Universidad Norbert Wiener

Powered by Arizona State University

FACULTAD DE DERECHO Y CIENCIA POLÍTICA
ESCUELA ACADÉMICO PROFESIONAL DE DERECHO Y CIENCIA POLÍTICA

Trabajo de Suficiencia Profesional

"El delito de fraude informático frente al uso doloso de los datos personales, Lima 2023"

Para optar el Título Profesional de

Abogada

Presentado por:

Autora: Panty Marrufo, Tayrona

Código Orcid: 0000-0003-3264-5789

Asesora: Mg. Meza Torres, Yelena

Código Orcid: https://orcid.org/0000-0001-5293-9894

Línea de Investigación

Sociedad y transformación digital

Sub línea de Investigación

Derecho Civil, Penal y Administrativo

Lima-Perú

2023

Universidad Norbert Wiener	DECLARACIÓN JURADA DE AUTORIA Y DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN		
	CÓDIGO: UPNW-GRA-FOR-033	VERSIÓN: 01 REVISIÓN: 01	FECHA: 08/11/2022

Yo, TAYRONA PANTY MARRUFO egresado(a) de la Facultad de Derecho y Ciencia Política, declaro que el trabajo académico "El delito de fraude informático frente al uso doloso de los datos personales, Lima 2023" Asesorado por el docente: YELENA MEZA TORRES DNI: 44363804 ORCID: 0000-0001-5293-9894 tiene un índice de similitud de siete (7%) con código verificable OID: 14912:304471999 en el reporte de originalidad del software Turnitin.

Así mismo:

1. Se ha mencionado todas las fuentes utilizadas, identificando correctamente las citas textuales o paráfrasis provenientes de otras fuentes.
2. No he utilizado ninguna otra fuente distinta de aquella señalada en el trabajo.
3. Se autoriza que el trabajo puede ser revisado en búsqueda de plagios.
4. El porcentaje señalado es el mismo que arrojó al momento de indexar, grabar o hacer el depósito en el Turnitin de la universidad y,
5. Asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión en la información aportada, por lo cual nos sometemos a lo dispuesto en las normas del reglamento vigente de la universidad.

TAYRONA PANTY MARRUFO

DNI: 76683373

YELENA MEZA TORRES

DNI: 44363804

Índice

Índice de tablas

Pág.

Dedicatoria

Dedico este esfuerzo a Dios y familiares por apoyarme en todo momento y docentes que contribuyeron con mi formación.

Agradecimiento

A Dios, por darme la fortaleza en este trayecto de mi día a día en mis estudios.

Agradezco al director de investigación el Dr. Jaime Sánchez y a mi asesor del curso.

Agradezco mi familia por las suficientes palabras de apoyo, comprensión y empatía que han tenido hacia mi persona en el trayecto de la carrera.

Agradezco a cada uno de los profesores que cultivaron sus aportes en mí.

“El delito de fraude informático frente al uso doloso de los datos personales, Lima 2023”

“The crime of computer fraud versus the malicious use of personal data, Lima 2023”

Línea de Investigación: Sociedad y transformación digital
Sub Línea de Investigación: Derecho Civil, Penal, Administrativo
Autor: Panty Marrufo,Tayrona
email :a2020103549@uwiener.edu.pe
Orcid : 0000-0003-3264-5789
Facultad Derecho y Ciencias Políticas
Universidad Norbert Wiener

Resumen

Introducción, desde la perspectiva actual, el uso de la tecnología ha ido evolucionando y con ello implementando mejoras que permitan optimizar los servicios públicos y privados. Sin embargo, este tipo de avances ha generado una inseguridad y desprotección en la identidad de los usuarios, convirtiéndose en una nueva forma de impulsar la criminalidad. El **objetivo** de estudio es determinar cómo impacta el delito de fraude informático frente al uso doloso de los datos personales, Lima 2023. La **metodología** desarrollada es de enfoque cualitativo, paradigma naturalista, investigación tipo básica, diseño no experimental - estudio de caso, nivel de la investigación exploratorio, por medio del método inductivo, a través de análisis documentario. Como **resultado** se encontró que la transferencia no autorizada de fondos afecta directamente al patrimonio del agraviado, además de halló que la confianza en las transacciones digitales y la seguridad de la información se ven comprometidas. **Conclusión**, se determinó que el delito de fraude informático impacta frente al uso doloso de los datos personales, Lima 2023, ya que se ha podido observar del expediente analizado que hubo una vulneración de datos personales respecto a la inseguridad originada en la entidad bancaria.

Palabras clave: Cibercrimen, ley, seguridad de los datos, identidad y hackers.

Abstract

Introduction, from today's perspective, the use of technology has been evolving and with it implementing improvements that allow the optimization of public and private services. However, this type of advance has generated insecurity and lack of protection in the identity of users, becoming a new way of promoting criminality. The **objective** of the study is to determine how the crime of computer fraud impacts the fraudulent use of personal data, Lima 2023. The **methodology** developed is a qualitative approach, naturalistic paradigm, basic type research, non-experimental design - case study, exploratory research level, through the inductive method, through documentary analysis. As **a result**, it was found that the unauthorized transfer of funds directly affects the assets of the aggrieved party, in addition to finding that trust in digital transactions and information security are compromised. **Conclusion**, it was determined that the crime of computer fraud impacts against the fraudulent use of personal data, Lima 2023, since it has been observed from the analyzed file that there was a breach of personal data regarding the insecurity originated in the bank.

Keywords: Cybercrime, law, data security, identity and hackers

I.- Introducción

En el transcurso del tiempo la tecnología ha ido evolucionando, trayendo consigo ventajas y desventajas, siendo una de ellas los delitos informáticos (fraude informático) el cual se encuentra vinculado al uso doloso de los datos personales. Tal es así que, en países de primer mundo como Italia, el autor Fusco (2020) abordó una cuestión de derecho comparado de gran importancia en donde actualmente el crimen informático revela ciertos problemas dentro del uso de la tecnología en el mundo, trayendo consigo el aumento de los delitos cibernéticos en el país, afectando a los usuarios o ciudadanos a diario.

Asimismo, en España el autor Gamón (2017) manifiesta que los conflictos que aborda al ciberdelito es la carencia de la identificación de los datos o lugares donde roban la información de las personas, siendo dificultoso a grandes escalas poder encontrar a los actores delictivos, por lo que los usuarios sufren la vulneración de sus datos en el ciberespacio.

Por otro lado, en Portugal, los investigadores Correia y Da Silva (2018) explicaron que el país presenta problemas en ciberseguridad, en consecuencia, las entidades a cargo, en aras de buscar proteger a su población de estos casos frecuentes tiene como fin proteger los datos y privacidad del individuo por medio de la seguridad digital. Así también en Estados Unidos, el autor Koto (2021) indicó que los problemas que viene enfrentando la tecnología incide en el comportamiento social, el cual es vulnerado por delincuentes que vienen transformando el uso de las distintas redes en materia cultural, política y jurídica, lo cual trae consigo consecuencias negativas para quienes no dominan estos espacios.

Continuando con países latinoamericanos, en México, los especialistas Casillas y Ehrenzweig (2023) describen que otro gran problema en el uso de la tecnología digital lo trajo la pandemia, pues al estar en confinamiento se tuvo que recurrir a la tendencia del uso de redes o plataformas para no salir del hogar, generándose robos, fraudes informáticos y acoso digital en los datos vulnerados de los usuarios afectados. Por otro lado, en Brasil, el autor Cruz (2017) analizó que las redes en su ambiente de gobernanza como el internet deben también garantizar la ciberseguridad a los países para asegurar la estabilidad económica y datos de las personas en el peligro existente del robo de su información.

De la misma manera en Chile, los autores Mayer y Oliver (2020) examinaron el problema existente en el fraude informático, como delitos cibernéticos, los cuales tienen alcance y conexión con otras organizaciones criminales delimitadas a robar información de los usuarios en un determinado espacio. Asimismo, en Ecuador, el investigador Campos (2019) nos relata que los programas maliciosos, cuando se infiltran en los servicios de internet se vuelven

peligrosos y destruyen silenciosamente no solo los equipos técnicos, sino también las finanzas personales, corporativas y nacionales.

Finalmente, en Perú Vereau (2021) precisa que uno de los problemas es la actividad delictiva cometida por sistemas informáticos, lo que trajo consigo la regulación de la Ley 30096, Ley de delitos informáticos modificada por la Ley 30171.

En consecuencia, actualmente en el Perú existe un alto índice de comisión del delito de fraude informático, debido a que no existe una protección idónea de los datos personales por parte de las entidades bancarias. Por consiguiente, se ha planteado como problema general de este estudio: ¿Cómo impacta el delito de fraude informático frente al uso doloso de los datos personales? y, como problemas específicos. (Ver Anexo I)

Además, como diagnóstico de esta investigación, podemos expresar que en la sociedad actual convivimos con los delincuentes cibernéticos, quienes utilizan diversas técnicas, siendo las más frecuentes el phishing y el carding, debido a que los sistemas de las entidades bancarias son vulnerados a fin de obtener acceso a información vulnerable de las personas. Al respecto, Bencomo et al. (2019) señala que un diagnóstico se aborda en neutralizar y evidenciar un problema existente e interpretar la información más resaltante de la situación o hecho identificado.

Asimismo, el presente estudio cuenta con una justificación teórica, la cual se define por el autor Álvarez (2020), quien señala que dicha justificación implica describir, profundizar y estudiar un conocimiento existente para crear nuevas perspectivas legales. Es así que el presente estudio busca utilizar la tecnología para prevenir el fraude cibernético. Por otro lado, los autores Deroncele et al. (2021) precisan que la justificación práctica es una aplicación de un hecho o evento a desarrollar como un aporte a futuro. En consecuencia, este estudio busca proteger las identidades de las personas, aplicando medidas de seguridad en el campo de la digital.

En el mismo orden de ideas, la justificación metodológica, segun Azuero (2019) está orientada a preparar a los investigadores para presentar una investigación introduciéndolos en el campo de estudio cumpliendo los parámetros metodológicos. Por ende, este trabajo de investigación busca aportar nuevos conocimientos a otros indagadores. En ese sentido, se tiene como objetivo general determinar cómo impacta el delito de fraude informático frente al uso doloso de los datos personales; y, como objetivos específicos. (Ver Anexo I)

II.- Presentación del caso Jurídico

2.1.- Antecedentes

En primer lugar, se abordaron los antecedentes internacionales, tal es así que en Ecuador Prieto y Vargas (2020) realizaron un trabajo para lograr el título de profesional en derecho, en el cual tuvieron como objetivo determinar si existen falencias en el sistema de verificación del perfil del ciberdelincuente en los medios electrónicos, en sus resultados se evidenció que existe una vulneración a romper con los parámetros de la intimidad personal de un individuo mediante la extorción por parte de los ciberdelincuentes en el país, concluyendo que es necesario optimizar las herramientas empleadas para luchar contra este tipo de casos surgidos en los medios tecnológicos y debe proyectarse una protección a los usuarios en línea mediante la protección de datos por parte del Estado hacia los ciudadanos.

En Colombia, Villa y Acuña (2018) realizaron una investigación en donde determinaron las fallas que existen en la normativa colombiana referente a los delitos informático y el impacto que ha venido teniendo la ciberdelincuencia en las empresas, demostrando que existe una inseguridad en los delitos informáticos en el país sobre el fortalecimiento de las instituciones, concluyendo que es necesario implementar medidas de solución para prevenir la ciberdelincuencia adoptando protocolos de seguridad digital a los usuarios.

Respecto con los antecedentes nacionales, en Lima, Monja (2022) realizó un trabajo para optar el título de abogado, teniendo como objetivo determinar el aumento de los delitos informáticos en las entidades bancarias, demostrando que existe perjuicios económicos para los usuarios respecto a los casos de suplantación de identidad, de esta manera concluyó que busca poder informar sobre las distintas modalidades que existe en la modalidad de estafa en la sociedad.

Además, en Lima Este, los autores Berrio y Orellana (2022) realizaron un artículo sobre el daño de la información digital no autorizado a causa del almacenamiento de información personal y financiera de las plataformas en línea. En sus resultados evidenciaron que el intercambio ilegal de información digital pone en riesgo a los usuarios, ya que puede resultar un fraude contra bancos, activos y personas en redes. Llegaron a la conclusión que es necesario contar con el uso de software legal para proteger de personas inescrupulosas los secretos bancarios y destruir información personal y documentos bancarios falsos en el comercio ilegal de información digital, dañando intereses individuales, propiedades y datos financieros en plataformas de internet.

2.2.- Fundamento del tema elegido

En relación a la primera categoría denominada delito informático, el autor Bramont-Arias

(1997) indicó que son comportamientos complicados de categorizar o agrupar en una sola definición. En general, el delito informático se puede definir como aquella persona que utiliza un sistema de procesamiento de datos, se expande en sus características las modalidades del phishing y carding. Aunado a ello, el autor Terreros (2014) indicó que se refiere a las conductas que persiguen la manipulación de los sistemas de seguridad, tales como la invasión de computadoras, correos o sistemas de información. Asimismo, los autores Ballesteros & Hernández (2014) mencionaron que comprenden cualquier irregularidad, ya sea un delito o falta, en la que se involucra un equipo informático en general, puede ser utilizada para comisión del delito o puede ser objeto de la misma responsabilidad.

Como subcategoría 1 se tiene el phishing, el cual según los autores Delgado et al. (2022) se trata de un delito que se originó en el ciberespacio, el cual se fundamenta en el engaño, en la captación de un usuario para obtener su información personal. Asimismo, Martínez et al. (2021) define como un método para obtener información de una persona, se utiliza para robar información de otros usuarios y ganar dinero. Esto se debe a que los hackers vulneran sistemas de seguridad en una plataforma o espacio digital donde hay personas vulnerables. En esa misma línea, el autor García (2018) señala que se ha examinado con atención durante los últimos años, como la conducta delictiva en la que se manipulan datos personales de forma manipuladora, asimismo es difícil identificar a estos individuos delictivos dentro de un ciberespacio en el que la información es manipulada de forma inadecuada para inducir a la manipulación de datos personales para inducir al engaño a los usuarios más vulnerables de poder llegar a obtener su información personal.

Como subcategoría 2 se consideró el carding, al respecto los autores Ospina y Sanabria (2020) consideran que se da cuando se vende o utilizan ilícitamente los datos personales. Esto puede causar pérdidas de información, datos personales y difusión de la información en tecnología o ciberespacio. En consecuencia, para el autor Vélez (2017), se trata de la copia de la información de las tarjetas de crédito de un individuo para crear un delito informático, afectando la intimidad y seguridad digital del usuario, en el cual dichos datos son utilizados para explotar económicamente en el sitio web, otorgando una ineludible disposición de la información de otra persona sin su autorización, y además, a otros individuos delictivos para evitar el tráfico de información robada. Del mismo modo, los autores Rosas-Lanas y Pila-Cárdenas (2023), indican que con el fin de lograr tal objetivo, el individuo adquiere la información de la tarjeta de datos personales, posteriormente los emplea en diversas transacciones, generando una forma de estafa.

En cuanto a la segunda categoría denominada datos personales, la autora Liébana (2023)

define en su libro que los derechos fundamentales se asocian en la esfera legal para resguardar y hacer prevalecer la seguridad y privacidad personal de las personas, desprendiendo los siguientes elementos como: la intimidad, imagen, identidad y la protección de datos personales. Seguido a ello, el autor Ortiz (2002) conceptualiza los derechos fundamentales como inherentes a cada individuo adscritos en lo mencionado líneas anteriores como aspectos característicos de estos derechos, respecto a valores que implica como objeto la tutela de estos derechos. En esa misma línea, el autor Sánchez (2017) ha definido que los derechos fundamentales son un paradigma que han ido trascendiendo conforme al avance tecnológico sujetos de derecho a una protección para las personas.

Como subcategoría 1 se propuso la intimidad, al respecto la autora Yanqui (2020) indicó en el mundo es jurídicamente un derecho legal sujeto a protección impartidos, en donde la persona debe recibir un cuidado y respeto sobre la información que íntimamente desea compartir. Asimismo, Carvajal y Estrada (2020) refieren que la intimidad se describe como un derecho enmarcado dentro de la esfera del encuadre constitucional aunado a un derecho fundamental, regulado y protegido por la norma y el Estado sobre el uso o tratamiento de datos o información. En ese orden de ideas, el autor Álvarez (2017) precisó que la intimidad forma parte relevante del ámbito personal la cual se mantiene en reserva una persona, siendo sujeto de protección por el derecho fundamental y adscrito al derecho a la intimidad, que recaen sobre un individuo.

Como subcategoría 2 se identificó la identidad, definido por el autor Maqueo (2017) como “una característica personal y parte del derecho fundamental autónomo de toda persona en relación a su vida privada de todo ser humano por su género o rasgos que lo identifican como una persona, protegidos por el derecho”. Además, según Arvelo (2022) nace del ser humano como aquellas características propias que lo diferencian de otro sujeto por sus rasgos o facciones genéticas que lo identifican como tal, siendo protegidas por el derecho fundamental en la constitución de cada Estado. Asimismo, Mendoza (2021) lo define como el reconocimiento de la persona o esencia que los caracteriza como un ser humano sobre la imagen que tiene los cuales son protegidos por el derecho que configuran la existencia identificable de esa persona.

Como subcategoría 3 se ha definido los datos personales, que de acuerdo con el autor Martínez (2022) es personalísimo, de acceso y toma decisión de la persona para proteger su información en la recolección, procesamiento, archivo, difusión o distribución de estos con la autorización del titular o la ley autoritativa respectiva. Asimismo, Guerrero (2022) lo describe como un derecho natural-individual, materialmente protegido que está siendo

vulnerado en relación a la información difundida sobre el individuo ante la autorización de su información personal. De esta forma, Tuesta (2022) indicó que se resalta en los sujetos determinados, los cuales deben ser resguardados a través de dispositivos tecnológicos en donde sus informaciones deben de asegurar la protección de sus datos.

2.3.- Aporte y desarrollo de la experiencia

Se ha empleado el enfoque cualitativo, basado en un estudio que se centra en explicaciones detalladas de los fenómenos, con el objetivo de comprenderlos metodológicamente de carácter epistemológico como la hermenéutica y otros asociados a la investigación (Sánchez, 2019). Asimismo, el método utilizado fue el inductivo, el cual se obtiene dentro del proceso de exploración teórico para abordar la realidad de un hecho el cual requiere ser estudiado por el investigador para conocer e identificar los posibles hallazgos que permitirán llegar a conclusiones (Urzola, 2020).

Además, el diseño fue no experimental, ya que según los autores Polanía et al. (2020) se basa en la no manipulación de los datos. Del mismo modo, se empleó el diseño de estudio de caso, puesto que se centra en indagar o profundizar sobre un hecho y tener en cuenta las fuentes, para ser interpretadas por el investigador en un determinado hecho identificado (Becerra, 2020). Aunado a ello, los autores Chaves y Weiler (2016) indicaron que en los estudios cualitativos se adaptan más al estudio de caso.

En cuanto al nivel de investigación se optó que sea exploratorio, toda vez que se han llevado a cabo investigaciones de tipo fenomenológico o narrativo constructivista que intentan explicar las representaciones subjetivas sobre un fenómeno específico en un grupo de personas (Ramos-Galarza, 2020).

Por otro lado, la investigación fue de tipo básica, debido a que busca adquirir nuevos conocimientos de manera organizada, con la finalidad de aumentar la comprensión de una situación específica (Álvarez, 2020). Asimismo, se ha utilizado la técnica de análisis documentario, entendida como un procedimiento de análisis de fuente o documentos, de donde se extrajeron ideas relevantes para abordar un estudio, igualmente para representación de este análisis se deriva de un archivo utilizando un conjunto de palabras (Liniers, 2009).

En relación con el instrumento de ficha documentaria, se introduce diferentes técnicas y herramientas basadas en cada ocupación, para que los estudiantes tengan una guía que les ayude a tomar las decisiones correctas para sus métodos y herramientas de medición. (Arias, 2020).

De acuerdo con la postura de los autores Schmalbach et al. (2010), se entiende que se inicia con un concepto teórico acerca del escenario y el campo donde se desarrolló la investigación. Por lo cual el escenario de estudio fue Lima.

En el Expediente 01539 – 2021 de Lima norte, de fecha fecha del 19 de octubre del 2020, mediante la denuncia interpuesta por el agraviado aprendí que la calificación del delito es de gran relevancia debido a la frecuencia que se viene suscitando este tipo de hecho en donde se vulnera la protección de los datos personales. Aunado a ello, a través del fiscal a cargo de la carpeta fiscal se ejecutó como medida las nuevas aplicaciones penales, en donde se apertura el proceso de delito contra el patrimonio – fraude informático.

Por consiguiente, al haberse recabado todos los elementos relevantes para acreditar la tipificación de la sanción punitiva, cometida por las partes ante el agraviado, así como también del acta donde intervinieron a la sentenciada el 20 de octubre de 2020, la entidad de la PNP la cual constato los datos obtenidos para poder esclarecer el caso y emitir el cargo hacia la fiscalía para que inicie las investigaciones preliminares.

Con fecha 20 de octubre del 2020, a la detenida se le realizó un acta de intervención donde en la misma vinculó a otra persona que indicó que era su primo que le había pedido el favor que vaya a cobrar una transacción; sin embargo, la fiscalía consideró que su manifestación fue contradictoria a la pericia de análisis digital que se realizó, en el cual se les implicaban a ambos en el delito cometido dando a lugar a la siguiente etapa intermedia.

Finalmente, en la audiencia de juicio oral de fecha 15/03/2023, los imputados solicitaron la conclusión anticipada, la misma que fue estimada por la fiscalía, se estableció que los imputados conjeturaron el “delito contra el patrimonio recaído en el fraude informático”, tipificándose para ambos la sentencia respectiva de pena privativa de su libertad de carácter suspendida en su ejecución por el periodo de prueba de 3 años bajo determinadas reglas de para dar cumplimiento, la pena de sesenta días multa equivalente a S/465.00 soles que deberá de pagar cada sentenciado, además la reparación de S/2,000.00 soles que debieron de pagar de forma solidaria y la devolución de del dinero sustraído de S/24,000.00 soles.

Se mejoró el conocimiento sobre las medidas de prevención y las consecuencias legales contra los infractores, se abordaron temas relacionados con las técnicas y herramientas utilizadas por los delincuentes cibernéticos, con el objetivo de saber sobre los riesgos y las formas de protegerse. Así como también, se aprendió sobre el uso de las fuentes relevantes para el estudio y el análisis exhaustivo del expediente respecto a la materia del caso señalado.

Tabla I.

Matirz de categorización apriorística

Problema General	Problemas Específicos	Objetivo General	Objetivos Específicos	Categorías	Subcategorías	Metodología
¿Cómo impacta el delito de fraude informático frente al uso doloso de los datos personales, Lima 2023?	¿Cómo impacta las modalidades del phishing y carding frente al delito de fraude informático, Lima 2023? ¿ Cómo impacta la protección de datos frente al uso doloso de los datos personales, Lima 2023?	Determinar cómo impacta el delito de fraude informático frente al uso doloso de los datos personales, Lima 2023	Determinar cómo impacta las modalidades de phishing y carding frente al delito de fraude informatico, Lima 2023. Determinar cómo impacta la protección de datos frente al uso doloso de los datos personales, Lima 2023.	Delito informatico	Phishing Carding	**Enfoque**: Cualitativo **Método:** Inductivo **Diseño**: No experimental – Estudios de caso **Nivel:** Exploratorio **Tipo de investigación**: Básica
				Los datos personales	Protección de datos	**Técnica:** Análisis Documentario **Instrumento:** Ficha Documentaria **Escenario de estudio:** Ciudad de lima

2.4.- Presentación del reporte de caso jurídico

En relación a los eventos y circunstancias ocurridos en el caso en cuestión, se dispone de la Carpeta Fiscal Nº 606014506 - 2020 – 696 – 0 de Lima Norte. El 19 de octubre de 2020, a las 11:15 horas, la parte afectada se encontraba en su residencia cuando recibió una llamada telefónica en su número celular. El individuo que llamó se identificó como representante de una entidad bancaria, manifestó a la afectada que se le había otorgado un beneficio en relación con un reclamo previo.

En el transcurso de la conversación, el interlocutor solicitó a la parte afectada que confirmara sus datos y procediera a actualizar su token digital. Al proporcionarle su token digital, el sujeto le informó a la afectada que dicho código era necesario para actualizar el sistema y los datos personales. Además, le aseguró que la información proporcionada sería utilizada para efectuar la devolución de dinero correspondiente al reclamo realizado previamente. Posteriormente, el sujeto concluyó la llamada; dicha persona no identificada ingresó a la cuenta del banco del agraviado y realizó la transacción en la cuenta de la imputada 1 por el monto de S/. 24,000 a horas 11:22 del día 19 de octubre de 2020 para posteriormente retirar el dinero que su primo le había dicho que lo haga, así como entregar el dinero a dicha persona. Por otro lado, el agraviado recibió un mensaje del banco consistente en una constancia de transferencia por el monto de S/. 24,000 que fue realizado

de su cuenta de ahorro a la cuenta de la imputada por lo que al no reconocer la transferencia llamó a banca por teléfono pidiendo que congelen esa transferencia más no logró anular dicha transferencia, es así como el agraviado acudió a denunciar los hechos a la comisaria Sol de Oro indicando lo acontecido.

El 20 de octubre de 2020, ante la evidencia de la flagrancia delictiva, el personal policial intervino a la investigada en el asentamiento humano registrado en su ficha de Reniec, según el acta previamente mencionada. Tras recorridos para localizarla, se logró identificar su residencia y se procedió a su detención. Asimismo, durante el interrogatorio, la investigada admitió haber retirado el dinero, señalando que fue su primo quien le encomendó la tarea y a quien le entregó la suma retirada, estableciendo así su vinculación con la planificación y ejecución del retiro de fondos.

El 22 de diciembre de 2022, en respuesta al requerimiento de control de acusación, se dictaminó que el imputado 1 sería considerado como presunto autor, mientras que la imputada 2 sería catalogada como presunta cómplice primaria. En el auto de enjuiciamiento, se estableció la relación entre ambas partes del proceso, indicando que el caso seguía adelante contra ambos imputados. Además, se declaró que el proceso continuaría, pasando a la fase de juicio oral.

Durante el juicio oral del 15 de marzo de 2023, los imputados optaron por la conclusión anticipada, resultando en la condena del imputado 1 como autor y de la imputada 2 como cómplice primario, ambos por el delito de fraude informático contra el patrimonio. La sentencia incluyó la restricción de libertad, ajustada por principios de proporcionalidad, racionalidad, lesividad y humanidad de las penas, junto con una reducción del 1/7 por la conclusión anticipada. A la imputada 2 se le impuso la sanción correspondiente, y ambos condenados deben cumplir con las reglas de conducta establecidas. Además, se les ordenó efectuar el pago de la reparación acordada y la devolución del dinero sustraído a la parte agraviada, configurando así las repercusiones legales y las medidas de compensación que deben cumplir.

III Resultados

Como resultado de nuestra investigación procedemos a presentar y explicar cada resultado en función a las categorías y subcategorías. Asimismo, se dará inicio con el cuadro respectivo donde se abordan los objetivos del presente estudio.

Objetivo general	Determinar cómo impacta el delito de fraude informático frente al uso doloso de los datos personales, Lima 2023
Categoría 1	**Delito informático**
Categoría 2	**Datos personales**

El caso de fraude informático descrito y analizado mediante el Expediente Nº 01539-2021-8-0901-JR-PE-08 revela la vulnerabilidad de los datos personales en el entorno digital, ya que la manipulación del estafador, que se hizo pasar por un trabajador bancario, resaltó cómo la entrega del token digital y otros datos por parte del agraviado se conviertió en la víctima clave para un acceso no autorizado a su cuenta bancaria.

Además, del caso previsto se ha podido identificar que la estafa se ejecuta persuadiendo al agraviado de que está participando en un reclamo legítimo; asimismo, en dicho expediente se señaló una posible implicación de la entidad bancaria en el fraude, debido a que la llamada se realizó por parte de un supuesto trabajador. Finalmente, el impacto financiero del fraude informático es evidente, ya que la transferencia no autorizada de fondos afectó directamente al patrimonio del agraviado, es más la confianza en las transacciones digitales y la seguridad de la información se ven comprometidas en Lima, 2023.

Categoría N°1	**Delito informático**
Objetivo específico 1	Determinar cómo impacta las modalidades de phishing y carding frente al uso doloso de los datos personales, Lima 2023.
Subcategoría 1	**Phishing y carding**

El caso analizado mediante el Expediente Nº 01539-2021-8-0901-JR-PE-08 se logró identificar la influencia de modalidades específicas, como el phishing y el carding en el uso doloso de los datos personales, generando un impacto considerable en Lima durante el año 2023. En primer lugar, el agraviado de iniciales J.C.C. fue inducido al engaño a través de un medio electrónico, lo que sugiere la utilización del phishing, en este contexto, se llevó a cabo una transferencia bancaria a la cuenta de la imputada, la constancia de transferencia, remitida al correo electrónico del agraviado mediante una notificación de aviso de la entidad bancaria, actuó como evidencia de este engaño electrónico.

Por otro lado, se encontró que la utilización de carding mediante la obtención de datos de tarjetas bancarias, la visualización del acta de llamada telefónica entrante y saliente en el teléfono celular de la acusada 1 reveló información almacenada, incluyendo el número del primo. Este último era contactado constantemente por una tercera persona, quien indagaba sobre la posesión de tarjetas bancarias, además la implicancia del acusado 1 de inciales C.J.P.D en la transferencia de fondos y retiros, junto con la complicidad de la acusada 2 de iniciales G.D.L.C.H en la retirada de efectivo, refuerza la conexión con técnicas de carding para obtener ganancias ilícitas.

En consecuencia, el impacto de estas modalidades son evidentes en la pérdida económica del agraviado y en la ejecución exitosa de transacciones fraudulentas; además, la relación entre el phishing y el carding resalta la complejidad y sofisticación de estos delitos, poniendo de manifiesto la necesidad de una mayor conciencia pública sobre las amenazas cibernéticas y de medidas de seguridad más rigurosas por parte de las instituciones financieras.

Categoría N°2	**Datos personales**
Objetivo específico 2	Determinar cómo impacta la protección de datos frente al uso doloso de los datos personales, Lima 2023.
Subcategoría 1	**Protección de datos**

El caso analizado en el Expediente Nº 01539-2021-8-0901-JR-PE-08 proporcionó información relevante sobre la respuesta del agraviado, la intervención policial, y evidencia digital obtenida a través de un análisis forense del celular de la acusada. En ese sentido, se puede resaltar la vulnerabilidad de los datos personales del agraviado de iniciales J.C.C., que fueron utilizados para llevar a cabo transacciones fraudulentas. La notificación por correo electrónico y la carta del banco, junto con la constancia de transferencia, evidencian cómo los datos fueron comprometidos, impactando directamente la privacidad y seguridad financiera del denunciante.

Además, la incapacidad del agraviado para anular la transferencia resalta las limitaciones en los procedimientos de seguridad y la necesidad de implementar medidas más efectivas para prevenir y abordar rápidamente actividades fraudulentas. No obstante, la denuncia oportuna del agraviado y la intervención policial demuestran la importancia de

la colaboración entre individuos afectados y las autoridades para mitigar el impacto de estos delitos.

En cuanto a la participación de la imputada 2 de iniciales G.D.L.C.H, que proporcionó su cuenta para el depósito dinerario, y la declaración del acusado 1 de iniciales C.J.P.D, revelando su conocimiento y colaboración en el hecho ilícito, destaca la importancia de la responsabilidad individual en la protección de datos. La información obtenida a través del análisis digital forense refuerza la necesidad de investigaciones exhaustivas para rastrear la participación y conocimiento de los involucrados en el uso doloso de datos personales.

Por lo tanto, el caso evidencia cómo la falta de protección de datos personales puede conducir a delitos financieros y cómo la colaboración de terceros puede facilitar estas acciones ilícitas. La respuesta legal y policial, junto con medidas más sólidas de protección de datos, son esenciales para contrarrestar estos impactos en Lima en 2023.

IV.- Discusión

En relación con el objetivo general, la posición teórica de Bramont-Arias (1997), enrelación a la categoría 1, es que el delito de fraude informático es el uso de la tecnología que ha permitido realizar actividades y situaciones prohibidas, es más que un producto del continuo y creciente proceso de informatización; al igual que la teoría del derecho fundamental de Liébana (2023) que sustenta la categoría 2 al mencionar que la protección de datos personales que forman parte de la esfera que el derecho debe proteger en el marco de la privacidad de toda persona; y que además se relaciona y sustenta en diverso autores como Ortiz (2002) y Sánchez (2017). Eso se evidencia en el caso analizado, ya que se determinó que el fraude informático tuvo un claro impacto económico, ya que la transferencia de fondos no autorizada afectó directamente al patrimonio de la víctima vulnerando sus derecho a la protección de datos personales. También se evidenció que la confianza en las transacciones digitales y la seguridad de la información se vieron comprometidas, por lo que se debe de aludir que la posición de los autores ratifica el objetivo general de la presente investigación.

En función al primer objetivo específico, la posición teórica de los autores Delgado et al. (2022) que sustenta la primera subcategoría, expresa que el *phishing* se considera como el ciberdelito que engaña a los usuarios para que obtengan información personal. Por otro lado, la posición teórica de Ospina y Sanabria (2020), que respalda la segunda subcategoría, manifiesta que el *carding* es el método mediante el cual se busca

mercantilizar el uso o el tratamiento indebido de los datos personales que lo obtienen ilícitamente, esto se puede ver en forma de fraude por parte de delincuentes que roban números de tarjetas e información personal y los utilizan para diversas transacciones; al igual que la teoría de Liébana (2023) que sustenta la categoría 2 al aludir que los derechos fundamentales se agrupan en el ámbito legal con el propósito de salvaguardar y preservar la seguridad y privacidad individual. Estos derechos engloban aspectos como la intimidad, la imagen, la identidad y la protección de datos personales; y que además se relaciona y sustenta en diversos autores como Ortiz (2002), Sánchez (2017), Yanqui (2020), Carvajal y Estrada (2020), Álvarez (2017), Maqueo (2017), Arevalo (2022) y Mendoza (2021).

Esto se evidenció en el caso analizado, ya que estas formas de fraude tienen un impacto claro en las finanzas del agraviado, resultando en pérdidas económicas y en la realización efectiva de transacciones fraudulentas, así la conexión entre el phishing y el carding destaca la sofisticación y complejidad de estos delitos, enfatizando la necesidad de concientizar al público sobre las amenazas cibernéticas y de que las instituciones financieras refuercen sus medidas de seguridad. La combinación de estas técnicas subraya la importancia de abordar de manera integral el uso malicioso de datos personales, no solo centrándose en el engaño electrónico, sino también considerando la obtención ilícita de información financiera mediante métodos como el carding, en efecto se debe de precisar que la posición de los autores ratifica el objetivo específico 1 de la presente investigación.

Respecto al segundo objetivo específico, la posición teórica de Martínez (2022) que sustenta la subcategoría 3, al expresar que la protección de datos personales, incluido el acceso y las decisiones sobre la información y los datos, así como la correspondiente protección, recopilación, transmisión, procesamiento, distribución o difusión de estos datos e información requiere el consentimiento del propietario o autorización legal; al igual que la teoría Liébana (2023) que sustenta la categoría 2, al indicar que los derechos fundamentales se agrupan en el ámbito legal con el propósito de proteger y asegurar la seguridad y privacidad individual. Estos derechos comprenden aspectos como la intimidad, la imagen, la identidad y la salvaguarda de los datos personales; y que, además, se relaciona y sustenta en diversos autores como Guerrero (2022), Tuesta (2022), Ortiz (2002) y Sánchez (2017). Esto se evidencia en el caso analizado, puesto que la revelación a través de correos electrónicos y cartas del banco, respaldada por la constancia de transferencia, deja claro cómo se vieron comprometidos los datos, afectando directamente la privacidad y estabilidad financiera del denunciante, en ese sentido, la postura de los autores ratifica el objetivo específico 2.

V.- Conclusiones

Primera. Se determinó que el delito de fraude informático impacta frente al uso doloso de los datos personales, Lima 2023, ya que se ha podido observar del expediente analizado que hubo una vulneración de datos personales respecto a la inseguridad originada en la entidad bancaria. Respaldado por la posición teórica de Bramont-Arias (1997), quien señaló que la delincuencia informática se refiere a la actividad de personas que utilizan sistemas de procesamiento de datos, ampliándose para incluir modalidades como el phishing y el carding.

Segunda. Se determinó del primer objetivo específico que las modalidades de phishing y carding impactan frente al uso doloso de los datos personales, Lima 2023, porque se ha evidenciado la ejecución exitosa de transacciones fraudulentas que han perjudicado el patrimonio del agraviado. Basado en la posición teórica de Delgado et al (2022) y Ospina y Sanabria (2020), quienes indicaron que el *phishing* se configura como un ciberdelito que engaña a los usuarios para obtener información personal, y el *carding* consiste en buscar la mercantilización del uso o tratamiento indebido de datos personales adquiridos ilícitamente para utilizarlos en diversas transacciones, respectivamente.

Tercera. Se determinó que la protección de datos impacta frente al uso doloso de los datos personales, Lima 2023, puesto que en se ha identificado que la notificación por correo electrónico y la carta del banco, junto con la constancia de transferencia, evidencian cómo los datos fueron comprometidos, impactando directamente la privacidad y seguridad financiera del agraviado. Respaldado por la posición teórica de Martínez (2022) al indicar que la información personal es extremadamente privada y su acceso y manejo dependen de la decisión de la persona, quien tiene el poder de resguardar sus datos durante su recolección, procesamiento, almacenamiento, divulgación o distribución.

Cuarta. Finalmente, es importante destacar las limitaciones encontradas en la búsqueda de diversas fuentes identificadas en este estudio, lo que impidió consolidar las subcategorías relacionadas con el derecho a la intimidad, identidad e imagen. Se recomienda que este tema continúe siendo explorado para profundizar en otras ideas, ya que involucra a la sociedad como sujeto de protección por parte del Estado e instituciones. Para garantizar un control social sobre los datos personales, se sugiere implementar medidas como el reconocimiento facial, la identificación dactilar de huellas y la adecuación jurídica al marco legal peruano de la prueba digital, esto contribuiría a asegurar la seguridad digital de las personas y prevenir la

vulneración de su información por sujetos inescrupulosos. Además, se propone el establecimiento de un sistema de rastreo de entidades responsables, la capacitación de la población en cuestiones de ciberseguridad y la promoción de políticas de Estado y políticas criminales actualizadas, con el objetivo de crear conciencia sobre el robo de información personal en entornos digitales, estableciendo mecanismos efectivos para navegar por diversas plataformas y colocando al ciudadano como eje central de estas iniciativas.

Referencias

Álvarez, A., y Risco, A. (2020a). *Clasificación de las investigaciones*. https://acortar.link/vB0vfN

Álvarez, A., y Risco, A. (2020b). *Justificación de la Investigación*. https://acortar.link/ztYFkb

Álvarez, E. (2017). Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. *Foro: Revista de Derecho*, *27*, 43–61. https://acortar.link/375Myu

Arias, L. (2020). *Técnicas e instrumentos de investigación científica*. https://acortar.link/4tOqZc

Arvelo, M., Paucar, P., y Párraga, C. (2022). Regulación global para evitar la suplantación de identidad digital. *Universidad y Sociedad*, *14*(6), 690–696. https://acortar.link/CIZ10k

Azuero, A. (2019). Significatividad del marco metodológico en el desarrollo de proyectos de investigación. *Revista Arbitrada Interdisciplinaria Koinonía*, *4*(8), 110–127. https://acortar.link/14m3IT

Ballesteros, M. C. R., & Hernández, J. A. G. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense*, *47*, 209–234. file:///C:/Users/User/Downloads/root,+189-662-1-CE.pdf

Becerra, K. (2020). Investigación cualitativa crítica y derecho: Análisis de su rol en la academia chilena y un estudio de caso. *Revista Pedagogía Universitaria y Didáctica Del Derecho*, *7*(1), 149–176. https://acortar.link/x3jFEt

Berrio, E., y Orellana, I. (2022). *El Tráfico Ilegal de Información Digital y Vulneración de los Datos Personales, Patrimoniales, Financieros en las Plataformas de Internet, Lima Este 2022* [Tesis para Obtener el Título Profesional de Abogado, Universidad Cesar Vallejo]. https://acortar.link/pJ44YS

Bramont-Arias, A. (1997). El delito informático en el Código Penal Peruano. In *Op. Cit* (Fondo Editorial PUCP). https://repositorio.pucp.edu.pe/index/handle/123456789/181585

Burgo, B., León, L., Cáceres, L., Pérez, J., y Espinoza, E. (2019). Algunas reflexiones sobre investigación e intervención educativa. *Revista Cubana de Medicina Militar*, *48*.

Campos, O. (2019). Normativa legal sobre delitos informáticos en Ecuador. *Revista Científica Hallazgos21*, *4*(1), 100–111. https://acortar.link/H8jw2R

Carvajal, B., y Estrada, R. (2020). Vulneración del derecho a la intimidad personal y familiar en las redes sociales. *Revista Jurídica Critica y Derecho*, *1*(1), 49–60. https://acortar.link/Udte8m

Casillas, A., y Ehrenzweig, M. (2023). Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas. *PAAKAT: Revista de Tecnología y Sociedad*, *24*. http://www.udgvirtual.udg.mx/paakat/index.php/paakat/article/view/759

Chaves, J. y Weiler, C. (2016). Los estudios de casos como enfoque metodológico. *Academo*, *3*(2). https://www.redalyc.org/pdf/6882/688273458012.pdf

Correia, R., y Da Silva, I. (2018). A ação do Estado em matéria de cibersegurança: Estudo de perceções no caso português. *Simbiótica. Revista Eletrônica*, *5*(2), 1–20. https://acortar.link/fxXGw2

Cruz, L. (2017). La política brasileña de ciberseguridad como estrategia de liderazgo regional. *URVIO Revista Latinoamericana de Estudios de Seguridad*, *20*, 16–30. https://acortar.link/ztJzD3

Delgado, V., Ortega, H., Sajhid, C., y Peraza, N. (2022). El análisis del crecimiento de phishing en los últimos años. *Revista Digital de Tecnologías Informáticas y Sistemas*, *6*(6), 7. https://www.redtis.org/index.php/Redtis/article/view/132

Deroncele, A., Gross, R., y Medina, P. (2021). El mapeo epistémico: herramienta esencial en la práctica investigativa. *Revista Universidad y Sociedad*, *13*(3), 172–188. https://acortar.link/B636fn

Fusco, E. (2020). Los delitos informáticos en el Código Penal Italiano. *Derecho Global. Estudios Sobre Derecho y Justicia*, *5*(14), 127–149. https://acortar.link/MnIu15

Gamón, P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO Revista Latinoamericana de Estudios de Seguridad*, *20*, 80–93. https://acortar.link/8ly4Ok

García, E. (2018). El Phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (rec. 1402/2016). *Iuris Tantum Revista Boliviana de Derecho*, *25*, 650–661. http://www.scielo.org.bo/scielo.php?pid=S2070-81572018000100025&script=sci_abstract&tlng=pt

Guerrero, M. (2022). El derecho a conocer los algoritmos utilizados en la toma de decisiones. Aproximación desde la perspectiva del derecho fundamental a la protección de datos personales. *Teoría y Realidad Constitucional*, *49*, 141–171. https://acortar.link/LlOkw0

Koto, I. (2021). Cyber crimen according to the ITE law. *International Journal Reglement & Society (IJRS)*, *2*(2), 103–110. https://acortar.link/kxkSwi

Liébana, C. (2023). *El derecho fundamental a la protección de datos personales y la responsabilidad proactiva*. ARANZADI/CIVITAS. https://acortar.link/kauCQx

Liniers, R. (2009). El análisis documental: indización y resumen en bases de datos especializadas. *E-LIS Repository, Http://Eprints. Rclis. Org/6015/1/Análisis_ Documental_indización_y_resumen. Pdf (Accessed March 15, 2018)*. https://acortar.link/avypJk

Maqueo, S., Moreno, J., y Recio, M. (2017). Protección de datos personales, privacidad y vida privada: La inquietante búsqueda de un equilibrio global necesario. *Revista de Derecho (Valdivia)*, *30*(1), 77–96. https://acortar.link/J36GUJ

Martínez, A., López, P., Cevallos, G., y Burgos, L. (2022). La protección de datos personales en Ecuador. *Estudios Del Desarrollo Social: Cuba y América Latina*, *10*(especial 1). https://acortar.link/gimTGd

Martínez, M., Osorio, C., y Lobo, M. (2021). Análisis del Phishing y la Ley de delitos informáticos en Colombia. *Cuaderno de Investigaciones: Semilleros Andina*, *1*(14). https://revia.areandina.edu.co/index.php/vbn/article/view/1948

Mayer, L., y Calderón, O. (2020). El delito de fraude informático: Concepto y delimitación. *Revista Chilena de Derecho y Tecnología*, *9*(1), 151–184. https://acortar.link/9KLWyh

Mendoza, O. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista Ius*, *15*(48), 179–207. https://acortar.link/tNV6XK

Monja, M. (2022). *Delitos informáticos en las entidades bancarias-suplantación de identidad* [Para Optar el Título Profesional de Abogado, Universidad Peruana de las Americas]. https://acortar.link/C6AmdP

Ortiz, H. (2002). *El derecho a la intimidad en la Nueva Ley Orgánica de Protección de Datos Personales*. Librería-Editorial Dykinson. https://acortar.link/zIYBXW

Ospina, R., y Sanabria, E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad*, *62*(2), 199–217. http://www.scielo.org.co/scielo.php?pid=S1794-31082020000200199&script=sci_arttext

Polanía, L., Cardona, A., Castañeda, I., Vargas, A., Calvache, A. y Abanto, I. (2020). *Metodología de investigación Cuantitativa & Cualitativa*. Institución Universitaria Antonio José Camacho. https://repositorio.uniajc.edu.co/handle/uniajc/596

Prieto, N., & Vargas, G. (2020). Ciberdelincuencia, enfocada en la apropiación de información a través de medios electrónicos y su influencia en el cometimiento de delitos informáticos [Tesis para optar el grado de Abogado, Universidad de Guayaquil]. In *Obtenido de Repositorio de la Universidad de Guayaquil: http://repositorio. ug. edu. ec/bitstream/redug/50396/1/Nicole% 20Prieto*. http://repositorio.ug.edu.ec/handle/redug/50396

Ramos, A. (2020). Los alcances de una investigación. *CienciAmérica*, *9*(3), 1–6. https://acortar.link/nbPUzU

Rosas-Lanas, G., y Pila-Cárdenas, G. (2023). La protección de datos personales en Ecuador: Una revisión histórica-normativa de este derecho fundamental en el país suramericano. *VISUAL REVIEW. International Visual Culture Review/Revista Internacional de Cultura Visual*, *13*(2), 1–16. https://www.journals.eagora.org/revVISUAL/article/view/4568

Sánchez, A. (2019). Fundamentos epistémicos de la investigación cualitativa y cuantitativa: Consensos y disensos. *Revista Digital de Investigación En Docencia Universitaria*, *13*(1), 102–122. https://acortar.link/wWbRg

Sánchez, A. (2017). Las nuevas tecnologías y su impacto en los derechos al honor, intimidad, imagen y protección de datos del menor. Mecanismos jurídicos de protección: Carencias, interrogantes y retos del legislador. *Iuris Tantum Revista Boliviana de Derecho*, *23*, 168–191. https://acortar.link/JQD4CV

Schmalbach, V., Herrera, F. y Ávila, M. (2010). La planeación por escenarios: Revisión de conceptos y propuestas metodológicas. *Prospectiva*, *8*(2), 21–29. https://www.redalyc.org/pdf/4962/496250978004.pdf

Terreros, V. (2014). Delitos informáticos. *Ius et Veritas*, *49*, 284–304. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Tuesta, R. (2022). *Fraude informático y su impacto en los derechos fundamentales de la persona en el Cercado de Lima–2022* [Trabajo de Suficiencia Profesional para optar el Título de Abogado, Universidad Norbert Wiener]. https://repositorio.uwiener.edu.pe/handle/20.500.13053/8054

Urzola, M. (2020). Métodos inductivo, deductivo y teoría de la pedagogía crítica. Revista Crítica Transdisciplinar, 3(1), 36-42. https://acortar.link/0zgimS

Vélez, C. (2017). La explotación de los datos personales por los gigantes de internet. *Estudios En Derecho a La Información*, *3*, 27–55. https://dialnet.unirioja.es/servlet/articulo?codigo=7399685

Vereau, V. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Ius et Praxis*, *053*, 95–110. https://acortar.link/oJJTOM

Villa Motato, S. M., & Acuña López, L. F. (2018). *Estado actual del cibercrimen en Colombia con respecto a Latinoamérica.* [Tesis para optar el título de abogado, Universidad Nacional de Colombia]. https://repository.unad.edu.co/handle/10596/25619

Yanqui, A. (2020). TikTok: La ineficacia del derecho a la intimidad en la era digital en tiempos de Covid-19 y el "famoso" derecho al olvido en Perú. *Revista de Derecho: Universidad Nacional Del Altiplano de Puno*, *5*(1), 194–204. https://acortar.link/LSX6m3

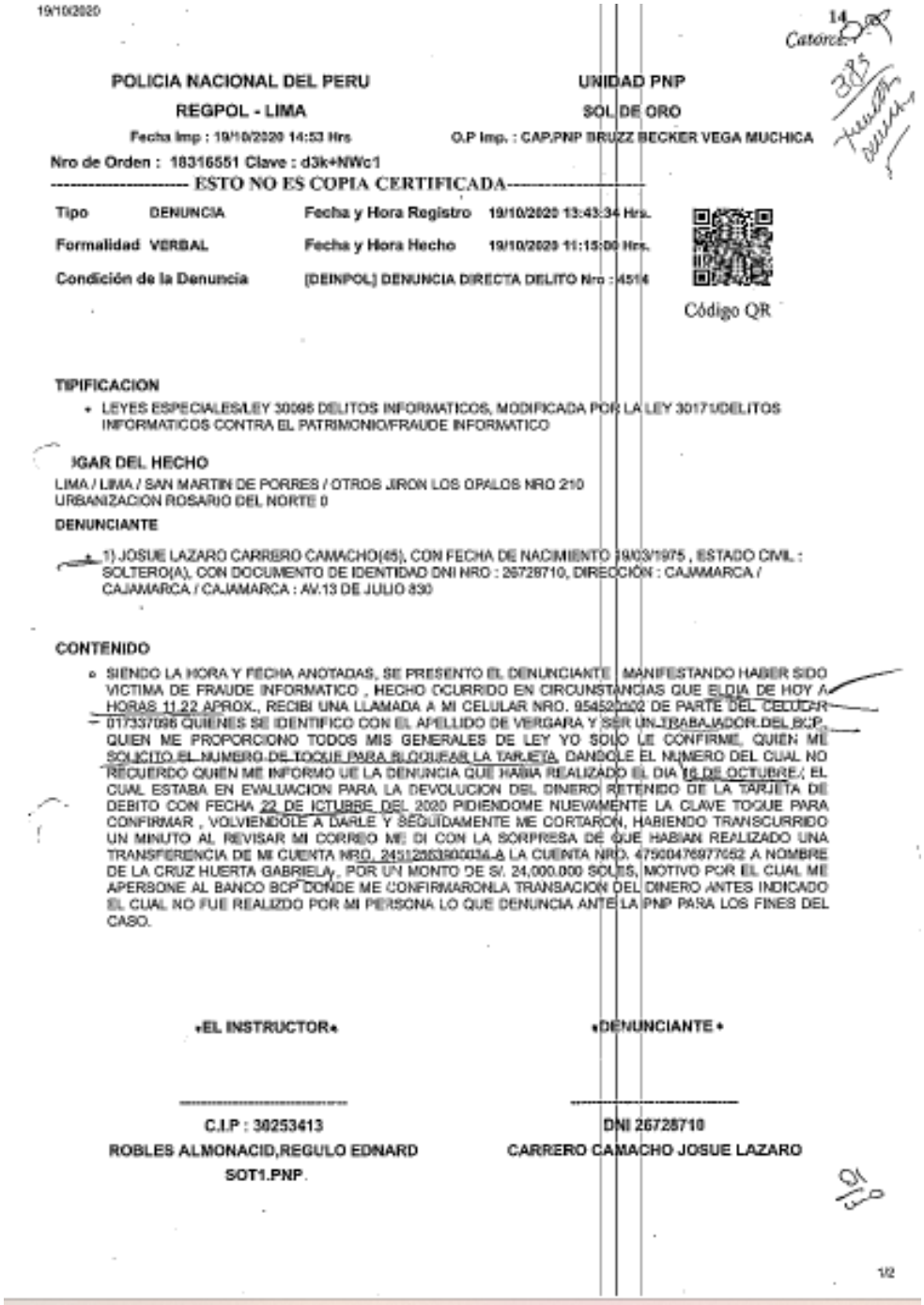
Anexos

Anexo 1: Matriz de categorización o apriorística

Problema General	Problemas Específicos	Objetivo General	Objetivos Específicos	Categorías	Sub categorías	Metodología
¿Cómo impacta el delito de fraude informático frente al uso doloso de los datos personales, Lima 2023?	¿Cómo impacta las modalidades del phishing y carding frente al delito de fraude informático, Lima 2023? ¿ Cómo impacta la protección de datos frente al uso doloso de los datos personales, Lima 2023?	Determinar cómo impacta el delito de fraude informático frente al uso doloso de los datos personales, Lima 2023	Determinar cómo impacta las modalidades de phishing y carding frente al delito de fraude informatico, Lima 2023. Determinar cómo impacta la protección de datos frente al uso doloso de los datos personales, Lima 2023.	Delito informatico	Phishing Carding	**Enfoque**: Cualitativo **Método:** Inductivo **Diseño**: No experimental – Estudios de caso **Nivel:** Exploratorio **Tipo de investigación**: Básica
				Los datos personales	Protección de datos	**Técnica:** Análisis Documentario **Instrumento:** Ficha Documentaria **Escenario de estudio:** Ciudad de lima

Fuente: Elaboración Propia (2023)

Anexo 2. Resolución judicial que contiene el caso jurídico



19/10/2020

14
Catorce

POLICIA NACIONAL DEL PERU
REGPOL - LIMA
Fecha Imp : 19/10/2020 14:53 Hrs

UNIDAD PNP
SOL DE ORO
O.P Imp. : CAP.PNP BRUZZ BECKER VEGA MUCHICA

Nro de Orden : 18316551 Clave : d3k+NWc1

---------- ESTO NO ES COPIA CERTIFICADA----------

Tipo	DENUNCIA	Fecha y Hora Registro	19/10/2020 13:43:34 Hrs.
Formalidad	VERBAL	Fecha y Hora Hecho	19/10/2020 11:15:00 Hrs.
Condición de la Denuncia		[DEINPOL] DENUNCIA DIRECTA DELITO Nro : 4514	

Código QR

TIPIFICACION

- LEYES ESPECIALES/LEY 30096 DELITOS INFORMATICOS, MODIFICADA POR LA LEY 30171/DELITOS INFORMATICOS CONTRA EL PATRIMONIO/FRAUDE INFORMATICO

IGAR DEL HECHO

LIMA / LIMA / SAN MARTIN DE PORRES / OTROS JIRON LOS OPALOS NRO 210 URBANIZACION ROSARIO DEL NORTE 0

DENUNCIANTE

- 1) JOSUE LAZARO CARRERO CAMACHO(45), CON FECHA DE NACIMIENTO 19/03/1975 , ESTADO CIVIL : SOLTERO(A), CON DOCUMENTO DE IDENTIDAD DNI NRO : 26728710, DIRECCIÓN : CAJAMARCA / CAJAMARCA / CAJAMARCA : AV.13 DE JULIO 830

CONTENIDO

- SIENDO LA HORA Y FECHA ANOTADAS, SE PRESENTO EL DENUNCIANTE MANIFESTANDO HABER SIDO VICTIMA DE FRAUDE INFORMATICO , HECHO OCURRIDO EN CIRCUNSTANCIAS QUE EL DIA DE HOY A HORAS 11.22 APROX., RECIBI UNA LLAMADA A MI CELULAR NRO. 954522002 DE PARTE DEL CELULAR 017337096 QUIENES SE IDENTIFICO CON EL APELLIDO DE VERGARA Y SER UN TRABAJADOR DEL BCP, QUIEN ME PROPORCIONO TODOS MIS GENERALES DE LEY YO SOLO LE CONFIRME, QUIEN ME SOLICITO EL NUMERO DE TOQUE PARA BLOQUEAR LA TARJETA, DANDOLE EL NUMERO DEL CUAL NO RECUERDO QUIEN ME INFORMO UE LA DENUNCIA QUE HABIA REALIZADO EL DIA 16 DE OCTUBRE./ EL CUAL ESTABA EN EVALUACION PARA LA DEVOLUCION DEL DINERO RETENIDO DE LA TARJETA DE DEBITO CON FECHA 22 DE ICTUBRE DEL 2020 PIDIENDOME NUEVAMENTE LA CLAVE TOQUE PARA CONFIRMAR , VOLVIENDOLE A DARLE Y SEGUIDAMENTE ME CORTARON, HABIENDO TRANSCURRIDO UN MINUTO AL REVISAR MI CORREO ME DI CON LA SORPRESA DE QUE HABIAN REALIZADO UNA TRANSFERENCIA DE MI CUENTA NRO. 24512663800034-8 LA CUENTA NRO. 47900476977052 A NOMBRE DE LA CRUZ HUERTA GABRIELA , POR UN MONTO DE S/. 24,000.000 SOLES, MOTIVO POR EL CUAL ME APERSONE AL BANCO BCP DONDE ME CONFIRMARONLA TRANSACION DEL DINERO ANTES INDICADO EL CUAL NO FUE REALIZDO POR MI PERSONA LO QUE DENUNCIA ANTE LA PNP PARA LOS FINES DEL CASO.

•EL INSTRUCTOR•

C.I.P : 30253413
ROBLES ALMONACID,REGULO EDNARD
SOT1.PNP.

•DENUNCIANTE •

DNI 26728710
CARRERO CAMACHO JOSUE LAZARO

1/2

SENTENCIA CONFORMADA

RESOLUCION Nº DOS
Independencia, quince de marzo
Del año dos mil veintitrés.-

VISTOS Y OIDOS: En audiencia oral y pública, la presente causa, se procede a dictar sentencia bajo los términos siguientes:

PARTE EXPOSITIVA y CONSIDERATIVA : Registrada en audio (00:24:38)
PARTE RESOLUTIVA : Se transcribe (00:50:16)

Por estas consideraciones la Juez del séptimo Juzgado Penal Unipersonal de la Corte Superior de Lima Norte, **FALLA:**

1. **CONDENANDO** a los ciudadanos **CHRISTIAN JESUS PONTE DONAYRE,** identificado con DNI N° 78969848 como **AUTOR** y a **GABRIELA DE LA CRUZ HUERTA,** identificada con DNI N° 74615298 como **CÓMPLICE PRIMARIO,** ambos por el delito contra el patrimonio en la modalidad de **FRAUDE INFORMATICO** previsto y sancionado en el primer párrafo del artículo 8 de la Ley Número 30096 modificado por el artículo 1 de la Ley Número 30171, en agravio de **JOSUE LAZARO CARRERA CAMACHO**; y como tal, **LE IMPONGO** a **CHRISTIAN JESUS PONTE DONAYRE** la pena de **TRES AÑOS Y SEIS MESES DE PENA PRIVATIVA DE LIBERTAD,** incluida la rebaja por los principios de proporcionalidad, racionalidad, lesividad y humanidad de las penas y la rebaja de 1/7 por conclusión anticipada de juicio, cuya ejecución **SE SUSPENDE CONDICIONALMENTE POR EL PERIODO DE PRUEBA DE TRES AÑOS** y a **GABRIELA DE LA CRUZ HUERTA** le impongo la pena de **DOS AÑOS Y SIETE MESES DE PENA PRIVATIVA DE LIBERTAD,** incluida la rebaja por los principios de proporcionalidad, racionalidad, lesividad y humanidad de las penas y la rebaja de 1/7 por conclusión anticipada de juicio, cuya ejecución **SE SUSPENDE CONDICIONALMENTE POR EL MISMO PERIODO DE PRUEBA**; quedando los sentenciados sujetos a las siguientes reglas de conducta: **a)** no ausentarse de su domicilio ni variar el mismo sin previa autorización del juzgado, **b)** concurrir a la Oficina de Control Biométrico de ésta sede judicial cada fin de mes en forma personal y obligatoria para registrar su firma y justificar sus actividades, **c)** no concurrir a lugares de dudosa reputación y **d)** reparar el daño ocasionado por su delito, cumpliendo el pago de la reparación civil acordada y la devolución del dinero materia del delito ascendente a la suma de veinticuatro mil soles (S/.24,000.00) conforme al acuerdo. Todo ello, **BAJO APERCIBIMIENTO** de aplicarse el artículo 59° inciso 3) del Código Penal en caso de incumplimiento de las reglas de conducta, previo requerimiento del Ministerio Público. Asimismo le **IMPONGO** a los sentenciados **CHRISTIAN JESUS PONTE DONAYRE** y a **GABRIELA DE LA CRUZ HUERTA** la pena de **SESENTA DIAS MULTA** a cada uno de ellos, equivalente al 25% de la remuneración mínima vital, por lo que teniendo en cuenta dicha remuneración, la multa diaria asciende a siete soles con setenta y cinco céntimos de sol (S/.7.75), lo que hace un total de cuatrocientos sesenta y cinco soles (S/465.00) que deberá pagar cada sentenciado a favor del Estado a más tardar el último día hábil del mes de abril del año 2023, bajo apercibimiento de ley en caso de incumplimiento.

2. **FIJO** como **REPARACIÓN CIVIL** la suma de **DOS MIL SOLES (S/2.000.00)** que los sentenciados deberán pagar en forma solidaria a favor del agraviado **JOSUE LAZARO CARRERA CAMACHO**, sin perjuicio de la devolución de la suma materia del delito de fraude informático, ascendente a **VEINTICUATRO MIL SOLES (S/24,000.00)** lo que sumado a la reparación civil da un total de **VEINTISEIS MIL SOLES (S/26,000.00)** que deberán pagar los sentenciados en forma solidaria en veintiséis (26) cuotas mensuales, cada cuota de **UN MIL SOLES (S/1,000.00)**, debiendo iniciar el pago de dichas cuotas el último día hábil del mes de mayo del 2023 y así sucesivamente deberán cancelar cada cuota en forma solidaria el último día hábil de cada mes, culminando con la última cuota, el último día hábil del mes de junio del 2025.

3. **SE EXIME** a los sentenciados **CHRISTIAN JESUS PONTE DONAYRE** y **GABRIELA DE LA CRUZ HUERTA** del pago de **COSTAS PROCESALES** al haber arribado a un acuerdo de conclusión anticipada de juicio.

4. **SE ORDENA** que consentida o ejecutoriada que sea la presente sentencia, se inscriban y remitan los boletines de condena para su debida inscripción al registro de condenas correspondientes y se remitan los autos para su ejecución al Juzgado competente.

5. **SE DISPONE** la devolución de la carpeta fiscal al Ministerio Público en caso que el juzgado haya recibido la carpeta física.

NOTIFICACION:

MINISTERIO PÚBLICO	: Conforme.
DEFENSA DEL SENTENCIADO CHRISTIAN JESUS PONTE DONAYRE	: Conforme.
SENTENCIADO CHRISTIAN JESUS PONTE DONAYRE	: Conforme.
DEFENSA DE LA SENTENCIADA GABRIELA DE LA CRUZ HUERTA	: Conforme.
SENTENCIADA GABRIELA DE LA CRUZ HUERTA	: Conforme.

00:58':36"hrs JUEZ: Señala que estando todos conformes, se expide la siguiente resolución:

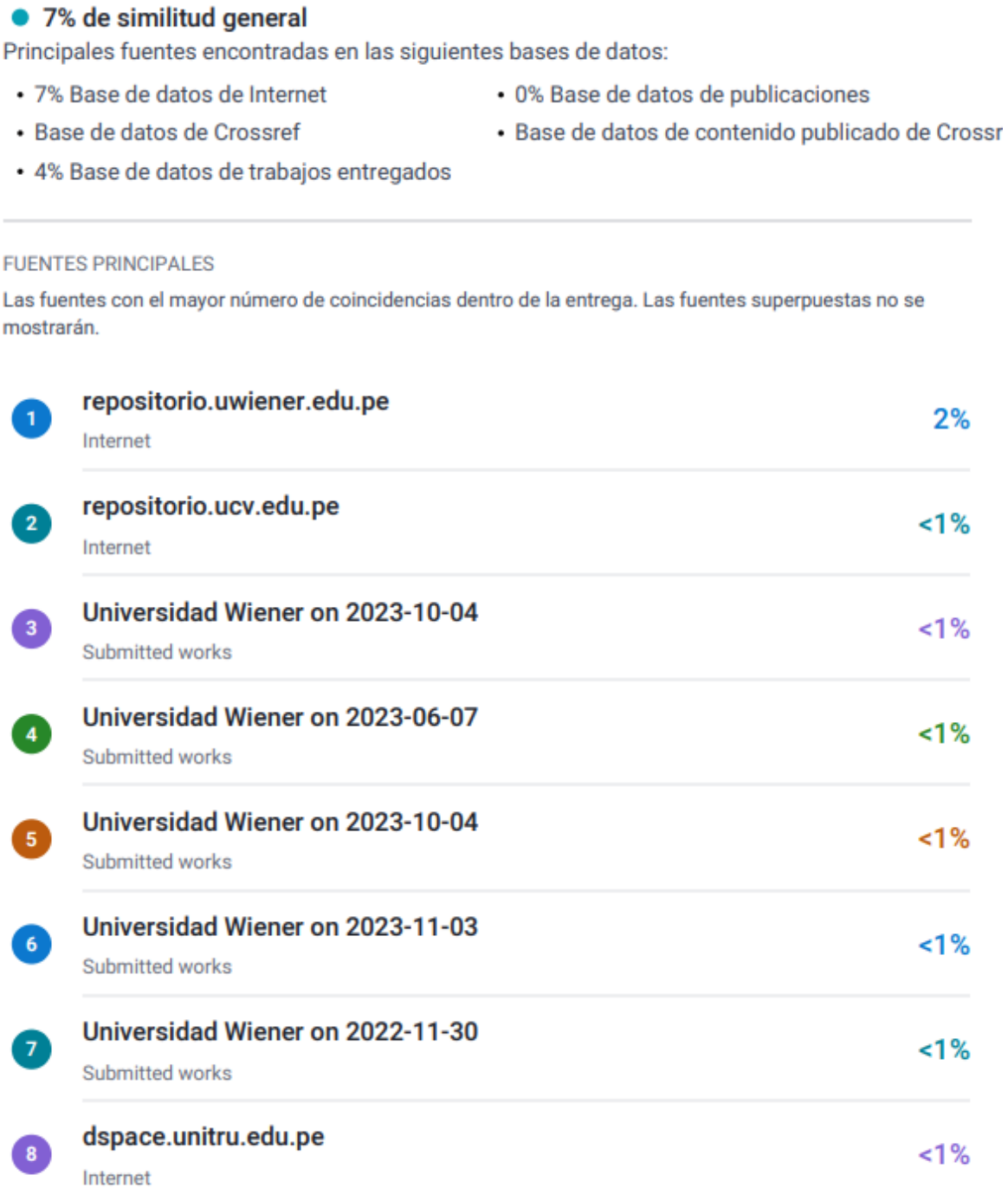
RESOLUCION Nº TRES
Independencia, quince de marzo
Del año dos mil veintitrés.-

AUTOS, VISTOS Y OIDOS; y Considerando: que en la presente audiencia se ha dictado sentencia conformada y que las partes procesales legitimadas han mostrado conformidad con la sentencia, y no habiendo constitución en actor civil, **RESUELVE: DECLARAR CONSENTIDA** la sentencia conformada.

CONCLUSIÓN:
Se da por concluida la audiencia y por cerrado la grabación del audio, y procediéndose a firmar el acta la Señora Juez y el especialista de audiencia, conforme a lo dispuesto en el artículo 121° del Código Procesal Penal.-

Anexo 3. Declaratoria de originalidad de autoría

Anexo 4. Reporte de informe de similitud



● 7% de similitud general

Principales fuentes encontradas en las siguientes bases de datos:

- 7% Base de datos de Internet
- 0% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossr
- 4% Base de datos de trabajos entregados

FUENTES PRINCIPALES

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1	repositorio.uwiener.edu.pe Internet	2%
2	repositorio.ucv.edu.pe Internet	<1%
3	Universidad Wiener on 2023-10-04 Submitted works	<1%
4	Universidad Wiener on 2023-06-07 Submitted works	<1%
5	Universidad Wiener on 2023-10-04 Submitted works	<1%
6	Universidad Wiener on 2023-11-03 Submitted works	<1%
7	Universidad Wiener on 2022-11-30 Submitted works	<1%
8	dspace.unitru.edu.pe Internet	<1%