 2, distrito de Santiago de Surco, con correo electrónico 2despachociberdelincuencialimacentro@mpfn.gob.pe, jportillodj@mpfn.gob.pe casilla electrónica SINOE 127420, número de celular 942-264-326.*

1.1.2. Parte Agraviada: BANCO DE CRÉDITO DEL PERÚ, *identificada con RUC N.° 20346662612, con domicilio en la calle Centenario N.° 156 - Urb. Las Laderas de Melgarejo, La Molina – Lima*
DEFENSA PARTICULAR DEL ACTOR CIVIL:Dr. Orlando Eduardo Cubillas Romero *abogado y representante legal del Banco de Crédito con registro CAL 30355 asi electrónica 44409 domicilio profesor jirón lampa 499 cercado de Lima, correo electrónico ocubillasr@bcp.com.pe, teléfono celular 98095966.*

1.1.3. Parte acusada: CENDY LIZETH MONJA SERRATO, *identificado con DNI: 75810652, edad 21 años, sexo femenino, fecha de nacimiento 01 de mayo de 2001, lugar de nacimiento olmos – Lambayeque -Lambayeque, grado de instrucción secundaria completa – técnico incompleto de administración bancaria, estado civil soltera, estatura 1.52 cm, nombre de sus padres Gabriel y Aquilina, laboraba en banco de crédito, Ingreso económico mensual s/. 1025, sin antecedentes penales ni judiciales, no tiene bienes escritos a su nombre, no tiene tatuajes en su cuerpo, no tiene cicatrices, teléfono celular 955080717, tiene cuentas en redes sociales Facebook y Instagram su perfil de nombre Lizzeth Monja, domicilio RENIEC -real jirón Contisuyo N° 627 - urbanización zarate, distrito de san juan de Lurigancho.*
DEFENSA PUBLICA DE LA INVESTIGADA: Dr. Tomás Gustavo de la Cruz Limaco, *con del colegio de abogados de Lima 73044, casilla electrónica 83006, correo electrónico delacruzgustavo@gmail.com teléfono móvil 979339608*

1.2. ACUERDO SOBRE LA PENA, REPARACIÓN CIVIL: El Ministerio Público procedió a oralizar el acuerdo arribado con el actor civil, la investigada y su defensa técnica, tomando en cuenta el beneficio de confesión sincera y Terminación Anticipada, solicitando que se imponga a la INVESTIGADA, ***SEIS AÑOS DE PENA PRIVATIVA DE LIBERTAD EFECTIVA, 90 DÍAS MULTA,*** *siendo su equivalente el monto de* ***S/. 712.50 (SETECIENTOS DOCE SOLES CON 50/100 CENTIMOS),*** *y una* ***REPARACION CIVIL*** *de* ***S/.104, 399.33 (CIENTO CUATRO MIL TRESCIENTOS NOVENTA Y NUEVE SOLES CON 33/100 CENTIMOS).***

1.3. POSICIÓN DE LA INVESTIGADA FRENTE A LA IMPUTACIÓN: Después de haber instruido de sus derechos a la INVESTIGADA e informado, los extremos que comprende la Terminación anticipada del proceso, se le preguntó si admite ser responsable del delito materia de investigación, de la pena y reparación civil acordado por las partes en audiencia; quien previa consulta con su abogado defensor; fecho ello la INVESTIGADA **CONTESTÓ POSITIVAMENTE**, esto es, **SE CONSIDERA CULPABLE**, esto es, ***acepto su responsabilidad de los hechos antes descritos como la pena y reparación civil íntegramente***

sin condicionamiento alguno, en forma libre y voluntaria; decisión que ha sido ratificada por su defensa técnica.

1.4. REFERENTE A LA TERMINACIÓN ANTICIPADA

La terminación anticipada es un proceso penal especial que forma parte de la simplificación procesal, que se sustenta en el principio del consenso y es, además, uno de los exponentes de la justicia penal negociada. Su regulación, en sus aspectos esenciales, está suficientemente desarrollada en el Libro V. Sección V, artículos 468° y siguientes del Código Procesal Penal (de aquí en adelante CPP). Este proceso importa la aceptación de responsabilidad por parte del imputado respecto del hecho punible objeto del proceso penal y la posibilidad de negociación acerca de las circunstancias accesorias, conforme fluye de los incisos 4 y 5 del artículo 468° del citado cuerpo normativo. Si es que las partes arriban a un acuerdo -que tiene como presupuesto la afirmación de la responsabilidad penal del imputado y, como condición, la precisión de las consecuencias jurídicos penales y civiles correspondientes, en perfecta armonía con el principio de legalidad-, corresponde al Juez en ejercicio de su potestad jurisdiccional llevar a cabo los pertinentes controles acerca de la legalidad del acuerdo y de la razonabilidad de la pena.

Conforme los estableció la Corte Suprema, en el Acuerdo Plenario N°5-2008/CJ-116, del 13 de noviembre del 2009, el control de legalidad del acuerdo se expresa en tres planos diferentes. A.- *El ámbito de la tipicidad o calificación jurídica penal, en relación a los hechos objeto de la causa y a las circunstancias que rodean al hecho punible. B.- El ámbito de la legalidad de la pena y, en su caso a su correspondencia con los parámetros, mínimo y máximo, que fluyen del tipo legal aplicado y de las circunstancias modificativas de la responsabilidad -esto es lo que se denomina pena básica-. También el juicio de legalidad alcanza al respeto de los ámbitos legalmente definidos de la reparación civil-siendo del caso resaltar que en este extremo prima por completo la disposición sobre el objeto civil- y de las consecuencias accesorias. C.- La exigencia de una suficiente actividad indiciaria. Ello implica que las actuaciones o diligencias de la investigación permitan concluir que existe base suficiente -probabilidad delictiva- (i) de la comisión de los hechos imputados y de su vinculación con el imputado, y (ii) que están presentes todos los presupuestos de la punibilidad y de la perseguibilidad.*

En este sentido, es preciso hacer un control respecto a la calificación jurídica penal de los hechos sometidos a proceso penal y las circunstancias que lo rodean, a efecto de verificar que efectivamente se encuadren o se subsumen en el tipo penal materia de incriminación. Seguidamente, debe hacer un control de razonabilidad de la pena, que está centrado en el examen del *quantum* de la pena y de la reparación civil objeto del acuerdo. Por ello, se debe hacer una valoración evitando que se vulnere, por exceso o por defecto, el principio de proporcionalidad, se lesione la finalidad de la pena o se afecte indebidamente los derechos e intereses legítimos de la víctima. De esta manera, solo será posible rechazar el acuerdo, si de modo palmario o evidente se estipule una pena o una reparación civil evidentemente desproporcionada o que en el caso de la pena se lesione ostensiblemente el principio preventivo. También deberá desaprobarse cuando, el examen de lo actuado, se advierta insuficiencia probatoria o algún caso de *in dubio pro-reo*, la inexistencia de los hechos, la atipicidad o cualquier otra situación que pueda llevar a la absolución del imputado.

Para ello, debe verificarse el respeto de los ámbitos legales referidos tanto a la configuración de la pena básica -definida como la configuración del marco penal establecido por el tipo penal y las diferentes normas que contienen las circunstancias modificativas de la responsabilidad genérica, sean agravantes y/o atenuantes- como al establecimiento de la pena concreta final, que es el resultado de la aplicación de los factores de individualización estipulados en los artículos 45°, 45°-A y 46° del Código Penal (de aquí en adelante CP), siempre dentro del marco penal fijado y a partir de criterio referidos, al grado de injusto y el grado de culpabilidad.

1.5. IMPUTACION FACTICA. -

a) ***Circunstancias Precedentes.-*** *Fluye del Acta de Intervención Policial que, personal policial de la División de Investigación de Delitos de Alta Tecnología - DIVINDAT, ¡por intermedio de una llamada telefónica del personal del Banco de Crédito del Perú - BCP, ubicado en Jr. Cuzco N.° 494 - Cercado De Lima, quién se identificó como Víctor SOLSOL DAVILA con DNI N.°42933530 el mismo que-indicó ser supervisor de la agenda BCP, mencionó que en dicha agencia habrían retenido a la promotora de servicios Cendy Lizeth MONJA SERRATO (trabajadora del BCP) Identificada con DNI N.° 75810652, por presunto Fraude Informático; Ante ello, personal de DIVINDAT se constituyó al lugar antes Indicada y se entrevistó con Víctor SOLSOL DAVILA quien indicó que la detenida el día de la fecha habría realizado siete (07) transferencias desde su sistema del BCP a su cuenta bancaria personal BCP N.° 194-97980968072.*

b) *Circunstancias Concomitantes.- Es en esas circunstancias que, la ciudadana Cendy Lizeth Monja Serrato quien se desempeñaba como Promotora De Servicios de la agencia de Emancipación del Banco de Crédito del Perú - BCP, el día 15 de agosto del año en curso, mientras se encontraba en ejercicio de sus labores dentro de la citada agencia bancaria, realizó siete (07) transferencias desde el sistema del Banco de Crédito BCP a su cuenta BCP N.° 194-97980968072, hecho que fue advertido el mismo día 15 de agosto de 2022, por el supervisor de agencia del Banco de Crédito del Perú, quien verificó que la trabajadora la Cendy Lizeth Monja Serrato, promotora de servicios de la agencia de Emancipación del BCP, había transferido a su cuenta BCP N.° 194-97980968072 la cantidad TOTAL de S/ 115,200.00 soles (CIENTO QUINCE MIL DOSCIENTOS NUEVOS SOLES), operaciones que se efectuaron de la siguiente manera:*

- *La primera operación a las 09:15 horas por la cantidad de S/ 3,500.00 soles.*
- *La segunda operación a las 10:00 horas por la cantidad de S/ 9,500.00 soles.*
- *La tercera operación a las 10:15 horas por la cantidad de S/ 500.00 soles.*
- *La cuarta operación a las 11:02 horas por la cantidad de S/ 21,700.00 soles.*
- *La quinta operación a las 13:20 horas por la cantidad de S/ 20,000.00 soles.*
- *La sexta operación a las 14:50 horas por la cantidad de S/30,000.00 soles.*
- *La última operación a las 15:37 horas por la cantidad de S/ 30,000.00 soles.*

Posteriormente, parte del dinero ilícitamente obtenido, fue transferido por la misma investigada las cuentas bancarias:

- *Número 0767372543 del Banco Scotiabank de titularidad de Juan Adries Azuaje García, de nacionalidad venezolana.*
- *Número 4457281071 del Banco Scotiabank de titularidad de Odalis del Carmen Machiquez Viera, de nacionalidad venezolana.*

c) *Circunstancias Posteriores.- Al ser intervenida la investigada Cendy Lizeth Monja Serrato indicó que las operaciones fraudulentas las realizó con la finalidad ser "invertido". Asimismo, en el transcurso de la investigación se han podido recabar diversos documentos e informes que acreditan la vinculación laboral de la investigada con la empresa agraviada, así como las transferencias efectuadas, la introducción de datos para la transferencia y la manipulación del sistema para dicho fin patrimonial en perjuicio del BCP, contando la investigada con una condición especial acreditada de acceso así como de información y preparación superior previa en mérito a la función desempeñada como promotora de servicios.*

*En consecuencia, para el Ministerio Público la imputación en contra de **CENDY LIZETH MONJA SERRATO** se encuentra debidamente corroborada con la sindicación de parte del agraviado del **BANCO DE CREDITO DEL PERU**, el mismo que satisface las exigencias del Acuerdo Plenario N.° 02-2005/CJ-116; asimismo conforme consta en la carpeta fiscal, documentos e informes recabados, así como en las actas de intervención policial y Acta de Visualización de Información de Equipo Celular, se evidencia que la imputada realizó a su favor siete (07) transferencias en ejercicio de sus funciones como Promotora de Servicios (cajera) en el Banco de Crédito del Perú - BCP, lo que permite evidenciar su accionar delictivo, corroborándose no solo la presencia física de la imputada **CENDY LIZETH MONJA SERRATO** en el lugar de los hechos en donde se encontraba laborando sino que además la recepción y disposición de efectivo fue realizada de forma personal a través de su banca por internet, siendo por ende que existen elementos de convicción suficientes para su reconocimiento pleno como la autora del hecho delictivo en grado de consumación y afectación patrimonial acreditara a la entidad bancaria; en consecuencia, y estando al resultado de la investigación se colige que existen indicios objetivos, razonables y reveladores de la comisión del delito denunciado, así como de la vinculación de estas en los hechos materia de imputación (tanto de la comisión del delito en los verbos rectores indicados como del conocimiento y una posición especial a la data e información reservada - incluyendo accesos al sistema y propio manejo del sistema del BCP en razón del ejercicio de su labor desempeñada); por lo que, habiéndose verificado que en el presente caso que concurren los presupuestos de procedencia de la acción penal.*

II. PARTE CONSIDERATIVA:

PRIMERO: Habiéndose expuesto en audiencia pública, los acuerdos arribados por la investigada, quien estuvo asesorada por su abogado defensor, el Ministerio Público, en cuanto a la responsabilidad penal, el *quantum* de la pena y reparación civil, respectivamente; corresponde, al juzgado, determinar si la pena y la reparación civil acordada, respetan el principio de razonabilidad y sobre las mismas no existe oposición alguna, luego de ser aclarado el acuerdo inicial planteado solo por el Ministerio Publico y la parte imputada.

SEGUNDO: Sobre lo particular se debe señalar lo siguiente: debe tenerse en cuenta el principio de proporcionalidad de las penas conforme a lo establecido por el artículo VIII del Título Preliminar del CP, en correspondencia entre el injusto cometido por el agente y la pena que le corresponde. Así como, el principio de humanidad de las penas, conforme lo previsto por el artículo IX del mismo título preliminar, este juzgador también lo considera correcto, adecuado y aplicable al presente caso, por cuanto, a discreción de este despacho, los criterios establecidos tanto en el CP como en el articulado pertinente del CPP -que regula el Proceso Especial de Terminación Anticipada- no impide que el juzgador aplique los Principios de Humanidad, Razonabilidad y de Proporcionalidad para determinar la pena final a imponerse, procurando la correspondencia que debe existir entre el injusto cometido y la pena a imponerse, sostener

lo contrario sería encasillar a los operadores de justicia a la determinación de una pena siguiendo parámetros netamente aritméticos, lo cual evidentemente contraviene los Principios del Derecho Penal, con respecto al quantum de la pena acordada entre el Ministerio Público y la defensa técnica de la imputada a criterio de este juzgador, el acuerdo respeta el marco de legalidad, proporcionalidad y razonabilidad de la pena, así como las normas previstas en los artículos 45°, 45°-A y 46° del CP.

RESPECTO DEL TIPO PENAL IMPUTADO

TERCERO: Delito informático contra el patrimonio, en la modalidad **FRAUDE INFORMÁTICO AGRAVADO,** en agravio del Banco de Crédito del Perú - BCP, el mismo que se encuentra tipificado en el primer párrafo del artículo 8 de la Ley N.° 30096 (y su modificada por Ley N.° 30171) establece *"El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito n 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."*; Este tipo penal (fraude informático) sanciona diversas conductas. Entre ellas a diseñar (proyecto o plan), introducir (entrar en un lugar), alterar (estropear, dañar, descomponer), borrar (desvanecer, quitar, hacer que desaparezca algo), suprimir (hacer cesar, hacer desaparecer), clonar (producir clones) datos informáticos o cualquier interferencia, o manipular (operar con las manos o con cualquier instrumento) el funcionamiento de un sistema informático procurando (conseguir o adquirir algo) un beneficio para sí o para otro en perjuicio de tercero; y por la forma como esta estructura se clasifica como un delito de resultado, porque no basta cumplir con el tipo penal para que se consuma el delito de fraude informático, sino que además, es necesario que esa acción vaya seguida de un resultado separado de la misma conducta el que consiste en causar un perjuicio a tercero, de otro modo el delito quedaría en tentativa. Por ejemplo, clonar tarjetas bancarias, el fraude informático que afecta los programas sociales destinados a apoyo social. Este artículo es compatible con el artículo 8 del Convenio de Budapest, porque ambos artículos sancionan el empleo indebido de datos informáticos y la manipulación del funcionamiento del sistema mismo[1].

CUARTO: Respecto al agravante estipulada en el artículo 11° numeral 2 que señala: *El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente ley cuando: (...) 2. el agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función (...)"* Del presente artículo se ha descrito que generalmente son terceros o personas externas a la organización quienes realizan actividades ilícitas; sin embargo, ello no impide que éstas sean cometidas por miembros de alguna organización, ya que tienen mayor posibilidad de acceder a la información de los usuarios utilizando mecanismos ilegales y/o violando protocolos de seguridad de la información propios de la empresa. Asimismo, respecto a la responsabilidad de la persona jurídica frente a la omisión de un debido cuidado frente al accionar ilícito de uno de sus trabajadores internos, además de englobar dicho riesgo como una medida de cumplimiento normativo que la empresa debe evaluar en el ejercicio de las funciones o cargos de sus trabajadores. Por otro lado, es pertinente resaltar que la Ley N.° 29733, Ley de Protección de Datos Personales, y el Decreto Supremo N.° 003-2020-JUS, Reglamento de la Ley de Protección de Datos Personales disponen que el responsable del tratamiento de los datos personales debe cumplir con implementar las medidas de seguridad técnicas, organizativas y legales pertinentes a fin de garantizar un tratamiento de datos adecuado. Ello implica, entre otros aspectos, establecer una gestión de accesos y privilegios del sistema para la verificación periódica de estos. En consecuencia, este despacho considera que dicha conducta requerida tiene que ver con el accionar de la persona en la posición especial de dominio de su cargo para cometer el delito. Es decir, que como trabajadora o trabajador tenga accesos a estos privilegios para facilitar la comisión del acto delictivo informático.

RESPECTO DE LOS ELEMENTOS DE CONVICCIÓN

QUINTO: El Ministerio Público, entre los elementos de convicción que acredita la imputación, ofrece los siguientes:

[1] *https://revistas.pucp.edu.pe/index.php/iusetveritas/article/download/13630/14253/. que cita al Diccionario de la Real Academia Española.*

5.1. **ACTA DE INTERVENCIÓN POLICIAL**, de fecha 15 de agosto de 2022, documento en el cual se narra en forma detallada, el modo y circunstancias en las que fue intervenida Cendy Lizeth Monja Serrato, quien minutos antes se había efectuado diversas transacciones (7 operaciones) bancarias a su cuenta del Banco de Crédito del Perú - BCP N.° 194-97980968072, por la suma de S/115 200.00 soles, desde su caja, monto que fue sustraído en siete (07) operaciones bancarias.

5.2. **ACTA DE DETENCIÓN**, de fecha 15 de agosto de 2021, de la persona de Cendy Lizeth Monja Serrato, donde se detalla el motivo de la detención.

5.3. **ACTA DE LECTURA DE DERECHOS**, de fecha 15 de agosto de 2021, de la persona de Cendy Lizeth Monja Serrato.

5.4. **ACTA DE REGISTRO PERSONAL E INCAUTACIÓN**, de fecha 15 de agosto de 2022, que detalla que en poder de la investigada CENDY LIZETH MONJA SERRATO, se halló un teléfono celular marca APPLE modelo IPhone 8 color rojo, con IMEI lógico 352996096745622.

5.5. **ACTA DE LACRADO**, de fecha 15 de agosto de 2022, efectuado al teléfono celular marca APPLE modelo IPhone 8 color roja, con IMEI lógico 352996096745622, de propiedad de la investigada

5.6. **ESCRITO DE PARTE AGRAVIADA**, de fecha 15 de agosto de 2022, suscrito por el supervisor del Banco de Crédito del Perú, Víctor Solsol Dávila, donde presentó la siguiente documentación respecto a la detenida Cendy Lizeth Monja Serrato: a)Movimientos de la cuenta de ahorros. b)Números de cuenta, c)interbancaria a donde transfirió dinero sustraído, d)07 váuchers de depósito realizados a su cuenta del Banco de Crédito del Perú - BCP N.° 194- 97980968072, por un monto total de S/ 115 200.00 soles, realizados en su espacio de trabajo (ventanilla asignada); y e)Una anotación de códigos interbancarios: 00925220076737254381 perteneciente a Azuaje García.

5.7. **ESCRITO DE PARTE INVESTIGADA**, de fecha 15 de agosto de 2022, documento por el cual la investigada de Cendy Lizet Monja Serrato, acepta haber transferido a cuenta de un tercero en cuenta bancaria el monto total de S/115 200.00 soles.

5.8. **ACTA DE VERIFICACION DOMICILIARIA DE ODALIS DEL CARMEN MACHIQUEZ VIERA**, de fecha 15 de agosto de 2022, llevada a cabo en el domicilio sito en Pasaje Faustino Sánchez Carrión, Mz. G, Lote 09, Asentamiento Humano Lampa de Oro, distrito de San Juan de Lurigancho, donde personal policial tomó conocimiento que la investigada Cendy Lizeth Maja Serrato, hace 05 meses había sido inquilina de la casa de su abuela María Isabel López Rojas, empero que a la fecha ya no vive en dicha dirección.

5.9. **ACTA DE AUTORIZACION DE CENDY LIZETH SERRATO**, de fecha 15 de agosto de 2022, documento por el cual autoriza de forma voluntaria que el personal de la policía visualice y extraiga información que contenga en el celular incautado.

5.10. **MANIFESTACION DE VICTOR SOLSOL DAVILA**, de fecha 16 de agosto de 2022, llevada a cabo en una de las Oficinas del Departamento de Adulteración de Telefónica Celular, quien en su calidad de supervisor de la agencia de Emancipación del Banco de Crédito del Perú: "...Que, el día de ayer 15AG02022, ingresamos a la agencia aproximadamente a las 08:30, todos nos comenzamos a distribuir en nuestro sitios respectivamente alistamos para la apertura de las 09:00 de la mañana, luego de apertura la agencia normalmente, aproximadamente a las 09:30 y 10:00 de la mañana se acercó Cendy Lizet MONJA para comunicarme que se sentía mal, igualmente le comunico a la promotora principal Nicole AYALA, que se sentía mal por eso iba baño, durante el día, se levantaba y se dirigía al baño luego se disculpaba por que se sentía mal, en el transcurso del día desde las 10:00 hasta las 13:00 horas, tuve una visita de seguridad para que pueda visualizar el estado de las instalaciones, luego también teníamos la visita de seguridad de Hermes quien nos dejó la remesa de efectivo, que es algo habitual en esta agencia, entre este ínterin observe que Candy Manja iba al baño muy continua, al ver que con tanta continuidad acudía al baño conversé, con Nicolle a fin de que acude a una clínica para chequear su salud, aproximadamente a las 17:00 voy a mi sitio para disponer que promotores iban a entregar efectivo excedente de sus cajas y es cuando Cendy MONJA se me acerca y solicita hablar en privado con mi persona, motivo por el cual nos trasladamos a la zona de ante bóveda, es allí donde le pregunto qué pasaba , ella me responde que había hecho unos depósitos y unas transferencias y que no le devuelven el efectivo, a lo que yo le pregunte con sorpresa, no le entendía por qué ella se puso nerviosa y agitarse, en ese momento salgo de la ante bóveda para llamar a Nicole AYALA y los dos ingresamos a la sala de ante bóveda, luego le pedí a Cendy que se explicara mejor, a lo que ella indica en una primera instancia que ella había hecho unas transferencias a unos familiares porque junto con su familia iban a comprar un inmueble, entonces yo le pregunte por qué había hecho eso y porque tu familia no te devuelve, igualmente Nicolle le comenta porque había hecho esos tipo de operaciones y en todo caso que su familia le devuelva, al escucharla alguna contradicciones donde indica que su familia no sabe nada, es allí cuando le increpo que como puedes comprar un inmueble sin que tu familia lo sepa, es allí donde le digo Cendy que es lo que está pasando y ella nos comienza explicarnos que había hecho operaciones por un aplicativo de Amazon, al ver esto con Nicolle salimos a su Box DE Cendy para ver si podamos eliminar algunas operaciones que ella había realizado, es cuando ella indica nuevamente que todo había sido por banco móvil, al ver que dichas operaciones no podíamos eliminar, nuevamente ingresamos a la ante bóveda, donde se queda Nicolle y Cendy, yo salgo a llamar a mis inmediatos superiores el Sr. Rosalía OLIVOS y Fidel Sagastegui con quien me logro comunicarte a grosso modo de lo que estaba ocurriendo también llamamos a la central de la policía para que acude a nuestro instalaciones. Después de aproximadamente de 10 minuto llego a nuestra agencia Rosalía OLIVOS Y Carlos MENDOZA nuestro Gerente Regional y dentro de la zona ante bóveda le pedimos a Cendy más calmada que nos explique qué es lo que había hecho, ella explica que el día domingo le había llegado unos mensajes a su celular al principio no le tomo importancia, pero luego ingreso al link del mensaje que la conducían a un aplicativo de Amazon y un numero de WhatsApp, nos indicó que había hecho dos operaciones de montos menores de las cuales ella entrega el importe de 100 soles e inmediatamente le devolvían 120. eso fue la modalidad del supuesto .aplicativo que tenía, dijo el día domingo había realizado esas dos operaciones, el día lunes quiso hacer dicha operación pero les solicitaban aproximadamente S/ 30000.00 soles, luego la preguntamos por qué ella había realizado dichas operaciones por esa cantidad la misma que no supo responder, luego ella indico ella esperaba que le devolvieran el efectivo, asimismo cuando le preguntamos porque seguía haciendo esto, ella no respondió solamente indico que había sido estafada, luego salimos de la zona de ante bóveda, el mismo que me dirigí cuadrar su caja de Cendy...'.

5.11. **MANIFESTACION DE JUAN JOSE CARRASCO PALOMINO**, de fecha 16 de agosto de 2022, llevada a cabo en una de las Oficinas del Departamento de Adulteración de Telefónica Celular - DIVINDAT, quien en su calidad de sub gerente de seguridad Cooperativa del Banco de Crédito del Perú: "...Que, el día de ayer 15AGO2022, aproximadamente 18:00 horas, la Unidad de CENTRASCAN de la seguridad Corporativa del BCP, nos reportó un faltante de caja señalado por la promotora de servicio Cendy MONJA SERRATO, luego nos comunicamos con la oficina Emancipación donde ocurrieron los hechos reportados, no indicaron que la indicada colaboradora al supervisor de agencia Víctor SOLSOL le había comunicado que había lamado dinero de su caja para depositárselo a su cuenta de ahorro y allá desde su teléfono realizo varias transferencias a dos cuentas del Banco Scotiabank, seguidamente se realizó el arqueo de caja y estableció que en el terminal financiero de la colaboradora se había transferido a su cuenta S/.115,200.00 soles, a través de siete depósitos, ante estos hechos la colaboradora autorizo al supervisar retirar de su cuenta de ahorro el importe de S/. 21,255.15 soles, luego el supervisor al hacer el cuadre final de la caja de la colaboradora se evidencio un faltante de caja de S/. 93,945.12 soles, que finalmente fue contabilizado como perdida de caja..."

5.12. **MANIFESTACION POLICIAL DE S3 PNP JESUS JHONATAN ZUÑIGA HUAMAN**, de fecha 16 de agosto de 2022, llevada a cabo en una de las Oficinas del Departamento de Adulteración de Telefónica Celular - DIVINDAT, refirió que; "...Que, ya que prácticamente recibimos una llamada telefónica de la agencia del Banco de Crédito, ubicado en el Jr. Cuzco 494, donde que nos dijeron que tenían una persona retenida, respondiendo al nombre de Cendy Lizeth Monja Serrato, el delito era fraude, nos constituimos al lugar para constatar la información, de los cuales era correcta encontramos a la señorita antes mencionada, y procedimos a hacer la intervención y entrevistaron con la señorita, nos explicó las circunstancias de los hechos, procedimos a constituirla a la avenida España 323, y todos los detalles que señala el acta de intervención...".

5.13. **MANIFESTACION POLICIAL DE S2 PNP CUYATE FLORES MERLLY KARIN**, de fecha 16 de agosto de 2022, llevada a cabo en una de las Oficinas del Departamento de Adulteración de Telefónica Celular DIVINDAT, refirió que; "...Que, a mérito de la Manada telefónica de personal de la agencia BCP, quién se identificó como Víctor SOLSOL DAVILA, el mismo que refirió ser supervisor del personal de la agencia BCP ubicada en el Jr. Cuzco-494 - Cercado de lima, quien refirió que en dicha agencia habrían retenido a la promotora de servicios Cendy Lizeth MONJA SERRATO (21). por presunto fraude; ante la noticia criminal, personal de la DIVINDAT al mando del Cmte. PNP José Augusto MONTERO PECHE, nos constituimos a la referida entidad financiera donde se entrevistó a Víctor SOLSOL DAVILA el mismo que indicó que la antes aludida le confesó que el día de hoy 15AG02022 se transfiere su cuenta BCP la cantidad de S/.115,200.00 soles desde su caja, asimismo cabe significar que Cendy Lizeth MONJA SERRATO (21) de manera espontánea y circunstancial acepto haberse transferido la cantidad de S/ 115200.00 soles a su cuenta, monto que según argumenta fue sustraído con la finalidad de ser invertido; motivo por el cual luego de hacerle conocer sus derechos que le asiste en calidad de detenida, fue conducida a las instalaciones de la DIVINDAT-DIRINCRI PNP...".

5.14. MANIFESTACION POLICIAL DE SS PNP ESPINOZA PRADO VICTOR, de fecha 16 de agosto de 2022, llevada a cabo en una de las Oficinas del Departamento de Adulteración de Telefónica Celular - DIVINDAT, refirió que; *"...Que, luego de recibir la llamada telefónica de los empleados de la Agencia BCP Emancipación ubicada en la jr. Cuzco 494-Cercado de Lima, quién se identificó como Victor SOLSOL DAVILA, supervisor de la indicada Agenda antes mencionada quien indico que en dicha agencia habían retenido a la promotora de servicios Cendy Lizeth MONA SERRATO (21), por haber incurrido en un presunto fraude; motivo por el cual, personal de la DIVINDAT al mando del Cmte. PNP José Augusto MONTERO PECHE, nos constituimos a la referida entidad financiera, al llegar nos entrevistamos con Victor SOLSOL DAVILA, quien indicó que la Promotora de Servicio había trasferido dinero del banco a su cuenta BCP la cantidad de S/.115,200.00 soles, que luego de entrevistarle a la retenida Cendy Lizeth MONJA SERRATO (21) de manera espontánea y circunstancial acepto haberse transferido la cantidad de S/.115,200.00 soles a su cuenta, monto que según argumenta fue sustraído con la finalidad de ser invertido; motivo por el cual luego de hacerle conocer sus derechos que le asiste en calidad de detenida, fue conducida a las instalaciones de la DIVINDAT-DIRINCRI PNP".*

5.15. INFORME T-114292, de fecha 16 de agosto de 2022, emitido por el Banco de Crédito del Perú, de cuyo anexo se tiene el detalle de las transferencias efectuadas a favor de Juan Adries Azuaje García y Odalis del Carmen Machiquez Viera (Se detalla imagen en requerimiento de terminación anticipada)

5.16. CERTIFICADO MÉDICO LEGAL N.° 042830, de fecha 16 de agosto de 2022, donde se detalla que la persona de Cendy Lizeth Monja Serrato, no presenta lesiones traumáticas corporales recientes.

5.17. CONSULTA ANTE LA PÁGINA DE LA SUPERINTENDENCIA NACIONAL DE MIGRACIONES, respecto a los ciudadanos venezolanos Juan Adries Azuaje García y Odalis del Carmen Machiquez Viera.

5.18. ACTA DE BUSQUEDA EN FUENTE ABIERTA, de fecha 17 de agosto de 2022, en la cual se realizó la búsqueda en la página Web; https://www.familyserch.org/es/, de la persona de Juan Andrés Azuaje García y Odalis del Carmen Machiquez Viera, donde se detalla que estos son de nacionalidad venezolana.

5.19. ACTA DE BUSQUEDA EN FUENTE ABIERTA DE CUENTA BANCARIA Y/O FINANCIERA, de fecha 17 de agosto de 2022, en la cual se realizó la búsqueda en el aplicativo del Banco Scotiabank, sobre cuentas que tuviesen, las personas de Juan Andrés Azuaje García y Odalis del Carmen Machiquez Viera.

5.20. ACTA DE BUSQUEDA EN FUENTE ABIERTA, de fecha 18 de agosto de 2022, en la cual se realizó la búsqueda en la página Web; https://freecarrierlookuo.com/, del número del celular 943963264, dando como resultado que la empresa operadora es MOVISTAR (Telefónica Móviles S.A.).

5.21. CERTIFICADO DE ANTECEDENTES PENALES, de fecha 25 de marzo de 2022, donde se advierte que la imputada CENDY LIZETH MONJA SERRATO, no cuenta con antecedentes penales vigentes.

5.22. CARTA DEL BANCO DE CRETIDO DEL PERÚ - BCP, de fecha 16 de agosto de 2022, por media de la cual el Banco de Crédito del Perú - BCP, da cuenta de las cuentas existentes y las operaciones pasivas (cuentas bancarias), a nombre de la imputada Cendy Lizeth Monja Serrato.

5.23. ACTA DE APERTURA DE LACRADO Y VISUALIZACION DE INFORMACION CONTENIDA EN TELEFONO CELULAR, de fecha 17 de agosto de 2022, llevada a cabo en una de las oficinas de la División de Alta Tecnología - DIRINCRI PNP, diligencia que se realiza en el equipo celular mar Apple, modelo IPhone 8, color rojo, sin serie a la vista, con IMEI N.° 352996096745622, para lo cual la ahora imputada Cendy Lizeth Monja Cerrato, brindó la clave de acceso a su equipo celular y autorizó la extracción de su contenido.

5.24. CONTINUACION DE ACTA DE APERTURA DE LACRADO Y VISUALIZACION DE INFORMACION CONTENIDA EN TELEFONO CELULAR de la detenida, de fecha 18 de agosto de 2022 conversaciones que tuvo la investigada Cendy Lizeth Monja Serrato, a través de la red social WhatsApp con el número +44 7414685251.

En segundo lugar, se obtiene capturas de pantalla del mensaje texto enviado del número 76555, el mismo que contiene link wq.me/447414685251, el mismo que redirecciona a la red social WhatsApp con el número +44 7414685251.

En tercer lugar, se obtiene capturas de pantalla de las constancias de transacciones recibidas en la cuenta de correo electrónico cencymonjaoi@gmail.com.

En cuarto lugar, se obtiene capturas de pantalla en relación al link https://sw.97wsc.com enviado por el usuario de WhatsApp +44 7414685251, el mismo que según la plataforma whois, fue creado el 06 de mayo de 2016, y actualizado el 29 de mayo de 2022, cuyo servidor web se encuentra en Hon Kong

Por último, se evidencia que las comunicaciones se realizaron a través de la red social WhatsApp con el numero +51 955080715 y al usuario +44 7414685251 registrado como "Collen", señalando además que el código "+44" pertenece a Reino Unido.

5.25. INFORME INTERNO, de fecha 17 de agosto de 2022, remitido por el Banco de Crédito del Perú - BCP, mediante el cual informa que la promotora de Servicios, Cendy Lizeth Monja Cerrato, utilizó indebidamente sus accesos para tramitar depósitos de efectivo en su terminal financiero, sin contar con el dinero físico, a su Cuenta de Ahorros N.° 194-97980968-0-72 por un total de S/115 200.00. Asimismo, se precisa que la investigada Cendy Lizeth Monja Cerrato se desempañaba como promotora de servicios en la agencia Emancipación desde el 1 de enero de 2022.

5.26. ACTA DE COMPROBACION DOMICILIARIA, de fecha 17 de agosto de 2022, llevada a cabo en el domicilio de la ciudadana Cendy Lizeth Monja Serrato, sito en: Calle Contisuyo N.° 627, urbanización Zarate, distrito de San Juan de Lurigancho; donde personal policial se logró entrevistar con la persona de nombre María Norciza Monja Meza, la misma que refirió que la persona antes mencionada, que vive en el cuarto piso del citado predio.

5.27. OFICIO N.° 007638-2022-MIRACIONES-UGD. de fecha 18 de agosto de 2022, mediante el cual la Superintendencia Nacional de Migraciones, pone en conocimiento el movimiento migratorio e información de los ciudadanos Juan Andrés Azuaje García y Odalis Del Carmen Machiquez Viera, advirtiéndose que estos no registran salida de territorio peruano.

5.28. ACTA DE VERIFICACION DOMICILIARIA DE JUAN ADRIES AZUAJE GARCIA, de fecha 18 de agosto de 2022, llevada a cabo en el domicilio sito Mz D Lot 7- N.° 07 - Piso 4 - Mz D - Lot 7 - Km 10 - AAHH La Floresta - Lima - Lima - San Juan de Miraflores, donde personal policial se logró entrevistar con la persona de nombre Samuel Águila Sánchez identificado con 47544090, el mismo que refirió no conocer a la persona de Juan Adries Azuaje García.

5.29. ACTA DE APERTURA DE LACRADO, VISUALIZACIÓN Y EXTRACCION DE IMÁGENES DE LOS VIDEOS DE CAMARAS DE SEGURIDAD DEL BCP, de fecha 18 de agosto 2020, llevada a cabo en una de las Oficinas del Departamento de Adulteración de Telefónica Celular - DIVINDAT, donde acto seguido se procedió a visualizar el contenido del primer DVD+RW-4X/2H - 4.7GB/2H, IMATION, con rotulado "1", remitido por el Banco de Crédito del Perú, accediendo al mismo donde se observa 5 archivos de video en formato MP4 de fecha 16AGO2022.

5.30. MANIFESTACIÓN DE LA INVESTIGADA CENDY LIZETH MONJA SERRATO, de fecha 19 de agosto 2022, llevada a cabo en una de las Oficinas del Departamento, la misma que en merito al artículo 87° del Código Procesal Penal guardó silencio.

*5.31. **CARTA DEL BANCO DE CREDITO DEL PERÚ – BCP**, de fecha 19 de agosto de 2022 por medio de la cual el Banco de Crédito del Perú – BCP, brinda información de las cuentas existentes a nombre y las operaciones pasivas (cuentas bancarias), balance de caja, roles y responsabilidad del puesto de Promotor de Servicios y contrato de trabajo celebrado entre la Entidad y la investigada, diario electrónico del 15 de agosto de 2022, déficit faltante de caja relacionado a Cendy Lizeth Moja Serrato y las generales de la ley de las personas de la Agencia BCP Emancipación.*

SEXTO: RESPECTO DE LA SUBSUNCIÓN EN EL TIPO PENAL

6.1. ***RESPECTO A LA TIPICIDAD.*** - A los elementos de convicción glosados, cumplen de manera satisfactoria la exigencia de suficiencia requerida, ya que se advierte que de manera deliberada una agente a manipulado el funcionamiento de un sistema informático que se le fue asignado realizando así trasferencias bancarias en beneficio propio y en terceros por la posición de cargo que tenía dentro del banco al ser cajera por lo cual se cumpliría la materialidad del delito y la agravante; por lo que este despacho concluye que la materialidad del presente delito se cumple satisfactoriamente.

6.2. ***SOBRE EL JUICIO DE ANTIJURICIDAD***, corresponde determinar si la acción típica es contraria al ordenamiento jurídico o si por el contrario se ha presentado alguna causal de justificación, cuyos supuestos se encuentran enumerados en el artículo 20° del CP; por lo que, habiéndose realizado una valoración objetivo y general del acto imputado, se advierte que es un acto contrario al orden jurídico, no apareciendo ninguna de las causales previstas en la norma precitada en la investigada.

6.3. ***EN RELACIÓN AL JUICIO DE CULPABILIDAD***, por la forma y circunstancia en que se han desarrollado los hechos y al no haber ninguna alegación de las partes, se determina que el investigada es una persona que no sufre de alguna anomalía o enfermedad que tuve su conocimiento sobre el ilícito cometido; en consecuencia se encontraba en plena capacidad de establecer que su accionar era contrario al ordenamiento jurídico, pues participo activamente en calidad de AUTORA; donde la imputada producto de una presunta estafa, realizo (07) siete transferencias desde su sistema del BCP asignado a la misma cuando ejercía funciones dentro de un horario laboral como Promotora de Servicios de la agencia de Emancipación del BCP (Cajera) a su cuenta bancaria personal y de otros dos sujetos, aprovechando tal sustracción del dinero debido al acceso del funcionamiento del sistema informático; en consecuencia, la investigada se debe hacer merecedora de la imposición de una pena, quedando establecido que ha reconocido los hechos y que existe un mínimo de base probatoria de lo actuado a nivel preliminar para dar por acreditados los hechos materia de acusación; por lo que, tiene responsabilidad penal por del delito imputado.

RESPECTO A LA UBICACIÓN DE LA PENA EN EL SISTEMA DE TERCIOS

SETIMO: La intervención del poder penal no puede generar más daño -entiéndase pena- que el hecho concreto al cual responde. La ilicitud puede reflejarse bajo la relación del hecho concreto (delito) y la respuesta punitiva estatal (pena), y esta relación solo se admite como admisible si es proporcionada. Se entenderá proporcionada cuando la reacción penal (tomadas todas las circunstancias y el principio de mínima intervención), logra un balance positivo frente al daño causado por el delito, siempre dentro de un máximo admisible de violencia por la conjunción de otros principios. Dentro de ese marco estrecho, proporcionalidad no significa equivalencia entre la gravedad del delito y la pena, sino que el mal que causa la pena es el mínimo posible según el grado de necesidad que surge de la falta de otros instrumentos de respuesta que no sea la violencia[2]. En ese contexto, corresponde analizar la legalidad del acuerdo respecto a la pena propuesta para establecer la pena justa y equitativa, se considera el efecto retributivo, preventivo y resocializador de la misma, debiendo respetar siempre la proporcionalidad en la reacción penal, racionalidad y sobre todo su equidad; criterios que nos deben llevar a una individualización judicial de la pena que a su vez haga legitima la reacción del Estado en términos de condena y reproche legal al sujeto que lesiona un bien jurídico que se tutela penalmente, con vistas a restituir la valía de la norma penal vulnerada; aunado a ello, este despacho considera que en un Estado Constitucional de Derecho, que propugna que el fin supremo de la sociedad y del Estado es la persona, la

determinación judicial de la pena no se agota con un análisis legal tasado de la pena, puesto que no es posible dejar de lado los principios básicos para su imposición como son los principios de lesividad, culpabilidad y proporcionalidad, establecidos en los numerales II, IV, V, VII y VIII del Título Preliminar del CP, ya que la aplicación de dichos principios al caso en concreto nos van a permitir imponer una pena proporcional.

OCTAVO: El artículo 45-A° del CP establece los criterios para la determinación de la pena concreta dentro de los límites fijados por la ley, determinando los Jueces la pena aplicable en dos etapas: en *primer lugar* identificando el espacio punitivo y dividirlo en tres tercios, y en *segundo lugar* identificando la pena concreta, atendiendo a la concurrencia o no, de circunstancias agravantes y atenuantes a las que hace referencia el artículo 46° del CP; así, si concurren sólo circunstancias atenuantes corresponde fijar la pena en el *primer tercio*, si concurren circunstancias agravantes y atenuantes al pena se fija en el *tercio intermedio* y si concurren sólo circunstancias agravantes se fija la pena en el *tercio superior*; por ello, atendiendo al delito imputado señala un extremo mínimo y máximo de la pena, se operativiza el siguiente esquema respecto de tomando en cuenta la agravante estipulada:

PENA PRIVATIVA DE LIBERTAD (8 a 10 años y 8 meses)		
Tercio inferior	Tercio intermedio	Tercio superior
8 años – 8 años con 10 meses y 20 días	8 años y 10 meses y 20 días – 9 años con 9 meses y 10 días	9 años con 9 meses y 10 días – 10 años y 8 meses

En tal sentido, considerando que la representante del Ministerio Público inicialmente solicito **OCHO AÑOS DE PENA PRIVATIVA DE LA LIBERTAD EFECTIVA** para la investigada, A dicha pena concreta, , el mismo que se encuentra acorde con lo prescrito en el literal a), numeral 2) del artículo 45° – A, que expresamente establece: *"Cuando no existan atenuantes ni agravantes, o concurran únicamente circunstancias atenuantes, la pena concreta se determina dentro del tercio inferior"*; teniendo en cuenta la carencia de antecedentes penales del investigada y que el Ministerio Público sustenta que no encuadra en la reincidencia ni en la habitualidad.

RESPECTO A LA PENA DE DÍAS MULTA

NOVENO: El primer párrafo del artículo 8 de la Ley N.° 30096 (y su modificada por Ley N.° 30171) determina la imposición de 60 a 120 días multas, pero con la agravante en el artículo 11 inciso 2, de la mencionada ley, determina la imposición de 120 a 160 días multas, es decir existe una unidad de pena; por ello, el Ministerio Público está aplicando el mismo análisis que para la pena privativa de libertad corresponde aplicar el tercio inferior para la acusada, que sería 120 días multa y tomando en cuenta la remuneración mínimo vital vigente al momento de los hechos de S/. 950.00 (novecientos cincuenta 00/100 soles), según D.S. N.° 004-2018-TR que entró en vigencia el 01.04.2018, el mismo que dividido entre 30 días obtenemos S/. 31.67 (treinta y un 67/100 soles), aplicando un 25%, tenemos un resultado de S/. 7.92 (Siete con 92/100 soles) de ingreso diario, **MULTIPLICADO POR 120 DÍAS**, obtenemos la suma de **S/. 950.00 (NOVECIENTOS CINCUENTA SOLES CON 00/100 CENTIMOS)**; por tanto, monto que conforme al artículo 44° del CP deberá ser pagada dentro de los diez días de pronunciada la sentencia.

PENA DE MULTA (120 a 160 días)		
Tercio inferior	Tercio intermedio	Tercio superior
120 a 133 días	133 a 147 días	147 a 160 días

RESPECTO A LA REDUCCIÓN POR CONFESIÓN SINCERA

DECIMO: En el fundamento jurídico vigésimo primero del Acuerdo Plenario N°5-2008/CJ-116 se precisa que la sinceridad de la confesión equivale *"a una admisión (1) completa -con cierto nivel de detalle que comprenda, sin omisiones significativas, los hechos en los que participó-, (2) veraz -e l sujeto ha de ser culpable sin ocultar datos relevantes del injusto investigado-, (3) persistente -uniformidad esencial en las oportunidades que le corresponde declarar ante la autoridad competente- y (4) oportuna -en el momento necesario para garantizar y contribuir a la eficacia de la investigación-, a la que se aúna, a los efectos de la*

cuantificación de (a pena atenuada, (5) su nivel de relevancia" . Por lo que, si se trata de un delito evidente o, lo que es lo mismo, si este sido descubierto flagrantemente, cualquier aceptación del hecho y colaboración del agente con la Policía o el Ministerio Público en el ejercicio de sus funciones -así se produzca de forma concomitante o inmediatamente después de cometido- resulta irrelevante para la investigación o esclarecimiento del hecho y, consecuentemente, no determina reducción de pena en virtud de la aplicación de la fórmula de derecho premial referida a la confesión sincera. (SALA PENAL PERMANENTE R. N. N° 370-2017); en ese sentido el Ministerio Público realizó un análisis de la presente figura en atención a que la investigada previamente a la intervención por el personal policial confeso el delito a su jefe inmediato, brindado facilidades para el extorno del dinero depositado; aunado a ello proporciono la identificación de la personas a los cuales se realizaron los depósitos, lo cual fue corroborado con otros elementos de convicción posteriores, contribuyendo a la investigación de otro ilícito; pues en el caso esta no hubiera dado a viso a su jefe inmediato, no se hubiera podido recuperar el dinero sustraído; por lo que el razonamiento del ente persecutor resulta acorde a ley; en esa línea, se tiene que Artículo 161° del CPP señala que el juez puede disminuir prudencialmente la pena hasta en una tercera parte por debajo del mínimo legal, más aun si la investigada no es reincidente o habitual; por lo que, el Ministerio Público ha dispuesto la **REDUCCIÓN DE 08 MESES**, reducción que se encuentra dentro del marco establecido por la ley, al no ser una reducción tasada; quedando la misma en **SIETE AÑOS Y CUATRO MESES DE PENA PRIVATIVA DE LA LIBERTAD EFECTIVA.**

DECIMO PRIMERO: En el caso de la pena multa el ministerio Publico ha dispuesto la reducción **DE 10 DÍAS MULTA**, reducción que se encuentra dentro del marco establecido por la ley, al no ser una reducción tasada; quedando la misma **110 DÍAS MULTA** y tomando en cuenta la remuneración mínimo vital vigente al momento de los hechos de S/. 950.00 (novecientos cincuenta 00/100 soles), según D.S. N.° 004-2018-TR que entró en vigencia el 01.04.2018, el mismo que dividido entre 30 días obtenemos S/. 31.67 (treinta y un 67/100 soles), aplicando un 25%, tenemos un resultado de S/. 7.92 (Siete con 92/100 soles) de ingreso diario, multiplicado por 110 días, obtenemos la suma de **S/. 870.83 (OCHOCIENTOS SETENTA SOLES CON 83/100 CENTIMOS).**

RESPECTO A LA REDUCCIÓN DE PENA POR BENEFICIO PREMIAL

DECIMO SEGUNDO: La terminación anticipada es un proceso penal especial y, además, una forma de simplificación procesal, que se sustenta en el principio del consenso. Es, además, uno de los exponentes de la justicia penal negociada. Su regulación, en sus aspectos esenciales, está suficientemente desarrollada en el Libro V, Sección V, artículos 468° al 471°, del CPP (Fundamento 6 del Acuerdo Plenario N° 5-2009/CJ-116). El artículo 471° NCPP estipula una reducción adicional acumulable de la pena de una sexta parte, cabe puntualizar que la última frase del citado dispositivo legal precisa que el beneficio en cuestión es adicional y se acumulará al que reciba por confesión. Ahora bien, la aplicación del beneficio de una reducción de una sexta parte se refiere a la pena concreta o final. Sobre ésta, una vez definida, es que ha de operar la reducción en una sexta parte –es una pauta de disminución fija y automática, es decir, tasada-. El acuerdo podrá consignarla, pero en todo caso siempre diferenciándola de la pena concreta y final, del resultado final como consecuencia del beneficio aludido, a efecto de que el Juez pueda definir con seguridad y acierto la realidad del beneficio premial y su exacta dimensión. (Fundamento 14° del Acuerdo Plenario N° 5-2009/CJ-116).

DECIMO TERCERO: Como se ha precisado precedentemente al inicio de la presente audiencia, escuchada los cargos formulados por el Ministerio Público, informado sobre los alcances de la Terminación Anticipada del Debate Oral; el Acusado y su defensa estos aceptaron los cargos formulados en su contra; por tanto, en el presente caso corresponde aplicar la rebaja de pena hasta en un sexto. El Ministerio Público propuso en esa línea, la aplicación la reducción solo de **UN AÑO CON CUATRO MESES** al presente caso de la bonificación procesal de rebaja de pena correspondiente, lo que da como resultado **SEIS AÑOS DE PENA PRIVATIVA DE LIBERTAD EFECTIVA**, lo que debe ser aprobado por estar conforme con la normativa antes reseñada y lo desarrollado en la presente sentencia.

DECIMO CUARTO: En el caso de la pena multa el ministerio Publico ha dispuesto la reducción **DE 20 DÍAS MULTA**, reducción que se encuentra dentro del marco establecido por la ley, al no ser una reducción

tasada; quedando la misma **90 DÍAS MULTA** y tomando en cuenta la remuneración mínimo vital vigente al momento de los hechos de S/. 950.00 (novecientos cincuenta 00/100 soles), según D.S. N.° 004-2018-TR que entró en vigencia el 01.04.2018, el mismo que dividido entre 30 días obtenemos S/. 31.67 (treinta y un 67/100 soles), aplicando un 25%, tenemos un resultado de S/. 7.92 (Siete con 92/100 soles) de ingreso diario, multiplicado por 90 **días**, obtenemos la suma de **S/. 712.50 (SETECIENTOS DOCE SOLES CON 50/100 CENTIMOS)**, lo que debe ser aprobado por estar conforme con la normativa antes reseñada y lo desarrollado en la presente sentencia.

RESPECTO DE LA REPARACION CIVIL

DECIMO QUINTO: En lo que respecta a la reparación civil, el artículo 93° del CP, establece: i) la restitución del bien o -de no ser posible-; y. ii) La indemnización de los daños y perjuicios; iii) La ejecución de sentencias Sumando. Asimismo, cabe precisar los alcances de la Ejecutoria Vinculante N°948-2005, de 07 de junio del 2005, en cuyo considerando tercero preciso: *"[...] la naturaleza de la acción civil ex delito es distinta, pues tiene como finalidad reparar el daño o efecto que el delito ha tenido sobre la víctima y, consecuentemente, debe guardar proporción con los bienes jurídicos que se afectan"*. Es decir, debe existir una adecuada proporción entre el monto fijado como reparación civil y el bien jurídico lesionado mediante el delito sancionado; sin embargo, no debe dejarse de lado, la entidad de la afectación concreta del bien jurídico al momento de establecer el monto de la reparación. En ese sentido, la reparación civil, es una de las consecuencias jurídicas del delito, que se impone, conjuntamente con la pena, a la persona responsable de la comisión de un delito, con la finalidad de resarcir el daño ocasionado a la víctima, en razón de restituirle al *status* anterior al desarrollo del suceso delictivo, conforme lo establece el artículo 93° del CP. En ese sentido, esta judicatura entiende a la "restitución" como aquella *"forma de restauración de la situación jurídica alterado por el delito o devolución del bien, dependiendo el caso, al legítimo poseedor o propietario"*, siempre que se hayan vulnerado derechos patrimoniales. Asimismo, se entiende por indemnización de daños y perjuicios como aquella forma de reestabilización de los derechos no patrimoniales del perjudicado o incluso habiéndose realizado la sustracción del bien.

DECIMO SEXTO: Según San Martín Castro señala *que los plazos de prescripción de la acción civil y la acción penal no son iguales, lo que confirma su diversa naturaleza. Es más, los dos tienen regulaciones normativas propias -la primera, fija un plazo único de dos años, según el artículo 2001.4 del CC; mientras que la segunda, supedita la prescripción al tiempo máximo de la pena privativa de la libertad-. En todo caso, la acción civil derivada de un hecho punible no se extingue; en tanto subsista la acción penal (artículo 100 del CP). Se ha establecido la Casación Civil que el artículo 100 del CP constituye un supuesto de interrupción de la prescripción extintiva, de cuyo texto se desprende que el derecho a la indemnización por responsabilidad extracontractual no se extingue mientras se esté tramitando la acción penal correspondiente.*

Siguiendo esa línea de análisis, el Acuerdo Plenario 4-2019/CIJ-116 señala que *en virtud del principio de legalidad, el plazo previsto en el inciso 1 del artículo 2001 del CC, según el cual prescriben, salvo disposición diversa de la ley, «a los diez años, la acción personal, la acción real, la que nace de una ejecutoria y la de nulidad del acto jurídico», de ningún modo puede ser considerado un plazo de caducidad. Al ser un plazo de prescripción se produce la interrupción por los actos de la parte agraviada tendientes a conseguir el pago efectivo del monto de la reparación civil de acuerdo a los supuestos de hecho contemplados en el artículo 1996 del CC. (Fundamento 45°). De igual modo, señala que es necesario aclarar que la caducidad del pago de la reparación civil no está regulada en el proceso penal ordinario de 1940, ni en el Código Procesal Penal de 2004. Por tanto, no puede aplicarse un plazo legal establecido para la prescripción, que admite interrupciones, como uno de caducidad frente a una situación fáctica no prevista legalmente para tal fin(Fundamento 47°);* por ello del acuerdo entre la parte investigada y el actor civil -debidamente constituido- se tiene que el momento del pactar el monto de reparación civil no se ha establecido un cronograma de pago para el cumplimiento de dicho resarcimiento; por lo que debe entenderse de acuerdo a lo ya mencionado anteriormente, que debe ejecutarse el pago hasta antes del vencimiento de la pena privativa de libertad respetando el acuerdo de las partes.

DECIMO SETIMO: Para el presente caso, las partes acordaron una reparación civil por i) Restitución del bien con un monto de s/.94,994.85 soles; y. ii) La indemnización de los daños y perjuicios con un monto de s/.9,394.48; sumados los mismos arroja un monto de s/.104, 399.33 soles, que deberá pagar la sentenciada a través de depósitos judiciales al Banco de la nación a favor de la parte agraviada, monto que a criterio de este despacho que resultan razonable, de acuerdo con la naturaleza de los hechos y el daño, naturaleza del delito materia de autos; por lo que, el monto acordado por concepto de reparación civil responde a los principios de necesidad, proporcionalidad y razonabilidad.

EJECUCIÓN PROVISIONAL DE LA CONDENA

DECIMO OCTAVO: Que según el artículo 402° inciso 1 del CPP, la sentencia condenatoria en su extremo penal se cumplirá provisionalmente, aunque se interponga recurso contra ella, corresponde disponer la ejecución inmediata de la misma.

IMPOSICIÓN DE COSTAS

DECIMO NOVENO: El artículo I del Título Preliminar del CPP señala que, la justicia penal es gratuita, salvo el pago de las costas procesales, precisando el artículo 497° del CPP, toda decisión que ponga fin al proceso penal establecerá quien debe soportar las costas del proceso; además, dispone que, el órgano jurisdiccional deberá pronunciarse de oficio y motivadamente sobre el pago de las costas.

Los costos y costas procesales constituyen conceptos que forman parte de los denominados *"gastos procesales"*, montos dinerarios que se generan como consecuencia de la obligación de dar accesoria, que surge intra-proceso entre la parte vencida (deudor) y el vencedor (acreedor). Respecto a la naturaleza jurídica de dichos gastos ha existido arduo debate doctrinario, siendo sus principales teorías la sancionatoria, la resarcitoria y la del vencimiento, nuestro ordenamiento procesal adopta la última de estas teorías; empero, al haberse acogido la investigada a la terminación anticipada del proceso cabe exonerarla de las costas procesales, al haberse ahorrado al Estado la realización de una etapa intermedia y juicio oral con concurrencia de órganos de prueba y demás.

Por los fundamentos precedentes expuesto, con la facultad conferida en el artículo 138° de la Constitución Política del Perú, concordante con el artículo 1° de la Ley Orgánica del Poder Judicial y en aplicación de los artículo II, IV, V, VII, VIII, IX del Título Preliminar del CP, artículos 11°, 12°, 23°, 36°, 45°, 45°-A, 46°, 52°, 92°, 93°del CP, concordante con los numerales 399°, 468°, 469° y 471° del CPP, impartiendo justicia a nombre de la Nación, **SE RESUELVE:**

1. **APROBAR EL ACUERDO DE TERMINACIÓN ANTICIPADA,** del proceso solicitado por el representante del Ministerio Público, la imputada Cendy Lizeth Monja Serrato y su abogado defensor.

2. **CONDENAR A CENDY LIZETH MONJA SERRATO**, *identificado con DNI: 75810652, edad 21 años, sexo femenino, fecha de nacimiento 01 de mayo de 2001, lugar de nacimiento olmos – Lambayeque -Lambayeque, grado de instrucción secundaria completa – técnico incompleto de administración bancaria, estado civil soltera, estatura 1.52 cm, nombre de sus padres Gabriel y Aquilina, laboraba en banco de crédito, Ingreso económico mensual s/. 1025, sin antecedentes penales ni judiciales, no tiene bienes escritos a su nombre, no tiene tatuajes en su cuerpo, no tiene cicatrices, teléfono celular 955080717, tiene cuentas en redes sociales Facebook y Instagram su perfil de nombre Lizzeth Monja, domicilio RENIEC -real jirón Contisuyo N° 627 - urbanización zorate, distrito de san juan de Lurigancho;* en su calidad de **AUTORA**, por el delito Contra el Patrimonio en la modalidad **FRAUDE INFORMÁTICO AGRAVADO**, el mismo que se encuentra tipificado en el primer párrafo del artículo 8°, agravado con el artículo 11° numeral 2), ambos de la Ley N°30096 (modificada por Ley N°30171), en agravio de la **BANCO DE CRÉDITO DEL PERÚ**

3. **IMPONER** a la investigada **SEIS AÑOS DE PENA PRIVATIVA DE LIBERTAD EFECTIVA,** la misma que computara desde el día de su detención esto es el 15 de agosto del 2022, por tanto vencerá el día **14 de agosto del 2028,** ORDENANDOSE que la sentenciada sean internada en el Establecimiento Penitenciario correspondiente que el INPE designe, para el cumplimiento de la sentencia, al variar su situación jurídica, oficiándose para su cumplimiento.

4. **IMPONER** a la investigada el pago de **90 DÍAS MULTA,** siendo su equivalente el monto de **S/. 712.50 (SETECIENTOS DOCE SOLES CON 50/100 CENTIMOS),** los cuales deben ser abonados en la Cuenta N° 00-068-371341-MEF-DGETP-PENA DE MULTA del Banco de la Nación en el **PLAZO DE DIEZ DÍAS.**

5. **FIJAR LA REPARACION CIVIL** en la suma de **S/.104, 399.33 (CIENTO CUATRO MIL TRESCIENTOS NOVENTA Y NUEVE SOLES CON 33/100 CENTIMOS)**, el cual deberá pagar la sentenciada a través de depósito(s) judicial(es) al Banco de la nación a favor de la parte agraviada.

6. **DISPONER** la exoneración del pago de costas y costos de este proceso para el sentenciado.

7. **CONSENTIDA O EJECUTORIADA**, que sea la presente sentencia, **ORDENAMOS** se inscriba en el Centro Operativo del Registro Nacional de Condenas, **EXPIDIÉNDOSE** con dicho fin el Boletín de condena de ley. **FORMANDOSE** el cuaderno de ejecución

8. **NOTIFÍQUESE.**

LA FALTA DE MOTIVACIÓN PARA LA DETERMINACIÓN DE LA REPARACIÓN CIVIL

Sumilla. Al momento de justificar el monto reparatorio, los magistrados del Colegiado Superior no consideraron la propuesta del Ministerio Público (diez mil soles) ni lo solicitado por la Procuraduría, que contaba con legitimidad para hacerlo por ser parte civil (treinta mil soles); por tanto, la decisión en ese extremo no contiene la motivación suficiente.

Lima, veintitrés de enero de dos mil veinte

VISTO: el recurso de nulidad formulado por el señor abogado de la Procuraduría Pública del Orden Público (folios seiscientos sesenta y cinco a seiscientos setenta), con los recaudos adjuntos.

Intervino como ponente en la decisión el señor Salas Arenas, juez de la Corte Suprema.

1. DECISIÓN CUESTIONADA

La sentencia conformada del veintisiete de setiembre de dos mil dieciocho (folios seiscientos cincuenta y cuatro a seiscientos cincuenta y nueve), emitida por los señores magistrados de la Sexta Sala Especializada en lo Penal para Procesos con Reos Libres de la Corte Superior de Justicia de Lima, en el extremo que fijó cinco mil soles por concepto de reparación civil que deberá pagar el sentenciado don David Ricardo Moretti Valdivia a favor del Estado, al haber sido condenado como autor del delito de asociación ilícita para delinquir (en adelante AID)[1].

2. FUNDAMENTOS DEL RECURSO

El señor abogado de la Procuraduría solicitó el incremento del monto de la reparación civil, y argumentó lo siguiente:

[1] Es de mencionar que el acusado fue condenado por los delitos de fraude informático en perjuicio de don Mario Enrique Granda Cueto y asociación ilícita para delinquir en agravio del Estado, y se le impuso cuatro años de pena privativa de libertad suspendida condicionalmente por el término de tres años bajo el cumplimiento de reglas de conducta, noventa días de multa y cinco mil soles que deberá abonar a favor de cada agraviado.

2.1. Conforme el artículo noventa y tres del Código Penal (en adelante CP) la reparación civil comprende: i) la restitución del bien o, si no es posible, el pago de su valor; y, ii) la indemnización de daños y perjuicios.

2.2. El gasto que irroga el Estado peruano en la lucha contra el crimen organizado, es un problema que atenta de forma dramática contra el desarrollo de las naciones y demanda de presupuesto nacional de la República durante cada año.

2.3. La adquisición de la nueva tecnología para la lucha contra el crimen organizado, para optimizar y fortalecer acciones contra la delincuencia, así como su ejecución de operaciones diversas, constituye el daño emergente.

2.4. Los gastos que realiza el Estado peruano para luchar contra la criminalidad organizada, en términos de inversión social hubiesen permitido atender bienes jurídicos de primera generación reconocidos constitucionalmente, como son el financiamiento y construcción de hospitales, centros educativos, lo que se encuadra en el lucro cesante.

2.5. En suma, la pretensión reparatoria de treinta mil soles, no es excesiva y tampoco produce enriquecimiento indebido en la esfera patrimonial de la entidad agraviada ni vulnera el derecho patrimonial del acusado.

3. SINOPSIS FÁCTICA SEGÚN LA IMPUTACIÓN

Se imputó al procesado don David Ricardo Moretti Valdivia que junto a otros coprocesados efectuó operaciones fraudulentas de los fondos de las tarjetas de débito y crédito del Banco Interbank, cuyo titular es don Mario Enrique Granda Cueto; se realizó transferencias y pagos entre los meses de noviembre y diciembre de dos mil diez, por montos ascendentes a diecisiete mil ciento veinte soles y seiscientos sesenta y ocho dólares estadounidenses, para lo cual habrían obtenido el número de la tarjeta y la clave token del agraviado, por medio de páginas web falsas, creadas con el fin de acceder a la cuenta bancaria del agraviado, además se actualizó el número del teléfono del contacto del Banco Interbank para recabar la clave a través de mensajes de textos.

4. OPINIÓN DE LA FISCALÍA SUPREMA EN LO PENAL

Mediante Dictamen N.° 349-2019-MP-FN-SFSP (folios dieciocho a veinticuatro del cuadernillo formado en esta instancia), el señor fiscal de la Segunda Fiscalía Suprema en lo Penal opinó que se debe declarar no haber nulidad en la sentencia recurrida.

CONSIDERANDO

PRIMERO. SUSTENTO NORMATIVO (en adelante SN)

1.1. Es principio y derecho de la función jurisdiccional la observancia del debido proceso y la tutela jurisdiccional, conforme lo señala el inciso tercero, del artículo ciento treinta y nueve, de la Constitución Política del Estado; así como el artículo ocho de la Convención Americana sobre Derechos Humanos, aprobada y ratificada por el Estado peruano.

1.2. El numeral cinco, del artículo ciento treinta y nueve, de la Constitución Política del Perú establece que las decisiones judiciales deben ser motivadas.

1.3. El artículo noventa y tres del CP establece que la reparación civil comprende: **a)** la restitución del bien o, si no es posible, el pago de su valor, y **b)** la indemnización de los daños y perjuicios.

1.4. El primer párrafo, del artículo trescientos diecisiete, del CP (vigente al momento de los hechos) sanciona con pena privativa de libertad no menor de tres ni mayor de seis años, al que forma parte de una organización de dos o más personas destinada a cometer delitos será reprimido por el solo hecho de ser miembro de la misma.

1.5. El artículo cinco de la Ley número veintiocho mil ciento veintidós, considera los efectos del reconocimiento de los cargos por parte del encausado, y fija las condiciones que legitiman dar anticipadamente por concluido el debate oral.

1.6. En el Acuerdo Plenario N.° cinco-dos mil ocho/CJ-ciento dieciséis, del dieciocho de julio de dos mil ocho, se indicó que cuando la conformidad cumple los requisitos legales, importa necesariamente una reducción de la pena, dimensión que en cada caso concreto debe ser

establecida razonadamente por el juez correspondiente, y que debe ser inferior al sexto establecido para la terminación anticipada. Asimismo, en el fundamento veinticinco, señaló con relación a la reparación civil, que es evidente que si existe una pretensión civil alternativa, ejercitada conforme con lo dispuesto en el artículo doscientos veintisiete del Código de Procedimientos Penales, el imputado deberá referirse a ella en el marco de la responsabilidad civil que le corresponde admitir. En ese ámbito, por imperio de la garantía de tutela jurisdiccional –artículo 139.3 de la Constitución–, se debe dar plena intervención a la parte civil.

1.7. El Acuerdo Plenario número seis-dos mil seis/CJ-ciento dieciséis, destaca en su fundamento diez que:

> "[…] el daño civil lesiona derechos de naturaleza económica y/o derechos o legítimos intereses existenciales, no patrimoniales, de las personas. Por consiguiente, aun cuando es distinto el objeto sobre el que recae la lesión en la ofensa penal y en el daño civil, es claro que, pese a que no se haya producido un resultado delictivo concreto, es posible que existan daños civiles que deban ser reparados. […] En los delitos de peligro, desde luego, no cabe negar *a priori* la posibilidad de que surja responsabilidad civil, puesto que en ellos –sin perjuicio, según los casos, de efectivos daños generados en intereses individuales concretos– se produce una alteración del ordenamiento jurídico con entidad suficiente, según los casos, para ocasionar daños civiles, sobre el que obviamente incide el interés tutelado por la norma penal –que, por lo general y que siempre sea así, es de carácter supraindividual–. Esta delictiva alteración o perturbación del ordenamiento jurídico se debe procurar restablecer, así como los efectos que directa o causalmente ha ocasionado su comisión […]. Por consiguiente, no cabe descartar la existencia de responsabilidad civil en esta clase de delitos y, en tal virtud, corresponderá al órgano jurisdiccional en lo penal determinar su presencia y fijar su cuantía […]".

SEGUNDO. ANÁLISIS JURÍDICO FÁCTICO

2.1. El procesado se acogió la institución de la conclusión anticipada, en el margen de la denominada "conformidad absoluta" (hechos, responsabilidad penal, pena y reparación civil; es decir, la declaración de culpabilidad del imputado no se limita al hecho, también alcanza a las consecuencias jurídicas). De tal manera, el acusado, quien contó con el asesoramiento del abogado defensor (acto unilateral), aceptó los cargos incriminados por el señor fiscal superior y no manifestó su disconformidad en el requerimiento del monto dinerario por concepto

de reparación civil (como aparece en los folios seiscientos cincuenta y seiscientos cincuenta y uno vuelta).

2.2. Cabe señalar que todo delito acarrea como consecuencia no solo la imposición de una pena, sino también da lugar al surgimiento de la responsabilidad civil por parte del autor o los autores, la que será fijada en atención a lo previsto en la ley.

2.3. La Procuraduría Pública Especializada en Delitos de Orden Público del Ministerio del Interior, solicitó la constitución en parte civil el once de noviembre de dos mil trece (véase el los folios trescientos cincuenta y tres a trescientos cincuenta y cuatro), emitiéndose la resolución correspondiente el veintiséis de diciembre de dos mil trece (véase el folio trescientos cincuenta y siete).

2.4. Según se aprecia de los folios seiscientos doce a seiscientos dieciséis, la Procuraduría en cuanto al delito de AID solicitó, cinco días antes, del inicio de juicio oral, el incremento de reparación civil a la suma de treinta mil soles, por lo que la postulación fue oportuna.

2.5. El veinticinco de setiembre de dos mil dieciocho durante la audiencia de juicio oral, el director de debates dio cuenta a las partes de la pretensión de incremento de la reparación civil planteada por la procuraduría recurrente, disponiéndose que "se agreguen a los actuados y se tenga presente en lo que fuera de ley", luego de ello, se dio lectura a la acusación fiscal contra el procesado, ahora condenado, y finalmente se procedió a la conclusión anticipada del proceso, sin un pronunciamiento sobre la pretensión del procurador, postulando únicamente la pretensión civil incluida en la acusación fiscal (véase los folios seiscientos cincuenta a seiscientos cincuenta y dos).

2.6. El artículo cincuenta y ocho del Código de Procedimientos Penales indica que la parte civil "tiene personería para promover en la instrucción incidentes sobre cuestiones que afecten su derecho, e intervenir en los que hayan sido originados por el Ministerio Público o el inculpado"; en consideración a ello, consta del expediente que el señor abogado de la Procuraduría expresó su disconformidad en la cantidad del monto fijado por concepto de reparación civil en cuanto al delito

de AID, sin que el juzgado exprese las razones para para desestimar la pretensión civil.

2.7. El procurador alegó que el monto por concepto de reparación civil al Estado debió responder a la afectación del bien jurídico, las políticas de prevención y los gastos ocasionados por el Estado peruano en la lucha contra el crimen organizado, lo que demanda de presupuesto nacional de la República cada año en la adquisición de nueva tecnología para optimizar y fortalecer acciones contra la delincuencia, así como su ejecución de operaciones diversas.

2.8. Al momento de justificar el monto reparatorio, los magistrados del Colegiado Superior no consideraron la propuesta del Ministerio Público (diez mil soles) ni lo solicitado por la Procuraduría, que contaba con legitimidad para hacerlo por ser parte civil (treinta mil soles); por tanto la decisión en ese extremo no contiene la motivación suficiente.

2.9. En cuanto al monto de la reparación civil de treinta mil soles solicitada, debe tenerse presente que el delito que dio origen al monto indemnizatorio es AID, delito de peligro cuyos márgenes para la imposición de una cuantía indemnizatoria no se hallan delimitados por reglamentos administrativos, como en el caso de la reparación civil por el delito de conducción en estado ebriedad[2], la ponderación debe

[2] Mediante Resolución de la Fiscalía de la Nación N.° 2508-2013-MP-FN, del treinta de agosto de dos mil trece, se modificó el "Reglamento de Aplicación del Principio de Oportunidad, aprobado por Resolución de la Fiscalía de la Nación N.° 1470-2005-MP-FN", estableciendo una tabla de referencias para la reparación civil en los delitos de conducción en estado de ebriedad:

Períodos de Alcoholemia		Vehículo motorizado menor de 04 ruedas, (incluye cuatrimotos)	Vehículo motorizado de 04 ruedas a más, (no incluye cuatrimotos)
1er período de alcoholemia: **subclínico**	De 0.25 a 0.5 g/l. (Ley N.° 29439)	*	*
2do período de alcoholemia: **ebriedad**	Más de 0.5 a 1.0 g/l Más de 1.0 a 1.5 g/l.	**5% UIT a 50% UIT** **10% UIT a 50% UIT**	**10% UIT a 1 UIT** **15% UIT a 1 UIT**
3er período de alcoholemia: **ebriedad absoluta**	Más de 1.5 a 2.0 g/l Más de 2.0 a 2.5 g/l	**15% UIT a 1 UIT** **20% UIT a 1 UIT**	**20% UIT a 1.5 UIT** **25% UIT a 1.5 UIT**
4to período de alcoholemia: **grave alteración de la conciencia**	Más de 2.5 a 3.0 g/l Más de 3.0 a 3.5 g/l.	**25% UIT a 1UIT** **30% UIT a 1 UIT**	**30% UIT a 2 UIT** **35% UIT a 2 UIT**
5to período de alcoholemia: **Coma**	Más de 3.5 g/l.	**35% UIT a 1 UIT**	**40% UIT a 2 UIT**

realizarse por el juzgador expresando las razones para tal determinación[3].

2.10. No cabe duda que el delito materia de proceso afecta gravemente a la sociedad, como se reconoce en la Exposición de Motivos del Decreto Legislativo N.° 1244, que modificó el artículo trescientos diecisiete del Código Penal, donde se expuso lo siguiente:

> […] la justificación de la criminalización se basa en el hecho que la existencia de la asociación genera inevitablemente alarma y preocupación en la ciudadanía, independientemente de si los delitos se ha cometido o no. Sin embargo, ello no quiere decir que, en el delito de asociación para delinquir se pena la actividad preparatoria del delito fin, sino que lo que se busca es castigar eficazmente, desde la perspectiva político–criminal, las conductas plurales de intervención activa en una asociación, en razón del peligro que generan contra bienes jurídicos, tanto colectivos como individuales […].

2.11. Además, debe tenerse en cuenta que el delito materia de imputación es el de AID, relacionado a la comisión de delitos de contenido patrimonial y de alta complejidad mediante el uso de la tecnología informática, puesto que según los hechos atribuidos los procesados lograron obtener el número de las tarjetas bancarias a través de la creación de una página web que emulaba una verdadera, técnica conocida como "Phishing" o también denominada "Phishing bancario" mediante la cual se simula la página web de una entidad bancaria para lograr la obtención del número de tarjetas y claves de seguridad, es por tanto la actuación de una asociación de cibercriminales.

2.12. En el caso en concreto, existió la aceptación de cargos del encausado, y el monto fijado por el Colegiado Superior, desconociendo la pretensión del procurador habilitado para solicitar la reparación civil no guarda relación directa con la dimensión de la afectación; por tanto, sobre la base de este criterio y teniendo en cuenta que la procuraduría propuso su pretensión a tiempo, el monto de reparación civil debe ser incrementado, en consonancia con el acuerdo plenario referido en el uno punto siete del SN, aunque no a la dimensión

[3] El ponente estima que el debate de la cuestión probablemente merecerá en adelante replanteamientos jurisdiccionales.

solicitada por la parte legitimada, resultando adecuada la suma de veinte mil soles[4].

2.13. Además, debe tenerse en cuenta que es línea pacifica en la jurisprudencia de esta Instancia Suprema la imposición de reparación civil en los delitos de peligro, como se recoge en el Recurso de Nulidad N.° 1895-2016-Callao, del treinta de mayo de dos mil diecisiete, en cuyo fundamento tres punto cuatro se reconoce que existen daños a la sociedad que no pueden ser viables de cuantificar, por lo que cabe de que la reparación se determine objetivamente en consideración a "la gravedad del delito", su trascendencia y de tal forma que no resulte un monto ínfimo.

DECISIÓN

Por ello, impartiendo justicia a nombre del pueblo, con lo expuesto por el señor fiscal supremo en lo penal, los integrantes de la Sala Penal Transitoria de la Corte Suprema de Justicia, **ACUERDAN**:

I. DECLARAR HABER NULIDAD la sentencia conformada del veintisiete de setiembre de dos mil dieciocho (folios seiscientos cincuenta y cuatro a seiscientos cincuenta y nueve), emitida por la Sexta Sala Especializada en lo Penal para Procesos con Reos Libres de la Corte Superior de Justicia de Lima, en cuanto fijó por concepto de reparación civil la suma de **cinco mil soles**, que pagará el sentenciado don David Ricardo Moretti Valdivia a favor del Estado peruano, al haber sido condenado como autor del delito de asociación ilícita para delinquir; **REFORMÁNDOLA**, la fijaron en **veinte mil soles**, en los términos señalados por el Colegiado Superior.

II. NO HABER NULIDAD en lo demás que contiene. Hágase saber y los devolvieron.

S. S.

PRADO SALDARRIAGA
SALAS ARENAS
CASTAÑEDA OTSU
PACHECO HUANCAS
AQUIZE DÍAZ

JS/blv

[4] Ni el presupuesto periódico de la política de lucha contra el crimen organizado ni los costos que importa al sistema judicial, justifican el incremento en el caso concreto. Se trata de argumentos genéricos muy extensivos.

RESOLUCIÓN FINAL Nº 2014-2016/CC1

PROCEDENCIA	:	**ÓRGANO RESOLUTIVO DE PROCEDIMIENTOS SUMARÍSIMOS DE PROTECCIÓN AL CONSUMIDOR Nº 2**
DENUNCIANTE	:	**[redacted] (LA SEÑORA [redacted])**
DENUNCIADO	:	**BANCO DE CRÉDITO DEL PERÚ S.A.[1] (EL BANCO)**
MATERIA	:	**PROTECCIÓN AL CONSUMIDOR** **TARJETA DE DÉBITO** **IDONEIDAD DEL SERVICIO** **MEDIDAS CORRECTIVAS** **GRADUACIÓN DE LA SANCIÓN** **COSTAS Y COSTOS**
ACTIVIDAD	:	**SISTEMA FINANCIERO BANCARIO**
SANCIÓN	:	***BANCO DE CRÉDITO DEL PERÚ S.A.: 0,54 UIT***

Lima, 28 de septiembre de 2016

ANTECEDENTES

1. Mediante escrito del 5 de junio de 2015, la señora [redacted]t denunció al Banco por presunta infracción de la Ley Nº 29571, Código de Protección y Defensa del Consumidor (en adelante, el Código)[2], manifestando lo siguiente:

   (i) El 11 de marzo de 2013, fue víctima de un robo informático bajo la modalidad de *Phishing*. Al darse cuenta del referido hecho, ingresó a la página web del Banco y se percató de la sustracción de su cuenta de ahorros por el monto de S/ 4 600,00.

   (ii) Agregó que, en ese momento, llamó a la entidad financiera para realizar el bloqueo de su cuenta; pero, debido a la lentitud de la atención, se sustrajo un monto adicional de S/ 2 150,00.

   (iii) Al observar la segunda operación, reclamó verbalmente mediante la Banca Telefónica, siendo que la persona con la que se comunicaba se limitó a llenar un formulario de reclamo.

   (iv) Luego de efectuar la llamada, se acercó a una agencia del Banco para solicitar impreso el reclamo formulado vía telefónica y además una nueva tarjeta. En ese momento, tomó conocimiento que los delincuentes informáticos se tomaron el tiempo de cambiar sus datos personales, incluyendo su correo electrónico donde esperaban recibir las notificaciones de las operaciones cuestionadas.

   (v) El sistema de seguridad del Banco falló al permitir que, de manera simultánea, se pueda estar en la Banca Móvil y vía página web, lo cual permitió la realización de las operaciones antes indicadas.

---

1 **RUC:** 20100047218

2 Publicado en el diario oficial El Peruano el 2 de septiembre del 2010 y vigente desde el 2 de octubre del 2010.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú / Telf.: 224 7800
e-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

(vi) Finalmente, decidió realizar la denuncia ante la División de Investigaciones de Delitos de Alta Tecnología (en adelante, DIVINTAD), quienes, a la fecha de interposición de la denuncia, se encuentran limitados para continuar con las investigaciones, en tanto el Banco no les brinda la información necesaria.

(vii) Solicitó como medida correctiva, que se ordene al Banco la devolución del monto total de S/ 6 750,00 , así como el pago de las costas y costos del procedimiento.

2. Mediante Resolución N° 1 del 15 de julio de 2015, el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor N° 2 (en adelante, el OPS2), inició un procedimiento administrativo sancionador contra el Banco, considerando el presunto hecho infractor:

> *"**PRIMERO**: iniciar un procedimiento administrativo sancionador a Banco de Crédito del Perú por la presunta infracción a lo establecido en los artículos 1° literal c), 18° y 19° del Código de Protección y Defensa del Consumidor, en tanto que, por falta de medidas de seguridad, habría autorizado dos (2) transferencia bancarias realizadas vía internet, descontadas de la cuenta de ahorros N° ****-4031 (Tarjeta de Débito N° 4557-****-****-0186) de la señora Grit Marlen [redacted], que no reconoce:*

Fecha	Descripción	Importe S/
11.03.15	TRAN.CTAS TERC. BM	4 600,00
11.03.15	TRAN.CTAS TERC. BM	2 150,00

> *(...)"*

3. El 4 de agosto de 2015, el Banco presentó sus descargos, señalando lo siguiente:

(i) Entregó a la seño[redacted]st la Tarjeta Credimás N° ****-0186 a fin de que realizara operaciones en su Cuenta de Ahorros N° ****-4031, mediante el empleo conjunto de dicha tarjeta y la clave secreta.

(ii) Las transferencias cuestionadas corresponden a dos (2) operaciones efectuadas a través de la Banca Móvil.

(iii) La Banca Móvil BCP permite realizar consultas y operaciones desde cualquier celular de forma rápida y segura, así como ubicar puntos de atención y descuentos más cercanos en simples pasos.

(iv) Para ingresar al sistema Banca Móvil se necesitaba efectuar lo siguiente: a) descargar la aplicación Banca Móvil BCP; b) ingresar el número de la tarjeta débito y la clave internet; y, c) asignar un seudónimo a las cuentas y teléfonos celulares que se registraron. Asimismo, por medidas de seguridad, si se ingresa tres (3) veces de forma incorrecta la Clave de Internet los accesos de la referida aplicación quedarán bloqueados por el resto del día.

(v) Del reporte emitido por su sistema, se verifica que el celular con el cual se realizaron las transferencias cuestionadas se afilió a la Banca Móvil, cumpliendo todos los requisitos y medidas de seguridad establecidas para ello.

(vi) Toda operación o afiliación efectuada con la tarjeta, requiere el empleo de la firma electrónica, por lo que se reputa como válida y aceptada por el cliente, toda vez que asume la obligación de mantener a buen resguardo y bajo su posesión su tarjeta y las respectivas claves secretas.

(vii) Las medidas de seguridad se encuentran determinadas por los mecanismos establecidos para la afiliación de teléfonos celulares a su Banca Móvil, los cuales son el empleo de la Tarjeta Credimás y las respectivas claves secretas.

4. Mediante Resolución Final N° 870-2015/PS2 del 25 de agosto de 2015, el OPS2 emitió el siguiente pronunciamiento:

(i) Sancionó al Banco con una multa de dos (2) UIT por infracción a los artículos 1° literal c), 18° y 19° del Código, pues no acreditó que las operaciones cuestionadas se hayan efectuado válidamente.

(ii) Ordenó al Banco, en calidad de medida correctiva, que cumpla con devolver a la denunciante el importe de S/ 6 750,00 por las operaciones que le fueron descontadas. Asimismo, lo condenó al pago de las costas y costos del procedimiento.

(iii) Dispuso la inscripción del Banco en el Registro de Infracciones y Sanciones del Indecopi, una vez que la referida resolución quede firme.

5. El 9 de septiembre de 2015, el Banco apeló la referida resolución, reiterando los argumentos vertidos en sus descargos.

6. El 28 de octubre de 2015, el Banco presentó un escrito adicional a su recurso de apelación, mediante el cual reiteró el procedimiento para efectuarse transferencias a cuenta de terceros de la misma entidad y señaló lo siguiente:

(i) A través de los reportes de su sistema se acredita que el celular utilizado para las transferencias cuestionadas se encontraba afiliado a la Banca Móvil. Asimismo, cumplió con remitir el código de validación al celular de la denunciante, quien culminó el proceso de afiliación ingresando el código de validación y la primera transferencia (S/ 4 600,00) fue confirmada con el uso de la Clave Digital (Token).

(ii) En relación a la segunda transferencia (S/ 2 150,00), en tanto fue registrada dentro de las operaciones favoritas, no se requirió el ingreso de la Clave Digital (Token) para confirmarse.

7. Mediante Resolución N° 3 del 8 de marzo de 2016, la Secretaría Técnica de la Comisión requirió al Banco que presente lo siguiente:

(i) Impresión de pantalla del reporte y consulta de operaciones realizadas en "Homebanking" y del reporte del sistema denominado "Log Ace Server", en donde se verifique el ingreso del número de la tarjeta, la clave de acceso a banca móvil y la clave digital token de las operaciones cuestionadas.

(ii) Precisar y explicar el rubro, de la impresión de pantalla de sus sistemas, donde se verifica el ingreso de la clave de acceso a banca móvil y la clave digital token de las operaciones cuestionadas.

8. El 16 de marzo de 2016, el Banco presentó un escrito reiterando el procedimiento establecido para efectuarse las transacciones a cuenta de terceros de la misma entidad, a través del aplicativo "Banca Móvil". Asimismo, adjuntó la impresión de pantalla de sus sistemas en el cual se observaría el ingreso de la clave de acceso a la referida vía y la clave digital token respecto a la operación por S/ 4 600,00.

9. El 6 de abril de 2016, el Banco presentó un escrito adicional, mediante el cual adjuntó copia visada del reporte denominado "LOG ACE SERVER", el cual acreditaría el uso de la clave digital "Token", en la operación de S/ 4 600,00.

10. Por Resolución N° 6 del 3 de junio de 2016, la Secretaría Técnica de la Comisión requirió al Banco lo siguiente:

(i) Impresión de pantalla del reporte de su sistema en el cual se pueda visualizar lo siguiente:

a. El ingreso del número celular afiliado a la Banca Móvil BCP, número de la tarjeta de crédito y clave de internet;
b. el envío del código de validación para afiliarse a la Banca Móvil al celular y/o correo electrónico elegido para dicho efecto; y,
c. constancia de la afiliación a la Banca Móvil del celular utilizado para la operación materia de cuestionamiento en el presente procedimiento.

(ii) El procedimiento y/o protocolo establecido para realizar operaciones a través de la Banca Móvil BCP.

(iii) Precisar si el sistema que se utilizan para la Banca Móvil es el denominado "*Homebanking*", caso contrario señalar y presentar impresión del sistema que utilizan para el mencionado canal.

11. El 30 de junio de 2016, el Banco absolvió el requerimiento efectuado por la Secretaría Técnica de la Comisión.

ANÁLISIS

Sobre el deber de idoneidad

Marco teórico

12. El artículo 65° de la Constitución Política del Perú consagra la defensa por el Estado peruano de los intereses de los consumidores[3], mandato que es recogido en el literal c)

[3] **CONSTITUCIÓN POLÍTICA DEL PERÚ, publicada el 30 de diciembre de 1993**
Artículo 65°.- El Estado defiende el interés de los consumidores y usuarios. Para tal efecto garantiza el derecho a la información sobre los bienes y servicios que se encuentran a su disposición en el mercado. Asimismo vela, en particular,

del numeral 1.1 del artículo 1° del Código, el cual reconoce el derecho de los consumidores a la protección de sus intereses económicos y establece la protección contra métodos comerciales coercitivos o cualquier otra práctica similar, así como frente a información interesadamente equívoca respecto de los productos o servicios que son ofrecidos en el mercado[4].

13. Al respecto, todo proveedor ofrece una garantía sobre la idoneidad de los bienes y servicios que ofrece en el mercado, lo anterior en función de la información que traslada a los consumidores de manera expresa o tácita. En tal sentido, para establecer la existencia de una infracción corresponderá al consumidor o a la autoridad administrativa acreditar la existencia del defecto, siendo que ante tal situación será de carga del proveedor demostrar que dicho defecto no le es imputable para ser eximido de responsabilidad[5].

14. En efecto, una vez que se ha probado el defecto, sea con los medios probatorios presentados por el consumidor o por los aportados de oficio por la Secretaría Técnica de la Comisión, si el proveedor pretende ser eximido de responsabilidad deberá aportar pruebas que acrediten la fractura del nexo causal o que actuó con la diligencia requerida.

15. Sin embargo, se debe tener presente que existen supuestos en los que la carga probatoria debe flexibilizarse. En efecto, el Tribunal de Defensa de la Competencia señaló mediante Resolución N° 270-2008/TDC-Indecopi de fecha 13 de febrero de 2008, que la comprobación de un hecho negativo –como la no realización de transferencias vía internet– no es factible para el interesado. Siendo ello así, el proveedor del servicio es quien debe probar que el hecho negado sí se produjo, esto es, que las operaciones cuestionadas se realizaron válidamente.

16. En ese sentido, la Sala de Defensa de la Competencia N° 2 (ahora, Sala Especializada en Protección al Consumidor y en adelante, la Sala) ha establecido que, en casos de

---

por la salud y la seguridad de la población.

4 **LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de septiembre de 2010**
Artículo 1°.- Derechos de los consumidores
1.1 En los términos establecidos por el presente Código, los consumidores tienen los siguientes derechos:
(...)
c. Derecho a la protección de sus intereses económicos y en particular contra las cláusulas abusivas, métodos comerciales coercitivos, cualquier otra práctica análoga e información interesadamente equívoca sobre los productos o servicios.

5 **LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de septiembre de 2010**
Artículo 18°.- Idoneidad
Se entiende por idoneidad la correspondencia entre lo que un consumidor espera y lo que efectivamente recibe, en función a lo que se le hubiera ofrecido, la publicidad e información transmitida, las condiciones y circunstancias de la transacción, las características y naturaleza del producto o servicio, el precio, entre otros factores, atendiendo a las circunstancias del caso.
La idoneidad es evaluada en función a la propia naturaleza del producto o servicio y a su aptitud para satisfacer la finalidad para la cual ha sido puesto en el mercado.
Las autorizaciones por parte de los organismos del Estado para la fabricación de un producto o la prestación de un servicio, en los casos que sea necesario, no eximen de responsabilidad al proveedor frente al consumidor.

Artículo 19°.- Obligación de los proveedores
El proveedor responde por la idoneidad y calidad de los productos y servicios ofrecidos; por la autenticidad de las marcas y leyendas que exhiben sus productos o del signo que respalda al prestador del servicio, por la falta de conformidad entre la publicidad comercial de los productos y servicios y éstos, así como por el contenido y la vida útil del producto indicado en el envase, en lo que corresponda.

operaciones vía internet, las entidades financieras deberán presentar la documentación que acredite que las transacciones se realizaron con el empleo de los datos de la tarjeta del cliente y las claves secretas que permitan validar las operaciones[6].

Aplicación al caso en concreto

17. El OPS2 declaró fundada la denuncia contra el Banco por la infracción a los artículos 1° literal c), 18° y 19° del Código, en tanto no acreditó que las operaciones cuestionadas se efectuaron válidamente.

18. En su escrito de apelación, el Banco reiteró los argumentos vertidos en su escrito de descargos, en tanto que las operaciones se efectuaron conforme al procedimiento establecido por este el cual implica:

    (i) Descargar la aplicación Banca Móvil BCP.
    (ii) Ingresar el número de la tarjeta de débito y la clave internet.
    (iii) Asignar un seudónimo a las cuentas y telefónos celulares que se registraron

19. De forma posterior, la entidad financiera presentó un escrito adicional, mediante el cual manifestó lo siguiente:

    (i) A través de los reportes de su sistema se acredita que el celular utilizado para las transferencias cuestionadas se encontraba afiliado a la Banca Móvil. Asimismo, cumplió con remitir el código de validación al celular de la denunciante, quien culminó el proceso de afiliación ingresando el código de validación y la primera transferencia (S/ 4 600,00) fue confirmada con el uso de la Clave Digital (Token).

    (ii) En relación a la segunda transferencia (S/ 2 150,00), en tanto fue registrada dentro de las operaciones favoritas, no se requirió el ingreso de la Clave Digital (Token) para confirmarse.

20. Sobre el particular, la Comisión considera que los consumidores o usuarios de servicios financieros esperan que sus proveedores les brinden un servicio responsable e idóneo, capaz de generar seguridad en cada una de las transacciones que realicen.

21. En ese sentido, el parámetro de idoneidad en este tipo de casos está constituido por los mecanismos de seguridad implementados por los proveedores para realizar operaciones a través de sus aplicativos móviles, por ello, es necesario que, dentro de un procedimiento de este tipo, en donde se cuestiona el servicio brindado por el Banco, sea este quien presente medios probatorios suficientes para desvirtuar el hecho denunciado y corrobore que autorizó válidamente las operaciones cuestionadas.

22. En mérito a ello, a fin de determinar la responsabilidad de las entidades financieras, la autoridad de consumo deberá verificar si la operación realizada a través del aplicativo Móvil se efectuó de acuerdo a parámetros de seguridad mínimos implementados por el proveedor, como es el ingreso de las respectivas claves que otorguen validez a dichas

[6] Ver Resolución N° 762-2010/SC2 del 19 de abril de 2010 en el procedimiento seguido por la señora María Esther Cárdenas Valencia en contra de Scotiabank Perú S.A.A.; Resolución N° 2684-2010/SC2 del 29 de noviembre de 2010 en el procedimiento seguido por el señor Christian Burgos del Campo.

transacciones. En tal sentido, de acreditarse que la operación fue realizada en observancia a dichas medidas de seguridad, las entidades financieras no incurrirán en responsabilidad administrativa.

23. Sobre el particular, de los actuados en el expediente y de acuerdo a lo manifestado por las partes en el procedimiento, se aprecia que el 11 de marzo de 2015 se realizaron dos (2) transferencias por internet por los importes de S/ 4 600,00 y S/ 2 150,00 con la Tarjeta Credimás ****-0186 de titularidad de la denunciante, hacia la Cuenta N° ****-3080 perteneciente al señor Percy Huayuri Santana.

24. De conformidad con lo manifestado por el Banco en sus descargos y en su recurso de apelación, a fin de que el cliente pueda utilizar la Banca Móvil BCP deberá descargar dicha aplicación al teléfono celular y de forma posterior afiliarse al mismo ingresando conjuntamente el número de la Tarjeta Credimás y clave de internet. Asimismo, deberá elegir el medio (celular o correo electrónico) mediante el cual se le hará llegar un código de validación, ello para completar con el procedimiento señalado.

25. Por otro lado, una vez que el cliente ingresa a su sesión a la Banca Móvil BCP, para efectuar una operación, como en el presente caso, es necesario el ingreso de una clave digital (Token), cuya digitación confirma la operación; sin embargo, cuando la cuenta sea registrada como favorita ya no se necesitará el ingreso de la mencionada clave.

26. Lo anterior significa que para efectuar operaciones por la Banca Móvil BCP, resulta imprescindible afiliarse a la misma, ingresando conjuntamente el número de la Tarjeta Credimás y clave de internet respectiva.

27. Adicionalmente, de una revisión del canal virtual del Banco (*https://www.youtube.com/watch?v=rt7VvMFHxlU*), este Colegiado verifica que los pasos a seguir a fin de que un usuario se afilie a la Banca Móvil BCP, son los siguientes:

Imagen N° 1: bajar el aplicativo al Móvil

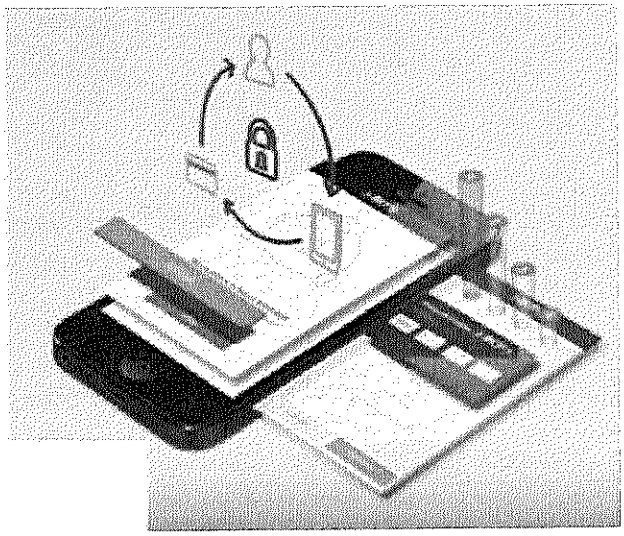


Imagen N° 2: digitar conjuntamente el número de la tarjeta Credimás y la Clave de Internet

Imagen N° 3: elegir un medio (telefónico o mail) al cual deberá llegar el código de validación

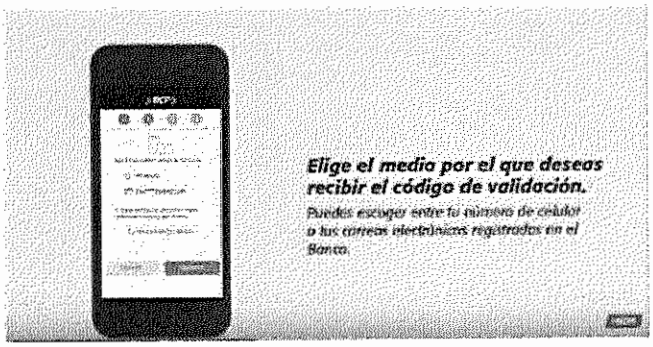


Imagen N° 4: completar datos personales e ingresar el código de validación

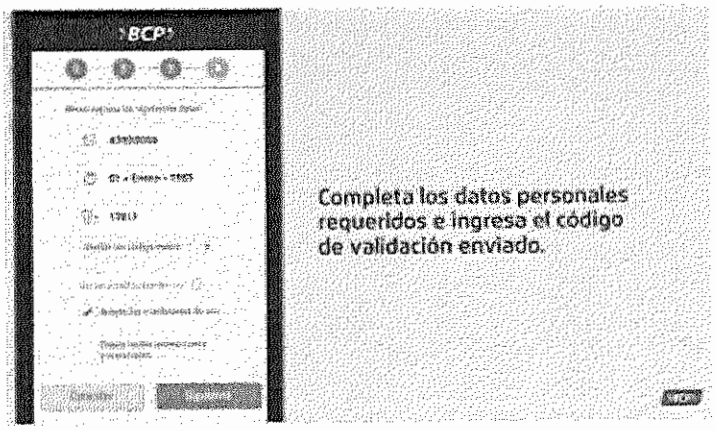


Imagen N° 5: confirmación de afiliación

28. A efectos de deslindar la responsabilidad del Banco respecto al hecho imputado, este Colegiado considera que en primer lugar, se debe analizar si el celular mediante el cual se efectuaron las operaciones materia de cuestionamiento se encontraba afiliado a la Banca Móvil BCP y de forma posterior comprobar que las referidas operaciones se efectuaron válidamente respetando los mecanismos de seguridad correspondientes.

29. Al respecto, a fin de acreditar que el denunciante se encontraba afiliado a la Banca Móvil, el Banco presentó un reporte emitido por su sistema que acreditaría la afiliación del teléfono celular del cual se efectuó las operaciones cuestionadas y la validación de la misma a través del ingreso de la clave token[7]:

Extracto del Reporte del Sistema del Banco y explicación del mismo:

User_Ac	Credimás	Operation Time	Name	Status	Status	Token Session	Server	Explicación
34765502		2015-03-11 14:43:56	REGISTER - login de la sesión de aplicación	Fin del Servicio Rest.	0	f48d4950c82611e4bd5fd2b3722a8102	PMOBANKAPPP01	Inicio de la aplicación
34766200		2015-03-11 14:44:16	LOGIN - registro de credimás/usuario	Inicio de Llamada al core para validar la tarjeta credimás	0	f48d4950c82611e4bd5fd2b3722a8102	PMOBANKAPPP01	Afiliación de dispositivo
34766581	****-0186	2015-03-11 14:44:25	SENDCHANNELCODE - Petición de envío de código al canal	Fin del Servicio Rest.	0	f48d4950c82611e4bd5fd2b3722a8102	PMOBANKAPPP02	Envío de código de afiliación a Banca Móvil
34767433		2015-03-11 14:44:58	NEWDEVICE - afiliación de usuario/dispositivo. Valida el código enviado al canal	Inicio del Servicio Rest	0	f48d4950c82611e4bd5fd2b3722a8102	PMOBANKAPPP01	Ingreso de código de afiliación a Banca Móvil

Fuente: transcripción elaborada por la Secretaría Técnica

7 A fojas 163 del Expediente.

30. Sobre el particular, del reporte emitido por el sistema del Banco este Colegiado observa que el celular de la denunciante se encontraba afiliado a la Banca Móvil BCP, cumpliendo los requisitos previamente establecidos para dicha finalidad, esto es, el ingreso conjunto del número de la tarjeta de débito de la consumidora y la respectiva clave virtual, así como la convalidación posterior con el ingreso del código de validación correspondiente. Así, correspondería verificar la validez de la operaciones cuestionadas por la denunciante.

31. Al respecto, el banco a fin de acreditar la validez de las operaciones presentó lo siguiente:

    (i) Reporte del documento denominado "log Ace Server" y del sistema del Banco[8], en el cual se verificaría el ingreso de la clave token para validar la operación de S/ 4 600,00:

Imagen N° 6: validación de la operación (ingreso token)

Log Ace Server

	Column 3	Column 4	Column 6	Column 7	Column 8	Column 16
1	03/01/2015	19:55:47	"MEIST NN GRIT MARLEN"	"10726377"	"000115354748"	"Passcode accepted"
2	03/01/2015	19:55:47	"MEIST NN GRIT MARLEN"	"10726377"	"000115354748"	"Passcode accepted"
3	03/11/2015	14:47:26	"MEIST NN GRIT MARLEN"	"10726377"	"000115354748"	"Passcode accepted"

Extracto del Reporte del Sistema del Banco y explicación del mismo:

User_Ac	Credimas	Operation_Time	Name	Status	Status	Token Session	Server	Explicación
34774458	****-0186	2015-03-11 14:48:05	TRANSCT - transferencia a cuentas BCP de terceros	Validación de token	0	f48d4950c82611e4bd5fd2b3722a8102	PMOBANKAPPP02	Ingreso de clave Token

Fuente: transcrito por la Secretaría Técnica

32. Conforme a los hechos expuesto, la denunciante no reconoce las transferencias de S/ 4 600,00 y S/ 2 150,00.

33. Respecto a la transferencia por el monto de S/ 4 600,00, los documentos denominados "Log Ace Server" y del sistema del Banco (Ver extracto del Reporte del punto ii) del numeral 28) generan certeza en este Colegiado que la referida transacción no reconocida por la señora [redacted] se efectuó en observancia de las medidas de seguridad establecidas por el propio denunciado, esto es, que de forma posterior a la afiliación a la Banca Móvil BCP, se autorizó la transferencia con el uso de la clave *Token* (ver imagen N° 6).

8 A fojas 162 y 164 del Expediente.

34. Respecto de la transferencia por el monto de S/ 2 150,00, el Banco señaló que para la validación de la misma no era necesario el ingreso de la clave digital token, en tanto la cuenta que fue favorecida con la referida operación se encontraba registrada por la señora Meist como "favorita".

35. Sobre el particular, es pertinente traer a colación que los sistemas de seguridad implementados por las entidades financieras para la autorización de operaciones de transferencia de fondos a través de canales electrónicos, se encuentran regulados por la normativa pertinente.

36. Al respecto, cabe precisar que para este tipo de operaciones la Superintendencia de Banca, Seguros y AFP ha emitido la Circular N° G-140-2009, Gestión de la Seguridad de la Información (en adelante, la Circular), la cual en el artículo 6° hace referencia a la implementación de sistemas de autenticación para transferencia de fondos por canales electrónicos, conforme a lo siguiente:

> *"Artículo 6°.- En el caso de las operaciones de transferencia de fondos a terceros ofrecidas por las empresas para su realización a través de* ***canales electrónicos****, las empresas deberán implementar un esquema de autenticación de los clientes basado en dos factores como mínimo. Para el caso en que el canal electrónico sea Internet, uno de los factores de autenticación deberá ser de generación o asignación dinámica. Las empresas podrán utilizar otros factores de autenticación, en tanto estos proporcionen un nivel de seguridad equivalente o superior respecto a los dos factores señalados, en particular cuando se trate de operaciones importantes según los límites que el banco determine de acuerdo a las características del producto o servicio ofrecido"* (el resaltado es nuestro).

37. Tal como lo señala la Circular, las entidades bancarias y financieras deben contar con dos factores de autenticación, siendo que uno de ellos debe ser de generación o asignación dinámica u otro factor de nivel de seguridad equivalente o superior a fin de autorizar operaciones de transferencia de fondos a través de Banca electrónica.

38. El acceso a la Banca electrónica, cuenta con un primer factor de autenticación denominado "clave web", la cual, en conjunto con el ingreso del número de la tarjeta de débito o crédito afiliada, permite al usuario financiero ingresar a la plataforma de servicios en línea brindados por las entidades bancarias para disponer de los fondos de las cuentas de ahorros o líneas de crédito vinculadas a las tarjetas antes mencionadas.

39. Ahora bien, el ingreso a la plataforma virtual mediante el ingreso de la "clave web" no es suficiente para la autorización de transferencias a cuentas de terceros, pues para ello resulta fundamental contar previamente con un factor de autenticación dinámico, el cual es conocido en el mercado financiero como "clave dinámica" (dispositivo *token*, tarjeta de coordenadas o clave dinámica SMS, entre otros), que es brindado por las entidades financieras con el consentimiento del titular mediante documento contractual. Los dispositivos de clave dinámica son de uso personal e intransferible por parte del titular de la cuenta afiliada.

40. El ingreso de la clave dinámica representa entonces la llave de autorización de las transacciones respectivas a través del canal virtual utilizado, la cual responde a un protocolo de seguridad implementado por las entidades financieras. Es de precisar que la clave de asignación dinámica varía para cada una de las operaciones a realizar, ello

con el fin de prevenir el riesgo de fraude electrónico, siendo que solo mediante el ingreso correcto de dicha clave, el titular de la cuenta podrá realizar sus transacciones mediante la Banca electrónica.

41. Es pertinente señalar que dentro de los dispositivos empleados por las entidades financieras en la implementación de factores de autenticación dinámico se encuentra el dispositivo denominado "*Token*", el cual se caracteriza por brindar un PIN (por sus siglas en inglés, *Personal Identification Number*) numérico de seis a ocho dígitos, que varía cada treinta (30) segundos o un minuto (lo cual depende de la entidad financiera administradora de la cuenta), generando una nueva clave al azar[9], que debe ser ingresada a fin de autorizar operaciones a través de internet antes de que dicha clave se modifique.

42. Asimismo, las operaciones a través de Banca electrónica pueden realizarse mediante el empleo de una clave contenida en una "tarjeta de coordenadas", la cual comprende una serie de datos numéricos dispuestos en forma de plano cartesiano, es decir, una tabla con una cabecera de letras y filas de números cuya intersección genera una coordenada, siendo que para autorizar una operación debe ingresarse las coordenadas o celdas solicitadas por el sistema de forma aleatoria[10] para cada transacción.

43. Otro método para validar operaciones a través de internet es el empleo de la clave dinámica remitida a través de SMS (por sus siglas en inglés *Short Message Service*). Para la utilización de dicho servicio, es necesario afiliar la cuenta del usuario a un número de teléfono celular. Una vez realizado dicho procedimiento, el Banco remitirá una clave al teléfono celular vinculado cada vez que el consumidor desee realizar una transferencia a cuenta de terceros o pagos de servicios, el cual deberá ser ingresado en el soporte web (ya sea a través de una página web o de aplicaciones móviles) a fin de autorizar la operación de transferencia[11].

44. En tal sentido, el ingreso de la clave dinámica es el mecanismo indispensable para efectuar una transacción a través de Banca electrónica (ya sea a través de clave *token*, clave de coordenadas o clave SMS, entre otros); sin embargo, pese a lo normado y antes indicado. Así, conforme a lo expuesto correspondería al Banco presentar el documento emitido por su sistema que acredite que para la operación de S/ 2 150,00 también se ingresó la clave de asignación así como se realizó con la primera transacción.

45. Al respecto, el Banco se ha limitado a señalar **-sin presentar prueba que lo sustente-** que la segunda transacción (S/ 2 150,00) al dirigirse a una cuenta que se encontraba

---

9 Ver la Resolución Final N° 1311-2014/CC1 del 13 de noviembre de 2014.

10 Ver por ejemplo, la página web del BBVA Banco Continental S.A. la cual describe a la tarjeta de coordenadas como una herramienta que "contiene una serie de datos numéricos dispuestos en forma de coordenadas, por cada operación o ingreso que realices se te solicitará UNA COORDENADA en forma aleatoria para la autorización cuando el sistema te lo solicite". En: <<https://www.bbvacontinental.pe/meta/seguridad/>>.

11 Ver por ejemplo, la página web de Banco Internacional del Perú S.A.A. - Interbank. la cual señala respecto a la cave dinámica SMS lo siguiente: La Clave Dinámica SMS funciona únicamente para hacer operaciones a terceros desde la Banca por Internet. Para poder solicitar tu Clave Dinámica SMS deberás estar afiliado al servicio de Banca Celular ya que ahí llegarán estas claves por mensajes de texto. En <<http://www.interbank.com.pe/banca-celular-sms>>.

registrada como favorita por la denunciante no necesitaba el ingreso de la clave digital token para validar la misma; por lo tanto, vulneró los mecanismos de seguridad establecidos por el ordenamiento jurídico vigente al momento de los hechos al permitir indebidamente la mencionada transferencia.

46. A mayor abundamiento, este Colegido considera pertinente señalar que el mecanismo de seguridad impuesto por la norma tiene como finalidad evitar el fraude cibernético como, por ejemplo, el "Phishing" método utilizado por terceras personas para la obtención de datos e información sensible de las tarjetas de crédito, débito, clave *token*, clave de coordenadas o clave SMS, entre otros, de los consumidores, con el fin de realizar operaciones a través de internet.

47. En ese sentido, a vista de este Colegiado, el ingreso de las referidas claves como mecanismo de seguridad, cobra mayor relevancia para la realización de cada una de las transacciones a través de Banca electrónica, en tanto protege al cliente que con la información sensible obtenida se realicen consecutivas operaciones.

48. Por todo lo expuesto, esta Comisión considera que corresponde confirmar la Resolución Final N° 870-2015/PS2 que declaró fundada la denuncia en el extremo referido a la transacción no reconocida por el monto de S/ 2 150,00, en tanto el Banco permitió indebidamente la realización de la mencionada operación.

49. Asimismo, corresponde revocar la Resolución Final N° 870-2015/PS2, que declaró fundada la denuncia contra el Banco en el extremo referido a la transacción no reconocida por el monto de S/ 4 600,00; y reformándola, declararla infundada, en tanto quedó acreditado que la entidad financiera cumplió con observar los mecanismos de seguridad respectivos para la realización de dicha transacción.

Sobre la medida correctiva

50. Los artículos 114°, 115° y 116° del Código establecen la facultad que tiene la Comisión para, actuando de oficio o a pedido de parte, adoptar las medidas correctivas reparadoras que tengan por finalidad resarcir las consecuencias patrimoniales directas e inmediatas ocasionadas al consumidor por la infracción administrativa a su estado anterior y medidas correctivas complementarias que tienen por objeto revertir los efectos de la conducta infractora o evitar que esta se produzca nuevamente en el futuro.

51. El OPS2 ordenó al Banco, en calidad de medida correctiva, que en un plazo no mayor a cinco (5) días hábiles, contado a partir del día siguiente de notificada la referida resolución, que cumplan con devolver a la denunciante el importe de S/ 6 750,00 por las operaciones que le fueron descontadas.

52. En ese sentido, en la medida que la Resolución Final N° 870-2015/PS2 que declaró fundada la denuncia ha sido revocada parcialmente por esta Comisión, corresponde analizar la medida correctiva a ordenar en el presente extremo.

53. En el presente caso, se ha acreditado que la entidad financiera permitió indebidamente la realización de la transacción por el monto de S/ 2 150,00.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú / Telf.: 224 7800
e-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

54. Por lo expuesto, corresponde revocar la medida correctiva dictada por el OPS2 y reformándola ordenar al Banco, que en un plazo no mayor a cinco (5) días hábiles, contados a partir del día siguiente de notificada la presente resolución, cumpla con devolver a la denunciante el importe de S/ 2 150,00.

Sobre la graduación de la sanción

55. En este extremo, el OPS2 sancionó al Banco con una multa de dos (2) UIT por infracción a los artículos 1° literal c), 18° y 19° del Código, en tanto no acreditó que las operaciones cuestionadas se hayan efectuado válidamente.

56. Al respecto, la Comisión considera necesario efectuar un análisis de la graduación de la sanción efectuada contra el Banco, en la medida que, si bien se ha verificado la existencia de una infracción administrativa, se ha revocado la Resolución Final N° 723-2015/PS2 que declaró fundada la denuncia; y reformándola, se ha declarado fundada en parte, únicamente respecto a la transacción por el monto de S/ 2 150,00, por lo que amerita realizar un nuevo análisis a fin de determinar la sanción a imponerse.

57. Para proceder a la graduación de la sanción, deberá aplicarse de manera preferente los criterios previstos en el Código, y de manera supletoria los criterios contemplados en la LPAG.

58. El artículo 112° del Código establece que para determinar la gravedad de la infracción, la autoridad administrativa podrá tomar en consideración diversos criterios tales como el beneficio ilícito esperado, la probabilidad de detección de la infracción, entre otros[12].

59. Al respecto, en la Resolución Final N° 1283-2010/CPC de fecha 31 de mayo de 2010, la Comisión estableció la metodología a emplear a efectos de determinar la sanción final a imponer. En ese sentido, para graduar la sanción, debe considerarse lo siguiente[13]:

---

12 **LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de septiembre de 2010**
Artículo 112°.- Al graduar la sanción, el INDECOPI puede tener en consideración los siguientes criterios:
1. El beneficio ilícito esperado u obtenido por la realización de la infracción;
2. La probabilidad de detección de la infracción;
3. El daño resultante de la infracción;
4. Los efectos que se pudiesen ocasionar en el mercado;
5. La naturaleza del perjuicio causado o grado de afectación a la vida, salud, integridad o patrimonio de los consumidores;
6. Otros criterios que, dependiendo del caso particular, considere adecuado adoptar la Comisión.

13 Al respecto, la citada resolución señaló lo siguiente:
"El beneficio ilícito es el beneficio real o potencial producto de la infracción administrativa. Es lo que percibe, percibiría o pensaba percibir el administrado cometiendo la infracción menos lo que percibiría si no la hubiera cometido. Así, por ejemplo, si un proveedor hubiera percibido 100 unidades respetando la ley, pero percibe (o percibiría o cree que va a percibir) 150 unidades al cometer la infracción, el beneficio ilícito es de 50 unidades. El beneficio ilícito también es lo que el infractor ahorra, ahorraría o pensaba ahorrar, al cometer la infracción. El beneficio ilícito, resulta pertinente precisarlo, no es utilidad ni ganancia en sentido contable o financiero.

La probabilidad de detección, por su parte, es la posibilidad, medida en términos porcentuales, de que la comisión de una infracción sea detectada por la autoridad administrativa. Si una infracción es muy difícil de detectar, le corresponderá un porcentaje bajo de probabilidad, como sería 10%, lo que significa que de cada 10 infracciones, una sería detectada por la autoridad; mientras que si es de mediana o fácil detección le corresponderá un porcentaje mayor, como por ejemplo, 50% (si de cada 2 infracciones, una sería detectada por la autoridad), 75% (si de cada 4 infracciones, 3 serían detectadas) ó 100% (todas las infracciones serían detectadas).

En tanto la propia norma establece que la sanción debe ser disuasoria, el criterio del beneficio ilícito es especialmente importante, pues permite analizar cuál fue el beneficio esperado por el infractor que le llevó a cometer la conducta

Beneficio ilícito

60. En el presente caso, la Comisión no cuenta con información que le permita cuantificar dicho beneficio obtenido por el Banco al autorizar indebidamente la segunda transferencia que ascendió a S/ 2 150,00, así como tampoco cuenta con un parámetro objetivo que permita efectuar una presunción del beneficio obtenido por el infractor.

61. Por tal razón, la graduación de la sanción se estimará a partir de los otros criterios previstos en el artículo 112° del Código.

Daño resultante y naturaleza del perjuicio causado

62. En ese sentido, para la Comisión el factor determinante para graduar la multa en el presente caso es el daño resultante luego de verificarse la infracción, el cual debe asociarse necesariamente a la afectación a los intereses económicos de los consumidores. Resulta relevante señalar que en el caso analizado, el consumidor afectado, en su calidad de titular de la tarjeta de débito, ha visto afectado su patrimonio de forma indebida, toda vez que se autorizó indebidamente una (1) transferencia a la cuenta de un tercero por el importe de S/ 2 150,00, monto equivalente a 0,54 UIT

63. En consecuencia, corresponde revocar la Resolución Final N° 870-2015/PS2 que sancionó al Banco con una multa de dos (2) UIT y reformándola, sancionar al Banco con una multa de 0,54 UIT.

Sobre el pago de las costas y costos del procedimiento

64. En la medida que el Banco cuestionó el pago de las costas y costos del procedimiento, únicamente bajo el argumento de no haber cometido infracción alguna al Código, y habiéndose verificado su responsabilidad, corresponde confirmar la Resolución Final N° 870-2015/PS2 en dicho extremo.

---

sancionada pese a su prohibición. Este criterio está estrechamente vinculado a la expectativa de detección, que influirá decisivamente al hacer el análisis costo/beneficio al momento de cometer la infracción. Adicionalmente, se trata de factores todos ellos susceptibles de cierta objetivación, lo que permite una mayor claridad en la motivación de la sanción, facilitando su comprensión y posterior control, tanto en sede administrativa como en sede judicial.

Sin embargo, no debe olvidarse que en materia sancionadora no se castiga únicamente por el beneficio ilícito del infractor, sino también por el daño potencial o causado como consecuencia de la infracción. Por tanto, los criterios indicados en el párrafo anterior no son los únicos que deben tomarse en cuenta para establecer una sanción, que puede verse agravada o atenuada en aplicación del resto de criterios establecidos en la normativa vigente; esto es, los efectos sobre el mercado, la naturaleza del bien jurídico lesionado, la conducta del infractor y la reincidencia o incumplimiento reiterado, entre otros.

Además, debe resaltarse que en caso el beneficio ilícito sea difícil de cuantificar o no exista, la Comisión podrá considerar los demás criterios establecidos en el artículo 41°-A de la Ley de Protección al Consumidor con la finalidad de determinar la sanción que considere pertinente a cada caso concreto, aplicando además los agravantes y atenuantes que correspondan.

En consecuencia, la metodología empleada por esta Comisión parte de la determinación, siempre que sea posible, del beneficio ilícito esperado por el infractor, determinándose además la probabilidad de detección. A partir de estos criterios se determina lo que denominamos «multa base», lo que permite tener una base para la sanción, para cuya determinación final deberán aplicarse, cuando sea pertinente, los demás criterios establecidos en el artículo 41°-A de la Ley del Sistema de Protección al Consumidor, así como los que, supletoriamente, se encuentran establecidos en el numeral 3 del artículo 230° de la Ley del Procedimiento Administrativo General. Por su parte, en aquellos supuestos en donde sea imposible o muy difícil establecer el beneficio ilícito, los demás criterios serán igualmente aplicables, para así determinar la sanción a imponer".

RESUELVE

PRIMERO: revocar la Resolución Final N° 870-2015/PS2 del 25 de agosto de 2015, emitida por el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor N° 2, que declaró fundada la denuncia interpuesta por la señora [redacted] contra Banco de Crédito del Perú S.A. por infracción a los artículos 1° literal c), 18° y 19° del Código de Protección y Defensa del Consumidor, en el extremo referido a la transacción no reconocida por el monto de S/ 4 600,00; y, reformándola, declararla infundada, en tanto quedó acreditado que la entidad financiera cumplió con observar los mecanismos de seguridad respectivos para la realización de dicha transacción.

SEGUNDO: confirmar la Resolución Final N° 870-2015/PS2, en el extremo que declaró fundada la denuncia interpuesta por la señora Grit Marlen [redacted] contra Banco de Crédito del Perú S.A. por infracción a los artículos 1° literal c), 18° y 19° del Código de Protección y Defensa del Consumidor, en tanto la entidad financiera permitió indebidamente la realización de la operación de S/ 2 150,00.

TERCERO: revocar la Resolución Final N° 870-2015/PS2, en el extremo referido a la medida correctiva ordenada; y, reformándola, ordenar a Banco de Crédito del Perú S.A. que, en un plazo no mayor a cinco (5) días hábiles, contados a partir del día siguiente de notificada la presente resolución, cumpla con devolver a la señora Grit Marlen [redacted] el importe de S/ 2 150,00.

CUARTO: revocar la Resolución Final N° 870-2015/PS2, en el extremo que sancionó a Banco de Crédito del Perú S.A. con una multa de dos (2) UIT y reformándola, sancionarlo con una multa de 0,54 UIT.

QUINTO: confirmar la Resolución Final N° 870-2015/PS2, en el extremo que ordenó al Banco de Crédito del Perú S.A. el pago de las costas y costos del procedimiento.

SEXTO: confirmar la Resolución Final N° 870-2015/PS2 en el extremo que dispuso la inscripción de Banco de Crédito del Perú S.A. en el Registro de Infracciones y Sanciones del Indecopi, una vez que la resolución quede firme en sede administrativa, conforme a lo establecido en el artículo 119° de la Ley N° 29571, Código de Protección y Defensa del Consumidor.

SÉPTIMO: informar a las partes que la presente resolución tiene vigencia desde el día siguiente de su notificación y agota la vía administrativa, pudiendo ser cuestionada vía proceso contencioso administrativo ante el Poder Judicial. Asimismo, de conformidad con lo dispuesto por el artículo 125 de la Ley 29571, Código de Protección y Defensa del Consumidor[14], el

---

14 **LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de setiembre de 2010**
Artículo 125°.- Competencia de los órganos resolutivos de procedimientos sumarísimos de protección al consumidor
(...)
Excepcionalmente, hay lugar a recurso de revisión ante la Sala competente en materia de protección al consumidor del Tribunal del Indecopi, de conformidad con lo dispuesto en el artículo 210 de la Ley 27444, Ley del Procedimiento Administrativo General. Su finalidad es revisar si se han dejado de aplicar o aplicado erróneamente las normas del presente Código, o no se han respetado los precedentes de observancia obligatoria por ella aprobados. El plazo para formular este recurso es de cinco (5) días hábiles y su interposición no suspende la ejecución del acto impugnado, salvo que la Sala en resolución debidamente fundamentada disponga lo contrario.

único recurso impugnativo que —de manera excepcional[15]— puede interponerse para cuestionar solo situaciones de derecho contra lo dispuesto por este órgano colegiado es el de revisión. Cabe señalar que dicho recurso deberá ser presentado ante la Comisión en un plazo máximo de cinco (5) días hábiles contado a partir del día siguiente de su notificación, caso contrario la resolución quedará consentida[16].

Con la intervención de los señores Comisionados: Juan Carlos Zevillanos Garnica, Erika Claudia Bedoya Chirinos y Diego Vega Castro-Sayán.

JUAN CARLOS ZEVILLANOS GARNICA
Presidente

---

15 **TEXTO ÚNICO ORDENADO DE LA DIRECTIVA QUE APRUEBA EL PROCEDIMIENTO SUMARÍSIMO EN MATERIA DE PROTECCIÓN AL CONSUMIDOR PREVISTO EN EL CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, aprobado por RESOLUCIÓN N° 298-2013-INDECOPI/COD y publicado el 6 de diciembre de 2013**
V. APELACIÓN Y REVISIÓN
5.3. Recurso de Revisión
5.3.1. El recurso de revisión es de puro derecho, no cabe la adhesión ni la actuación de pruebas. Este recurso se presenta ante la Comisión correspondiente, la cual verificará el cumplimiento de los requisitos de admisibilidad, incluyendo la oportunidad del recurso.
5.3.2. La Sala competente en materia de Protección al Consumidor del Tribunal del INDECOPI evalúa la procedencia del recurso verificando si la pretensión del recurrente plantea la presunta inaplicación o la aplicación errónea de las normas del Código; o, la inobservancia de precedentes de observancia obligatoria; notificando a las partes dicha decisión. Si dicha Sala declara la procedencia del recurso, en el mismo acto, podrá disponer la suspensión de la ejecución de la resolución recurrida.
(...)

16 **LEY N° 27444, LEY DEL PROCEDIMIENTO ADMINISTRATIVO GENERAL, publicada el 11 de abril de 2001**
Artículo 212°.- Acto firme
Una vez vencidos los plazos para interponer los recursos administrativos se perderá el derecho a articularlos quedando firme el acto.

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Declaratoria de Autenticidad del Asesor

Yo, RODRIGUEZ FIGUEROA JOSE JORGE, docente de la ESCUELA DE POSGRADO MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis Completa titulada: "Fraude informático en los sistemas de seguridad financiero, distrito fiscal de Lima Centro 2022

", cuyo autor es ROSAS MARROQUI BRENDA LISSET, constato que la investigación tiene un índice de similitud de 20.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis Completa 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, 04 de Agosto del 2023

Apellidos y Nombres del Asesor:	**Firma**
RODRIGUEZ FIGUEROA JOSE JORGE **DNI:** 10729462 **ORCID:** 0000-0002-0265-9226	Firmado electrónicamente por: JRODRIGUEZFIG el 07-08-2023 13:11:02

Código documento Trilce: TRI - 0640652

INVESTIGA UCV