FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Fraude informático y la protección del patrimonio en tiempos de pandemia en el distrito fiscal Lima Este, periodo 2021

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTOR:

Linares Vila, Juan Carlos (orcid.org/0000-0002-2823-2562)

ASESOR:

Dr. Vildoso Cabrera, Erick Daniel (orcid.org/0000-0002-0803-9415)

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

2022

DEDICATORIA

A Dios por su gracia y don de la vida; a mi madre por su amor incondicional, a mi familia por su tiempo y apoyo constante en este proceso.

AGRADECIMIENTO

A la DIVINDAT; a la presidencia de junta de fiscales Lima Este, al asesor Dr. Erick Daniel Vildoso Cabrera y a todos los abogados penalistas que han coadyuvado a la culminación de la presente tesis.

ÍNDICE DE CONTENIDOS

Pág.

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS Y FIGURAS

.

RESUMEN

El presente trabajo de investigación responde a la pregunta ¿De qué manera el fraude informático influye en la protección del patrimonio en época de pandemia en el distrito fiscal de Lima Este, periodo 2021?

Teniendo como objetivo general, establecer la manera en que fraude informático incide en la protección del patrimonio en época de pandemia en el distrito fiscal de Lima Este, periodo 2021.

El método de la investigación fue descriptivo y el diseño de la investigación fue no experimental, debido que no se alteró la realidad para su estudio. La población fue 50 personas entre abogados y fiscales, para el programa de procesamiento de datos se utilizó google drive y Excel.

Los resultados de estas tecnicas de investigación comprueban la hipótesis general llegando a brindar respaldo científico al afirmar que el fraude informático inciden negativamente en la protección del patrimonio en época de pandemia, los resultados de la medición de los indicadores guardan armonía con la teoría de delitos informáticos desarrollada en nuestro marco teórico.

Palabras clave: Fraude Informático, Transferencias Electrónicas Fraudulentas, Protección del Patrimonio, Ciberdelincuencia.

ABSTRACT

This research work answers the question: How does computer fraud influence the protection of assets in times of pandemic in the fiscal district of Lima Este, period 2021?

Having as a general objective, to establish the way in which computer fraud affects the protection of assets in times of pandemic in the fiscal district of Lima Este, period 2021.

The research method was descriptive and the research design was non-experimental, since reality was not altered for its study. The population was 50 people between lawyers and prosecutors, for the data processing program Google drive and Excel were used.

The results of these research techniques verify the general hypothesis, providing scientific support by stating that computer fraud has a negative impact on the protection of heritage in times of pandemic, the results of the measurement of the indicators are in harmony with the theory of computer crimes. developed in our theoretical framework.

Keywords: Computer Fraud, Fraudulent Electronic Transfers, Asset Protection, Cybercrime.

I. INTRODUCCIÓN

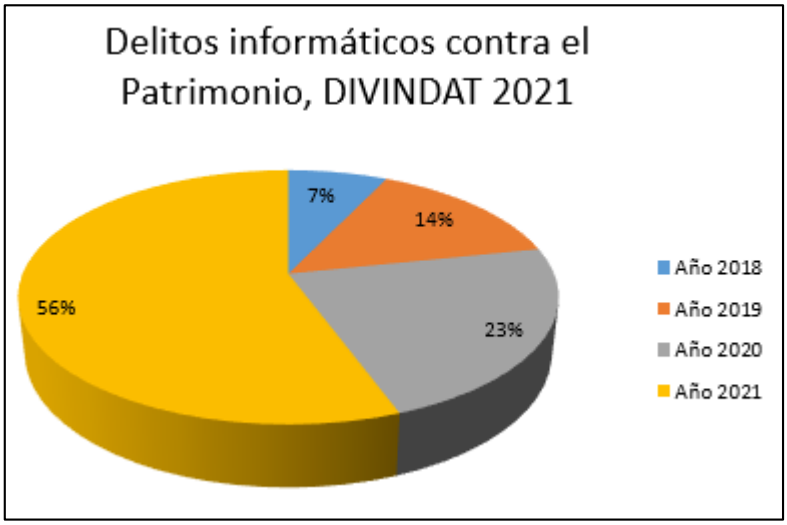
Las tecnologías de información y comunicaciones han cambiado el modo de vida del ser humano trayendo consigo nuevas oportunidades, pero también amenazas ya que los delincuentes abusan de la tecnología para cometer delitos como el fraude informático.

Aunque es verdad que los fraudes informáticos se cometen antes de la pandemia ocasionada por el COVID-19, se ha visto incrementada a partir del estado de emergencia Nacional, situación propicia para el aumento del pishing según lo reporta el Instituto Nacional de Salud del Perú. Gutiérrez (2020). Los establecimientos medianos y pequeños cerraron, razón por la cual se fortaleció el comercio virtual de bienes y servicios y como consecuencia de esto se incrementó el uso de transacciones electrónicas, duplicando su uso en el (2020) según la cámara de compensación electrónica.

Instituciones públicas encargadas de la seguridad ciudadana como la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), órgano especializado de la policía nacional del Perú, reportan un incremento de fraude informático**.** (Figura 1).

Figura 1

Delitos Informáticos contra el Patrimonio

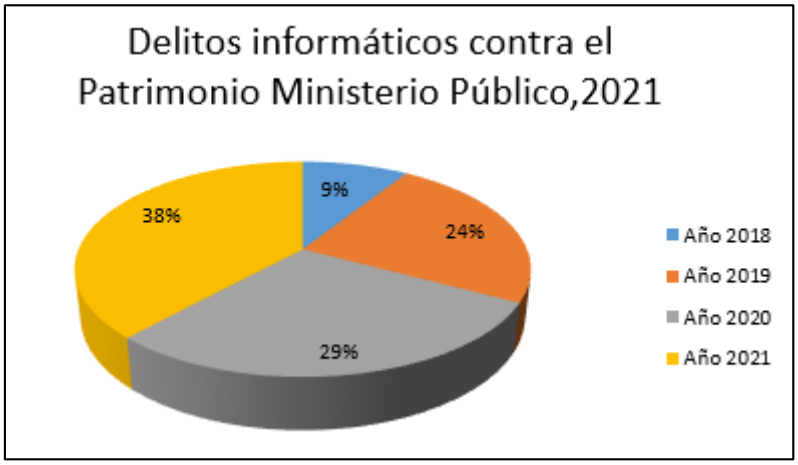


Nota. Tomado de *Informe de Ciberdelincuencia,* Ministerio del Interior, 2021

De forma similar ocurre con las cifras del Ministerio Público que evidencian la misma tendencia. Una particularidad de estos delitos es que rara vez llegan a sentencia generando una alta carga fiscal y también una sensación de impunidad. En un informe preliminar el ministerio público menciona que los delitos informáticos contra el patrimonio se vuelven más recurrentes a propósito de la pandemia Covid19. Ministerio Público (2021). (Figura 2)

Figura 2

Delitos Informáticos contra el Patrimonio. Ministerio Público



Nota. Tomado de *Ciberdelincuencia en el Perú.* Ministerio Público 2021

En este sentido desde la vigencia de la ley 30096 (ley de delitos informáticos) en octubre de 2013, se archivaron el 58% de las carpetas fiscales y se llegó a sentencia solo 108 casos que representa menos del 1%.

Algunos autores señalan que el incremento de los fraudes informáticos está relacionado en parte al acelerado avance de la tecnología de información que se renuevan a una velocidad mayor en la que progresa el marco jurídico, esta brecha entre la tecnología y la regulación jurídica se conoce como “cadencia tecnológica”. A esta cadencia tecnológica se le suma la falta de preparación de las personas en el uso de estas tecnologías, lo que hace un terreno favorable a los delincuentes para cometer ilícitos penales. Posada (2017).

Los delincuentes valiéndose de técnicas de phishing sustraen datos personales a sus víctimas tomando la identidad de las personas. La víctima es atraída por publicidad atractiva que hay en e-mail, mensaje de texto y redes sociales, haciendo que las víctimas entreguen información personal y confidencial al agente sin sospechar que la página web es falsa y creada para propósitos delictivos, esta técnica es denominada phishing y es la de mayor recurrencia para cometer este tipo de ilícitos.Hidalgo (2021)

Una particularidad de estos delitos es que pueden ser cometidos desde cualquier parte del mundo, afectando el principio de territorialidad de la norma penal, por lo que la cooperación internacional entre países es de suma importancia para el seguimiento del delito a fin de evitar su impunidad.

En este marco de cooperación internacional, Perú ha ratificado el convenio internacional de Budapest, con la finalidad de combatir la delincuencia informática, busca tener puntos en común entre las leyes de los países que son parte de este convenio. En la legislación interna estos delitos están comprendidos en la ley nº 30096 modificada por la ley nº 30171. Urpeque (2019).

En este orden de ideas, existe la necesidad de tomar medidas contra el fraude informático que influyen en la protección del patrimonio, máxime si las medidas decretadas por el Estado de emergencia favorecen la utilización de la tecnología.

Formulación del Problema

Problema General

¿De qué manera el fraude informático incide en la protección del patrimonio en tiempos de pandemia en el Distrito Fiscal de Lima Este, periodo 2021?

Problemas Específicos

Primer problema específico

- ¿De qué manera el phishing influye en el derecho de goce del bien en tiempos de pandemia en el distrito fiscal de Lima Este, periodo 2021?

Segundo problema específico

- ¿De qué manera las trasferencias electrónicas fraudulentas afectan la disposición del bien en tiempos de pandemia en el Distrito Fiscal de Lima Este, periodo 2021?

OBJETIVOS

Objetivo General

Determinar de qué manera el fraude informático incide en la protección del patrimonio en tiempos de pandemia en el Distrito Fiscal de Lima Este, periodo 2021

Objetivos Específicos

Primer objetivo específico

- Establecer cómo el phishing influye en el derecho de goce del bien en tiempos de pandemia en el distrito fiscal de Lima Este, periodo 2021.

Segundo objetivo específico

- Precisar de qué modo las transferencias electrónicas fraudulentas afectan la disposición del bien en tiempos de pandemia en el Distrito Fiscal de Lima Este, periodo 2021.

FORMULACIÓN DE HIPÓTESIS

Hipótesis General

El fraude informático incide negativamente en la protección del patrimonio en tiempos de pandemia en el Distrito Fiscal de Lima Este, periodo 2021

Hipótesis Específicas

Primera hipótesis específica

El phishing influye negativamente en el derecho de goce del bien en tiempos de pandemia en el Distrito fiscal de Lima Este, periodo 2021

Segunda hipótesis específica

Las transferencias electrónicas fraudulentas afectan negativamente la disposición del bien en tiempos de pandemia en el Distrito Fiscal de Lima Este, periodo 2021.

JUSTIFICACIÓN DE LA INVESTIGACIÓN

Justificación Teórica

Es necesario realizar el análisis jurídico respecto al fraude informático, siendo que bajo el ámbito de la Ley de delitos informáticos N° 30096 y sus modificatorias

Ley N° 30171 existen ambigüedades en los tipos penales, por lo que es necesario realizar una revisión de las teorías.

Justificación Práctica

Los reportes del ministerio público muestran que las denuncias por delito informático van en aumento, en contraposición del número de sentencias, como consecuencia se tiene una importante carga fiscal acompañado de una sensación de impunidad e inseguridad. Esto sumado a que nuestro país es uno de los más afectados con la pandemia de COVID19 y la tecnología se vuelve un medio más recurrente.

DELIMITACIÓN DE LA INVESTIGACIÓN

Delimitación Temporal

Período 2021

Delimitación Espacial

Distrito fiscal Lima Este

Delimitación Social

Este estudio está dirigido a Magistrados, Abogados y estudiantes de derecho interesados en investigación de denuncias por delitos informáticos contra el patrimonio.

II. MARCO TEÓRICO

Si bien es cierto que el derecho informático es una rama novel en comparación con las otras ramas del derecho y su existencia se relaciona con el desarrollo de internet, sin embargo, se han realizado ciertas investigaciones cuantitativas y cualitativas respecto a la problemática del fraude informático, tanto a nivel nacional como internacional.

En el ámbito internacional una de las más recientes investigaciones es realizada por Novoa Ignacio (2020), que titula Herramientas del Convenio de Budapest sobre ciberdelincuencia y su adecuación a la legislación nacional para alcanzar el grado de licenciado en ciencias jurídicas por la Universidad de Chile, tuvo como objetivo general analizar la respuesta normativa sobre el fenómeno de la ciberdelincuencia mediante la implementación del Convenio de Budapest y el proceso de adaptación en Chile, tomando especial atención a la proporcionalidad de las medidas propuestas en dicho convenio.

El estudio reconoce al convenio de Budapest como la mayor respuesta ante estos delitos informáticos por parte de la comunidad internacional. Este instrumento necesita fundamentalmente de la participación concurrente de los países miembros, además de conocer la realidad de cada país y adecuar los tipos para una interpretación internacional. El convenio en su versión original ha quedado desfasado con el transcurrir del tiempo por la aparición de nuevas modalidades delictivas que trae consigo el avance de la tecnología de la información y comunicaciones, mereciendo ser complementado por las normas de cada país y la realidad tecnológica.

Chile ha tomado como plataforma inicial este convenio para adecuarlo a la legislación nacional, teniendo precaución de no afectar los derechos fundamentales de los ciudadanos como la intimidad. El convenio no establece los límites taxativos para aplicar esta regulación, solo hace mención que para realizar la intervención se debe tratar delitos graves y respetar los derechos fundamentales.

El autor menciona que Chile ha realizado la adecuación al convenio y ha realizado la actualización de la ley 19233, ley de delitos informáticos, para la lucha contra la ciberdelincuencia, pero aún existe una baja aplicación de la norma en los tribunales, por lo que en efectos prácticos no resuelve los problemas de la criminalidad informática del país. Uno de los motivos fundamentales que descubre el autor es la deficiente capacitación de los operadores de justicia respecto a estos tipos de delitos por lo que se recomienda la capacitación y dotación de herramientas adecuadas al personal policial encargado.

En cuanto a los temas pendientes no cubiertos por la norma chilena a pesar de la implementación del convenio de Budapest es la responsabilidad de la tenencia de meta data de los ciudadanos en particular por las entidades particulares lo cual no está regulado.

Otra investigación contemporánea es la realizada por Hernández (2019), que realiza un estudio sobre la “Suplantación de identidad cibernética en el Ecuador”, trabajo que se realiza para obtener el grado de maestría por la Universidad externado de Colombia. El objetivo general del presente es determinar si las leyes en el Ecuador son lo suficientemente amplias para salvaguardar la identidad digital de sus habitantes.

En las conclusiones describe que Ecuador es un país en vías de desarrollo por lo que no cuenta con la suficiente educación tecnológica para salvaguardar la identidad digital de sus ciudadanos. No posee una cultura informática suficiente para poder distinguir entre las ventajas y desventajas del uso de internet lo cual lo hace vulnerable a los delitos informáticos ocupando el tercer puesto de vulnerabilidad a nivel de América del sur.

También podemos señalar en su conclusión respecto a las normas que regulan los delitos informáticos, en la cual menciona que son insuficientes e inadecuadas, puesto que fueron realizadas de manera temporal, la cuales no permiten abarcar la problemática de forma integral, y que con el transcurrir del tiempo han quedado desfasadas respecto a las nuevas tecnologías dejando a los ciudadanos sin

garantías para navegar en el ciberespacio. Siendo así, se recomienda a los legisladores, la creación de un marco legal de amplia interpretación de los delitos de suplantación de identidad cibernética que puedan cometerse en el futuro.

Otra investigación internacional es la desarrollada por Devia (2017) en la universidad de Sevilla – España que tiene como título: “Estafa Informática del artículo 248.2 del código penal” para optar el título de doctor en derecho, en la cual realiza un análisis detallado de este artículo tipificado en la norma penal española, para luego realizar una revisión sistemática sobre los requisitos necesarios para configurar este delito informático.

En las conclusiones de este trabajo se menciona que debido al fenómeno de la globalización han aparecido nuevas formas delictivas acorde con el avance tecnológico, estableciéndose cada vez más una influencia que existe entre delito y la informática. En esta relación se perfeccionan los delitos tradicionales como la estafa, delitos informáticos que utilizan la tecnología como un medio.

El estudio también menciona que a pesar que existe mayor cuidado para evitar ser víctima de operaciones fraudulentas, estas han ido en aumento debido en parte porque no todos están conscientes de los riesgos que implica el uso de medios tecnológicos. Los delincuentes se agencian de técnicas cada vez más sofisticadas para realizar estos ilícitos, acrecentando con este accionar el phishing

En el ámbito nacional, Cangalaya (2020) en su trabajo de tipo cualitativo, nivel descriptivo, con título “Fraude informático en los bonos de subsidio social en épocas de pandemia” efectuado para obtener el título de abogado por la Universidad de Huánuco, Perú. Tiene como objetivo general explicar la incidencia del fraude informático en los bonos entregados por el gobierno como subsidio social. El estudio se realizó en épocas de pandemia en la provincia de Chanchamayo, 2020.

En esta investigación gira en el entorno de la época del subsidio monetario entregado por el gobierno en la cual relaciona el incremento de incidencia del fraude informático en un 59% por lo cual concluye que tiene una relación marcada en la

provincia de Chanchamayo, 2020. Menciona luego que en esta provincia no puede atender este número de denuncias de fraude informático por falta de tecnología y personal capacitado. Por lo que recomienda la capacitación de los operadores de justicia y la implementación de medios tecnológicos para hacerle frente a esta situación. Así mismo no cuentan con personal capacitado de la policía nacional para atender esta demanda por lo que la descentralización de la DIVIDAT se hace necesaria para evitar que los delitos queden impunes.

Mori (2019) en su tesis de tipo cuantitativo sobre delitos informáticos y la protección penal de la intimidad para obtener el grado de maestro en la Universidad Federico Villarreal, Lima Perú. Este trabajo tiene como objetivo general entender las razones de la inexactitud de la tarea de los operadores de justicia en el proceso penal de los delitos informáticos, y cómo afecta este hecho la protección de la intimidad, el estudio de tipo longitudinal en el distrito Judicial de Lima, entre los años 2008 al 2012.

Urpeque (2019) realiza la tesis de adecuación de la Ley N°30096 en el marco del convenio internacional de Budapest 2001, estudio realizado en Huaura 2018, trabajo de tipo cualitativo efectuado para obtener el título de abogado en la Universidad Nacional Faustino Sánchez Carrión, Huacho Lima Perú. Está orientado a determinar si esta adecuación ha contribuido a reducir los delitos informáticos. Como conclusión señala que se debe considerar la relación de aspectos más importantes a brindar protección y cuales no han sido señalada en la legislación nacional, debido a las particularidades que presenta el ambiente donde se desarrolla los delitos informáticos

Entre las conclusiones menciona que la ley de delitos informáticos 30096 ha caído en obsolescencia debido a que no entiende del robo de información mediante phishing o hacking. También señala que se tiene que diferenciar la afectación de los bienes personales como un correo electrónico personal, de los servicios electrónicos de mayor alcance, hablando en los mismos términos cuando afecta un servidor de correos. Recomienda el autor que el legislador tenga en cuenta cuando se debatan los proyectos de ley, la opinión del ministerio público y del poder judicial

para lo cual se debería crear oficinas especializadas en estas entidades. También recomienda como parte de la seguridad informática que el software esté diferenciado por un identificador único. y que la entidad digital del usuario esté ligada al identificador del dispositivo.

(Vilca, 2018), realiza la tesis sobre la situación de los Hackers en el código penal peruano, trabajo cualitativo de nivel descriptivo efectuado para obtener el título de abogado por la Universidad Nacional Santiago Antunes de Mayolo, Ancash Perú. Este trabajo tiene como objetivo general conocer los vacíos legales en la norma peruana que imposibilitan la sanción de los Hackers.

Menciona que debe crearse una unidad especializada por parte del ministerio público, hecho que se ha cumplido, pero no se encuentra descentralizada en todo el territorio nacional, actualizar el cuerpo normativo de acuerdo a la realidad peruana, se debe tomar en cuenta también los delitos cometidos en las redes sociales.

Carrillo (2018), para obtener el título de abogado por la Universidad Señor de Sipán, Lambayeque, Perú. Presenta la tesis de tipo cuantitativo sobre la criminalidad informática o criminalidad con uso de tecnología, cuestiona las deficiencias legislativas del país en el ámbito de los delitos informáticos, sobre todo cuando se atenta contra el atributo de integridad de los sistemas informáticos.

En esta Investigación se menciona que delitos informáticos evolucionan constantemente debido a esto ha surgido diferentes modalidades delictivas por el uso de la tecnología, incluso poco después de la promulgación de la Ley 30096 – Ley de Delitos Informáticos. El autor señala que el delito contra la integridad de los sistemas informáticos no se encuentra regulado de manera precisa en este cuerpo normativo, proponiendo la modificación el artículo 4 de esta referida ley.

La modificación de esta ley debe considerar a los medios tradicionales, como por ejemplo la estafa y suplantación de identidad y no dejarlo en el ámbito del puro medio tecnológico en el atentado contra la integridad de sistemas informáticos.

La tesis también apoya la idea que este tipo penal que se analiza debe considerar circunstancias agravantes, cuando este afecta el normal desempeño de los servicios públicos. Estas circunstancias tienen mayor responsabilidad penal y deben ser sancionadas con penas más rigurosas porque causan perjuicios graves a terceros. Además, recomienda al legislador modificar la norma para fijar puntos de valoración de connotación económica a fin de cuantificar el daño ocasionado al sistema informático y también al daño que produce a los diferentes bienes jurídicos que afecta.

Zorrilla (2018), realiza la tesis sobre Inconsistencias y ambigüedades que se encuentran en la ley nº 30096, ley de delitos informáticos, actualizada por la ley nº 30171 que imposibilitan su cumplimiento, trabajo es de tipo cualitativo, presentada para obtener el título de abogado, en la Universidad Nacional de Ancash, Ancash – Perú 2017.

La investigación concluye que la informática se convierte en un medio propicio para el desarrollo de estas modalidades delictivas tradicionales con singularidad énfasis en los delitos patrimoniales. El trabajo menciona la singular importancia del lugar de comisión de estos delitos, destacando la afectación dentro de la empresa, que trasciende lo material e involucra la imagen y confianza de la misma, es por esta razón que existe cifras ocultas de estos delitos, ya que algunas entidades no denuncian para no ver perjudicados su imagen institucional.

El autor señala que dicha ley se superpone a conductas que ya están legisladas en nuestro código penal causando confusión tanto en los operadores de justicia como en los justiciables. Estas ambigüedades implican una mala tipificación de los delitos repercutiendo en un bajo nivel de sentencias en este tipo de delitos.

Esta confusión hace que los agraviados se ven entrampados en la ponderación del delito ocurrido dentro del código penal o de la Ley de delitos informáticos. A la vez menciona que, si bien es cierto que hay una superposición de algunos tipos

penales, pero por otro lado existe una falta tipificación de delitos como los que se cometen en las redes sociales.

Concluye al término del trabajo, que la tipificación de los delitos informáticos es compleja y confusa debido a la poca experiencia en esta área y la creación de nuevos instrumentos legales pueda no tener el resultado esperado, debido que los avances tecnológicos son de constante cambio. También es importante hacer notar la necesidad de desarrollar medios de prueba tecnológicas para este tipo de delitos, por lo que el papel de los peritos juega un papel importante para llegar a sentencias.

Pardo (2018), realiza una investigación de tesis que tiene por objetivo llevar a cabo un análisis sobre el tratamiento jurídico penal que amerita los delitos informáticos que se cometen contra el patrimonio, el ámbito de aplicación fue el distrito Judicial de Lima en el año 2018. Este estudio de tipo cualitativo fue realizado para obtener la licenciatura en derecho por la Universidad César Vallejo, Lima 2018. El instrumento utilizado fue la entrevista la cual fue aplicada a expertos nacionales e internacionales

El autor identifica que existe un vacío en la tipificación del delito contra el patrimonio, debido a que se considera como fraude informático a un conjunto de modalidades delictivas que afectan el patrimonio como la estafa, hurto y sabotaje, por lo que recomienda la tipificación de manera independiente de estas modalidades. Esta deficiencia en la tipificación no permite la sanción por estos delitos. Entre las recomendaciones dadas por el autor menciona que Perú debe suscribir el convenio de Budapest y la creación de la fiscalía especializada en delitos informáticos.

En la actualidad ya ha sido suscrito dicho convenio, como también se encuentra en funcionamiento la fiscalía especializada en delitos informáticos, lo cual no cubre la totalidad de distritos fiscales. Entre las recomendaciones dada por el autor queda pendiente la propuesta en la cual menciona que los delitos informáticos por ser de carácter transnacional deben ser vistos por la Corte Penal internacional y con

respecto a la educación debe formarse a los educandos en todos los niveles básicos de educación de acuerdo a las competencias de cada nivel educativo.

Se puede advertir que en esta investigación se clasifica al sabotaje informático como una modalidad de delito contra el patrimonio, porque se entiende que la destrucción de los datos informáticos tiene un valor económico.

Cotrina (2018), realiza la tesis sobre los principales factores que impiden la correcta aplicación de la reforma de la ley 30096, recogida en la ley 30171, esta tesis de tipo transversal se desarrolló en el año 2016 en la sede judicial Lima Norte**.** Es un trabajo de enfoque cualitativo presentado para alcanzar el título profesional de abogado por la Universidad César Vallejo, Lima 2018

La investigación concluye que no se ha aplicado correctamente la ley de delitos informáticos, principalmente porque no se ha realizado capacitaciones a los magistrados, fiscales y PNP. También menciona que la falta de cooperación internacional puede retardar el proceso de captura y sanción a los delincuentes informáticos.

Montoya (2018), realiza la tesis que lleva por título "Regulación expresa del delito informático de clonación de tarjetas - sede DIVINDAT, 2017", investigación cualitativa realizada para obtener el la licenciatura en derecho por la Universidad César Vallejo, Lima 2018, tiene como objetivo general, conocer cuál es la importancia de tipificar de manera taxativa del delito de clonación de tarjetas en la ley, para adecuar el tratamiento jurídico. Esta investigación expresa que actualmente este tipo de delito se encuentra regulado de manera genérica como fraude informático, por lo que resulta ambiguo al momento de tipificar el delito.

Concluye en base a instrumentos aplicados a especialistas; que se justifica la creación de un tipo penal propio de clonación de tarjetas como se realiza en otros países de manera específica, se menciona en la investigación los casos de México, España y Venezuela. En este sentido finaliza diciendo que la Ley Peruana N° 30096

resulta insuficiente con relación al derecho comparado, ya que solo se regula el fraude informático en forma genérica.

Habiendo revisado la problemática de la utilización de medios informáticos y su influencia en el patrimonio se presenta la (*Tabla 1*) con la información de las propuestas que se tiene para hacerle frente a estos delitos. En primer lugar, los autores coinciden que es imprescindible actualizar la norma de acuerdo a los avances tecnológicos teniendo en cuenta la realidad nacional. Esta actualización debe contemplar la regulación expresa de los artículos como por ejemplo en la clonación de tarjetas.

Conjuntamente con la actualización de la norma se tiene que tener en cuenta que este tipo de delitos se pueden cometer desde cualquier parte del mundo por lo que es importante ser parte activa de los tratados de cooperación internacional en el ámbito informático como el convenio de Budapest. Otro punto a destacar es la capacitación de los operadores de justicia en delitos informáticos, para que los delitos no queden impunes al no poder desarrollar un correcto proceso penal en el reconocimiento del autor del hecho. Y por último y no menos importante se debe realizar la capacitación de la población en general para prevenir ser víctimas de estos delitos.

Tabla 1

Propuesta frente a la problemática de los delitos de fraude informático

Acciones	(Novoa, 2020)	(Cangalaya, 2020)	(Hernández, 2019)	(Mori, 2019)	(Urpeque, 2019)	(Carrillo, 2018)	(Zorrilla, 2018)	(Pardo, 2018)	(Cotrina, 2018)	(Montoya, 2018)	((Vilca, 2018)	(Devia, 2017)	Total
- Actualizar la norma al avance tecnológico y la realidad nacional.	1	1	1		1	1	1				1		7
- Regular expresamente los artículos de la ley de delitos informáticos.					1	1	1	1		1			5
- Considerar agravantes cuando se atenta contra servicios públicos.						1							1
- Considerar límites de los derechos constitucionales relacionados a la intimidad	1												2
- Integrar tratados informáticos de cooperación internacional como el convenio de Budapest	1	1					1	1	1				5
- Capacitar operadores de justicia para aplicar la norma en los tribunales	1	1		1					1		1		5
- Legislar en tenencia de metadatos personales en entidades particulares	1												1
- Capacitar a la población en delitos informáticos			1					1				1	4
- Descentralizar la DIVINDAT y fiscalía especializada		1						1			1		3

Fuente: Elaboración propia

La investigación se enmarca en las siguientes teorías:

La Teoría constitucionalista, respecto al delito informático menciona que solo merece protección cuando este proviene de un valor constitucional, por lo debe de concretarse especialmente en proteger estos bienes. En este sentido se encuentra en la Constitución un conjunto de bienes reconocidos en el ordenamiento positivo, que nacen de un acuerdo entre la sociedad y el Estado para normar la convivencia social. Cabrera (2017)

Teoría clásica, será delito informático la acción que exprese un asunto de tratamiento automático de la información donde se pueda observar que la acción es típica antijurídica y culpable entendiendo la informática como un medio o como un fin. Mientras no cumplan con estos elementos no pueden ser considerados delito informático. Téllez Valdés (2008).

La teoría del bien jurídico, conocida por la protección del bien jurídico como legitimación para la actuación del Estado en materia punitiva. La teoría del bien jurídico tiene como contenido material la lesión o puesta en peligro del bien jurídico protegido en el tipo penal. El bien jurídico en el delito informático es propiamente la información, aunque hay autores que consideran como una modalidad de los delitos tradicionales como el fraude. Zorrilla (2018). El sujeto puede ser cualquier persona con conocimientos básicos de tecnología de información Villavicencio (2014). El sujeto pasivo sobre el cual se realiza la conducta ilícita, puede ser individuos o instituciones que usan sistemas automatizados de información, en el Perú los delitos informáticos sólo se admite la modalidad dolosa. Carrillo (2018). La consumación de los delitos informáticos se puede realizar sin limitaciones desde cualquier país, el delincuente cibernético tiene la posibilidad de ocultar la identidad, lugar y tiempo de los actos ilícitos y siguiendo la teoría del resultado debe ser atendido en la jurisdicción donde haya causado efectos esta acción. Pardo (2018).

Teoría del patrimonio-personalidad, la teoría fue propuesta en 1873 por Charles Aubry y Charles Rau. Para quienes el patrimonio es un conjunto indeterminado de bienes y derechos, a los cuales se debe de sumar las obligaciones y cargas que

pesan sobre la persona. La particularidad sobre estos elementos es que se deben considerar tanto presentes como futuros provistos de “universalidad jurídica”. Gamio (2018).

Estos elementos pertenecen a cada persona de manera que cada quien tiene su patrimonio, en consecuencia, el patrimonio llega a ser la manifestación de su propia personalidad. Por el mismo motivo, el patrimonio no puede ser dividido y es intransferible mientras la persona esté viva, pues de lo contrario sería enajenar su propia personalidad. Siendo la muerte de la persona la que transmite el patrimonio a sus herederos. Extinguiendo el patrimonio del difunto y creando el patrimonio para el heredero. Candelaria (2017).

Esta teoría, llamada clásica o subjetiva, ha recibido críticas en su aplicación a la vida real, mayormente en la distinción entre patrimonio y facultad de conseguir bienes futuros. Esto último indicaría que forzosamente toda persona posee un patrimonio, ya que tienen la posibilidad de adquirirlos a futuro.

Esta idea de patrimonio tiene problemas cuando se refiere a las personas jurídicas puesto que no tienen personalidad, a lo que los autores salvan este inconveniente refiriéndose al término mesa de bienes.

Por otro lado, se tiene la teoría moderna objetivista o del patrimonio-afectación, propuesta por Alois von Brinz y Ernst Beker. Esta teoría propone por el contrario a la teoría clásica que el patrimonio existe por sí solo y no requiere de una persona para existir, estos elementos se encuentran unificados por la afectación a un fin común, en este sentido lo importante del patrimonio es los objetos que lo componen y no la persona. Esta teoría parte de considerar que pueden existir derechos sin un sujeto al que pertenezca. Pazos (2017).

Para el autor, el patrimonio se constituye por bienes, acciones y derechos individualizados en un tiempo y lugar, los cuales están destinados a un fin jurídico económico, diferente a la universalidad jurídica que lo propone la teoría clásica. Gamio (2018).

Por último, es necesario que para la existencia del patrimonio tenga que existir bienes, pudiendo existir el patrimonio sin que pertenezca a alguien, esto facilita el entender del patrimonio empresarial. El patrimonio al estar enmarcado dentro de un tiempo determinado no cuenta la opción de obtenerlo a futuro, siendo importante notar que el patrimonio se considera en un momento dado.

Por otra parte, es importe analizar la temporalidad en la cual se realiza la presente investigación. El Estado de emergencia se encuentra regulada en la constitución de 1993 señala la suspensión o restricción de los siguientes derechos fundamentales libertad de reunión, libertad de tránsito, inviolabilidad del domicilio y seguridad personal. El Estado peruano declara estado de emergencia nacional (DS Nº 044-2020-PCM), para la protección de la salud, en concordancia con el artículo 44 de la constitución el cual señala que es una de la función del Estado garantizar la seguridad frente a las amenazas a la seguridad.

Respecto al marco histórico del delito de fraude informático, se puede mencionar que uno de los primeros ataques en la historia de Internet es creeper (1971), un primer acceso ilegítimo que afectó las computadoras mostrando un mensaje inocuo en toda la red de computadoras conectadas, este suceso fue base para el desarrollo de ataques posteriores, que sí comprometieron pérdidas multimillonarias. Ante estos sucesos uno de los primeros autores que se refirió a los delitos informáticos fue Parker (1976), el que lo define como abusos informáticos y lo precisa como incidentes asociados a la computadora en la que la víctima sufrió un daño y el autor obtuvo un beneficio.

El delito informático en Perú era un agravante del hurto tipificado en el artículo 186 del Código Penal de 1991, esto cambió con la entrada en vigencia de la Ley de Delitos Informáticos Nº 30096 publicado el 22 de octubre del 2013. Con la finalidad de adecuar la Ley 30096 a los estándares internacionales sobre la cibercriminalidad, se promulgó la Ley Nº 30171 el 17 de febrero de 2014 tomando como referencia el convenio de Budapest.

Los Instrumentos internacionales para hacer frente a estos delitos, se encuentra registrado en el Convenio de Budapest del 8 de noviembre de 2001, es un tratado internacional de legislación tipo que conforman los países miembros del Consejo de Europa. Perú se adhiere a este Convenio de Budapest, con algunas reservas que el mismo convenio deja a discreción de los países que se adhieren.

Si realizamos un análisis comparativo entre el Convenio de Budapest y la Ley N° 30096, el fraude Informático y suplantación de identidad descritas en el convenio encuentran su similitud en los artículos 8 y 9 de la Ley N° 30096. Según reporte de Ministerio Público (2021)

Marco Jurídico comparado

España. - Un punto significativo relacionado con los delitos informáticos es la Ley Orgánica 1/2015. En la cual modifica el artículo 26 del Código Penal para incorporar al documento informático como un documento que expresa datos de eficacia probatoria y jurídica. Otro hecho relevante es la aprobación del convenio sobre la ciberdelincuencia de Budapest por la Ley 1928 de 2018

Una jurisprudencia relevante es la sentencia N° 1915/2019 en casación del tribunal supremo por el delito de estafa informática que tiene como agraviado a la empresa "JAM TRADING CO", la cual realizó pagos que no fueron reconocidos por la empresa "CERÁMICA EXPOMED" por un monto de 85,914, porque había sido suplantada vía correo electrónicos, por lo que se encuadra en el tipo penal de estafa tipificada en los artículos 248.1, 248.2 a), 249 y 250.1.5°, sancionando con prisión de hasta dos años, además de manera complementaria se lo inhabilita para el sufragio y una multa de 1,920 euros. Además de la indemnización de 85,900 euros a las empresas afectadas. El motivo de casación que proponía error en la valoración de la prueba informática fue rechazado.

Sentencia 533/2007, Casación 2249/2006, Sala Penal. Delito contra el patrimonio. Por el delito de estafa en la cual se manifiesta NO A LUGAR. Los hechos se refieren a una organización concebida por un menor de edad, este persuade a un grupo de

individuos mayores de edad para abrir cuentas bancarias en España, para trasladar dinero de estafas informáticas realizadas en Estados Unidos, por medio de una página falsa de Citibank. El recurso de casación señalaba que en ninguna circunstancia se realizó el engaño porque no sabían a qué fin estaban destinados las cuentas, a lo que el tribunal entiende que en caso de empleo informático no es preciso la concurrencia de engaño por una persona, sino basta con el medio informático.

Sentencia 738/2000 referente a tarjetas de crédito el Tribunal Supremo español alude que no se puede tildar como estafa el pago efectuado con una tarjeta de crédito que no pertenece al sujeto que efectuó la compra, se considera como actuación diligente del vendedor porque no verificó al momento de efectuar la compra. Así mismo la Audiencia Provincial de Málaga del 19 de diciembre de 2005, si bien es cierto utilizaron una tarjeta ajena pero no manipularon un sistema informático por lo que no se puede aplicar el tipo penal.

México. - En el Código Penal Federal de México reformado y publicado el 25 de enero del año del 2013, se encuentra en el segundo libro, título Noveno del código penal, capítulo uno, publicación de secretos y entrada ilícita a sistemas y equipos informáticos, en el cual se dispone la protección de las comunicaciones a través de tecnologías.

Artículo 211 Bis. A quien dé a conocer, publique o use en forma indebida información o imágenes o en detrimento de un tercero, conseguidas en una intervención de comunicación privada, será pasible de sanción de un mínimo de seis y un máximo de doce años de prisión y de trescientos a seiscientos días multa.

En el capítulo tres, se describe la entrada indebida a sistemas y equipos informáticos, artículo 211 bis1. El que sin consentimiento altere, destruya o cause perjuicio en la información almacenada en sistemas o equipos informáticos provistos de protección de dispositivo de seguridad, se le sancionará de seis meses a veinticuatro meses de pena privativa de la libertad y de cien a trescientos días multa.

El fraude informático regulado en el Artículo 231. XIV. Para conseguir un provecho para un tercero o para sí mismo, acceda por cualquier medio, introduciéndose a los sistemas o programas informáticos del sector financiero y fraudulentamente efectúe movimientos o transferencias de dinero o valores, ya sea interno o externo a la institución.

Brasil. - Los delitos informáticos se encuentran tipificados en la Ley núm. 12737 del año 2012, que dispone sobre la tipificación criminal de los delitos informáticos modificando el Código Penal los artículos 154-A, 154-B, 266 y 298.

Se sanciona el acceso no autorizado a computadores enlazados a internet, mediante la violación de sus dispositivos de seguridad. El robo de credenciales y contenidos de correos electrónicos. Colapsar con intención un sitio Web. La incursión de aparatos electrónicos extraños con el "objetivo de conseguir, modificar o destruir el almacenamiento de datos o información". La elaboración y distribución de aparatos que permitan invadir dispositivos móviles inteligentes o tabletas electrónicas. La adquisición ilegal de datos bancarios por vías electrónicas. Además, cabe señalar el país cuenta con ley de internet que pretende regular las transacciones que se realizan por esta vía mediante decreto reglamentario 771-2015.

Chile. - El país latinoamericano que fue el pionero en decretar una Ley contra Delitos Informáticos. El 7 de junio de 1993 La ley 19223 fue publicada en el Diario Oficial de Chile, señalando tipo penales como la destrucción o anulación de un sistema de información, acceso ilegítimo al sistema, virus informático, afectación a datos almacenados en los registros del sistema. Solo se pena el cracking, cuando se ingresa a un sistema con el ánimo de apoderarse o interferir su normal funcionamiento, como hacer uso de manera indebida de esta información almacenada, siendo pasible de pena de prisión de cinco años. La modalidad de hacking, es decir al entrar al sistema sin consentimiento, siempre que las intenciones no sean de divulgar su contenido no constituye delito. Divulgar información guardada en un sistema puede ser sancionado con pena privativa de

la libertad de hasta tres años, pero si el que lo hace es el responsable de dicho sistema puede aumentar a cinco años. No está contemplado la estafa informática (Künsemüller, 2017).

El Tribunal de apelaciones de Santiago convalidó la sentencia N° 44.191–2017 del Tercer Juzgado de Policía Local, en la cual se sanciona al Banco de Chile a abonar una multa de $500.000 a estudiante que fue víctima de fraude informático en su modalidad de phishing (suplantación de identidad), deja establecido que existen defectos en el sistema de seguridad del Banco de Chile, lo que el banco no negó en su oportunidad

La Corte Suprema de Justicia de Chile por los casos de la empresa Comercial Agrícola e Industrial Novapro Spa dejando en claro que la responsabilidad de la custodia es del banco, debiendo éste implementar de las medidas para salvaguardar las claves digitales garantizando la seguridad, esto siempre y cuando se ingresa a las páginas oficiales del Banco. Caso distinto caso Melipilla cuando se ingresa a una página falsa de un banco, por lo que no se trata de una vulneración de la seguridad del sino un ardid tramado por un tercero para obtener las claves de seguridad.

III METODOLOGÍA

3.1 Tipo y Diseño de Investigación

Tipo de investigación

La presente investigación es de tipo aplicada, porque usa o aplica fundamentos de la investigación a fin de sustentar y enriquecer el carácter utilitario y práctico del trabajo.

Diseño de investigación:

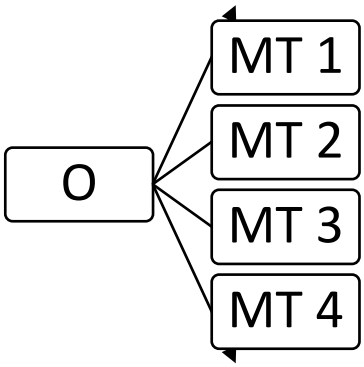
El diseño de la tesis es no experimental, se observa los fenómenos en su entorno natural, no se manipula intencionalmente la variable dependiente para ver sus efectos.

Es de tipo transeccional o transversal en virtud de que los datos que se recogerán en un solo momento.

Es correlacional – causal porque busca conocer cómo puede comportarse una variable respecto a la otra. Así estos diseños describen relaciones entre dos o más variables en un momento determinado. En esta razón se busca el grado de influencia del “fraude informático” (causa) en la protección del patrimonio” (efecto).

El enfoque es cuantitativo, porque se busca establecer la influencia de la variable fraude informático sobre la protección del patrimonio en tiempos de pandemia, y de acuerdo a Hernández (2018) este enfoque utiliza la recolección de datos para probar la hipótesis con sustento de análisis estadístico.

La simbología para efectos de la investigación es la siguiente:

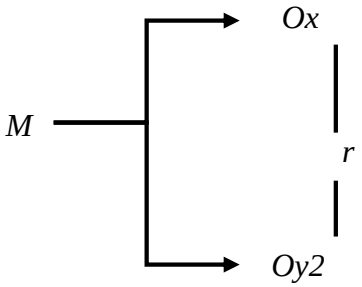


En donde:

MT: Muestra de estudio.

O: Observación de las muestras.

Diagrama Simbólico Correlacional:



En donde:

M= Tamaño de la muestra.

Oy2= Observación de la variable dependiente.

Ox1= Observación de la variable independiente

3.2 Variables y operacionalización

Fraude informático

Es toda acción dolosa que conlleva un perjuicio a personas naturales o jurídicas utilizando de forma activa dispositivos informáticos y que afecta el patrimonio. En este aspecto las conductas sólo pueden ser cometidas por medio de la tecnología afectando directamente derechos y libertades de naturaleza patrimonial. Villavicencio (2014)

El fraude informático se debe entender como una ampliación del modo delictivo tradicional, una especialización delictiva en un contexto particular que se comete en el ciberespacio. Mediante el uso de medios informáticos el sujeto activo atenta contra del sujeto pasivo con el propósito de despojarlo de su patrimonio. Entre las modalidades más comunes de fraude informático se encuentran la estafa informática. Posada (2017).

La ciberdelincuencia comprende delitos como el fraude informático cuando las herramientas utilizadas para cometer estos ilícitos son equipos informáticos. Estos delitos logran ser cometidos en parte por falta de conocimiento de las técnicas de estafa en internet, por negligencia o curiosidad. Mesa (2017).

La postura tradicional niega la existencia del fraude informático como un nuevo delito independiente, sino más bien con un nuevo modus operandi de los delitos tradicionales que se ven empoderados con el desarrollo de la tecnología. Mayer (2020). Aunque parezca anticuado el gran número de fraudes justamente se comente en modalidades que hacen uso de perfiles falsos, páginas en Internet que se asemejan a bancos o tiendas. Almeida (2017).

Como se ha podido revisar en todas las definiciones de los distintos investigadores a lo largo del tiempo, el hilo principal es el desempeño de la informática como un medio para perpetrar ilícitos penales, afectando bienes jurídicos como el patrimonio. Mori Quiroz (2019)

La Ley Nº 30096-2013 hace referencia al fraude informático, como la procura deliberada e ilegítima de un provecho ilícito que causa perjuicio a un tercero. Esto se realiza mediante el diseño informáticos, introducción o alteración de datos al sistema informático, borrado o supresión de datos de un sistema, clonación o copia de datos informáticos, que tiene como fin el deterioro del patrimonio de la víctima.

Se ha generado confusión al momento de interpretar esta figura delictiva al confundirse con los delitos contra datos y sistemas informáticos, por la similitud de los verbos rectores que describen este delito como “diseñar, introducir, alterar, borrar y suprimir” los mismos verbos puede encontrarse en el delito de daño, lo que causa que los alcances de la imputación no sean claras cuando se enfrenta un delito de fraude informático. Una particularidad de este último es que exige un perjuicio patrimonial a un tercero por ser un delito de resultado, este delito también admite el grado de tentativa. Villavicencio (2014).

El phising

Es la técnica preferida de los delincuentes para efectuar estafas y obtener información reservada fraudulentamente, el término inglés significa salir de pesca, llamada así porque se espera que la víctima muerda el anzuelo. Una de las primeras modalidades es la estafa informática, está relacionado con conductas de ingeniería social donde los delincuentes se valen de sus capacidades persuasivas para despojar de su patrimonio. Hidalgo (2021).

Mediante técnicas de engaño se instrumentaliza la informática para enviar correos electrónicos, mensajes de texto fraudulentos o llamadas telefónicas suplantando la identidad de funcionarios del banco, a fin que la víctima le proporcione información confidencial como número y contraseña de tarjeta de crédito con la finalidad de generar un perjuicio económico, ya que una vez obtenidos los datos verdaderos sustraen o transfieren el dinero. Vinelli (2021).

Las modalidades del phishing han ido perfeccionando dependiendo cada vez menos de las habilidades de persuasión, y más de las capacidades técnicas del agente, de manera que se puede señalar como típicos casos de fraude informático

la clonación de tarjetas de crédito y las réplicas de páginas que se asemejan casi a la perfección a los, modalidad que se conoce como pharming. Enmarcándose estas acciones en los verbos rectores “diseñar, introducir, alterar, borrar y suprimir”. Mayer (2020).

El phishing tiene como modo de operación el envío de supuestos ofrecimientos de naturaleza económica a través de links contenidos en medios electrónicos que, invitan a llenar datos personales, para que con esta información afecten el patrimonio de su víctima, tomando conocimiento estos últimos del delito cometido tan solo al momento de revisar su estado de cuenta. Esta técnica también es conocido como robo de identidad. Hancco (2017).

Transferencias electrónicas fraudulentas

En las transferencias electrónicas fraudulentas o no consentidas no existe un bien físico objeto de sustracción, sino que para efectuar la transferencia económica se realiza una manipulación informática dolosa que ocasiona un perjuicio a la víctima. Suele tener como objetivos negocios que funcionan a través de una página web, usa la transferencia bancaria como método para hacerse con nuestro dinero. Vinelli (2021).

En la Transferencia electrónica fraudulenta existe una manipulación o artificio informático a fin de conseguir la transferencia no consentida de algún activo en detrimento de un tercero. Estas operaciones automáticas son realizadas por sistemas informáticos como resultado directo de manipulaciones defraudadoras desarrolladas o ejecutadas por el sujeto activo. La transferencia se diferencia de la estafa, pues el sujeto pasivo (víctima) sobre el cual recae la acción en nada interviene durante la producción del perjuicio patrimonial que es originada a raíz de una transferencia automática de activos. Posada. (2017)

Estas transferencias son realizadas una vez el timador haya obtenido mediante el phishing información sobre las claves de seguridad para acceder a cuentas bancarias de la víctima. La transferencia bancaria se realiza por lo general a cuenta

de terceros que son conocidos como muleros quienes son los que proporcionan sus cuentas bancarias por un monto mínimo de dinero, estas personas por lo general no participan en las fases previas. Hidalgo (2021)

Cuando se habla de transferencias electrónicas ilegales están involucradas principalmente las transferencias bancarias que se realizan de manera inmediata a través de los diferentes canales de servicio de la entidad financiera, tanto las páginas web como los aplicativos móviles. Otro punto que se tiene que tomar en cuenta son las estafas que se cometen con tarjetas de crédito, al utilizar la tarjeta de manera fraudulenta se genera una transacción electrónica de deuda que tiene que asumir la víctima. Por estas razones cobra mayor importancia la ciberseguridad Huayre (2021)

En cuanto a la jurisprudencia en territorio nacional de los delitos informáticos se debe señalar la sentencia 100/2020 del pleno del tribunal constitucional, expediente 01189-2019-PHC/TC recurso de agravio constitucional contra la Segunda Sala Penal para Reos Libre de la Corte Superior de Justicia de Lima por haber declarado no procedente un recurso de habeas corpus. Esta demanda de Hábeas corpus se interpuso contra la sentencia de la Primera Sala Penal de la Corte Superior de Justicia de Lima Norte por condenar falsificación de firma en documento privado y delitos de fraude informático. Se argumenta violación en los derechos del debido proceso, a la libertad personal, a la tutela jurisdiccional efectiva, como también al principio de legalidad al señalar que se condenó por un tipo penal que no estaba vigente a la fecha que se suscitaron los hechos, puestos estos fueron cometidos entre los meses enero y octubre de 2013, a pesar de ello fue condenado por la Ley 30096, que entró recién en vigencia recién el 23 de octubre de 2013. La procuraduría hace su descargo indicando que la condena interpuesta por los jueces fue por hechos cometidos en el 2014 estando en vigencia la ley en cuestión. Los hechos que se imputan es haber sustraído de forma sistemática. 194,934.69 soles de la Caja Municipal de Ahorros y Crédito de Trujillo aprovechando su posición del cargo que ejercía en la misma. Después del debate constitucional se declara infundado el recurso de habeas corpus, al comprobarse que los hechos se habían realizado el 2014.

La sentencia N.° 2041-2018, Sala penal permanente, Corte suprema de justicia de Lima, sobre titularidad de actor civil en fraude informático reposa en el afectado del delito siendo el ministerio público puede formular pretensión de oficio cuando el afectado no se apersona. Los hechos imputados son la conformación de una asociación ilícita dedicada a perpetrar fraudes informáticos, provistos de hardware y software que les posibilitaron extraer las cuentas y claves bancarias de las víctimas. Es así que ingresan a las cuentas de la empresa Selme S. A. C. en el Banco continental y realizan una transferencia electrónica por 4800 soles, por medio del canal Banca por internet. La fiscal superior de Lima formula acusación contra los imputados por el delito de fraude informático artículo 8 de la Ley 30096. Habiendo sido probado el hecho del fraude informático, la pretensión impugnativa de los imputados sobre la reparación civil de los imputados al no poder pagarlo por no contar con los medios económicos y además que aceptó la condena por la economía procesal y dar por concluido el proceso sumado a que solo dio su número de cuenta para otros propósitos. Ante esto solo la procuraduría formula oposición de los montos de reparación civil, no haciendo lo mismo la parte agraviada. En la decisión final, al haber oposición de parte del estado se deja con el mismo monto de la resolución y al no presentarse la parte agraviada se reduce a la cuarta parte el monto indemnizatorio.

En la (Tabla 2) se muestra las jurisprudencia en delitos informáticos analizados en la presente tesis.

Tabla 2

Jurisprudencia delitos de fraude informático

Instancia	Expediente	Antecedentes	Recurso	Delito	Resolución
Tribunal Constitucional	01189-2019 PHC/TC	Por haber declarado improcedente un recurso de habeas corpus. Supuesta violación al principio de legalidad penal al condenar por un tipo penal que no estaba vigente al momento que se cometieron los hechos	Habeas corpus	Fraude informático y falsificación de firma en documento privado.	Infundado
Corte suprema	R.N.N. 2041-2018	La titularidad del objeto civil reposa en el afectado por el delito. Pero cuando este no se apersona el Ministerio Público debe realiza la petición del monto indemnizatorio.	Recurso de nulidad	Fraude informático y asociación ilícita para delinquir	No haber nulidad para ministerio Haber nulidad para la empresa

Fuente: Elaboración propia

Patrimonio Económico

El patrimonio bajo la concepción económica, representa la suma de los bienes con valor dinerario de una persona y sobre los cuales se puede ejercer el derecho de propiedad. La configuración del perjuicio patrimonial bajo este enfoque del patrimonio se da cuando existe una disminución del saldo contable. Schlack (2008)

Según la teoría de la pertenencia, la propiedad es la conexión entre una persona y una cosa, atribuyendo a la persona todas las facultades sobre el bien. Se tiene sobre el bien las facultades de usar, gozar, disponer y reivindicar, solo con las restricciones que se presentan en la ley. Rospigliosi (2019).

Una definición de propiedad la encontramos en el artículo 923 del Código Civil, en la cual la señala como la potestad en lo jurídico que tiene la persona la cual le permite usar el bien para lo que fue concebido, disfrutar de los frutos que produzca el bien, disponer tanto material como jurídicamente del bien y reivindicar un bien a su legítimo propietario si algún tercero se encuentra ilegítimamente en posesión,

debiendo realizarse en conformidad con el interés de la sociedad y dentro del ámbito la ley. (Código Civil, 1984).

Estos cuatro atributos representan de mejor manera la filosofía humanista de la propiedad, al establecer que los bienes están al servicio de la persona, por lo que ejerce pleno poder sobre la propiedad dentro de los límites de la ley. (Rospigliosi, 2019). En este sentido Harvey (2017) al referirse a la propiedad en entornos virtuales, como cualquier clasificación de propiedad tangible e intangible, real y virtual otorga el derecho de usar, excluir a otros y enajenar o transferir objetos. Atributos de la propiedad que a continuación se describe.

Uso o ius utendi; este atributo se hace presente cuando el bien es utilizado para lo cual existe de acuerdo a su naturaleza o destino, antes el propietario debe ejercer el derecho de poseerlo. Por ejemplo, se usa una casa morando en ella, se usa un vehículo como medio de transporte. En el caso de bien consumible esta característica se ejecuta junto con la de disfrute. Gonzales (2015)

Goce o disfrute ius fruendi, este atributo es donde la propiedad adquiere contenido económico y social, y como consecuencia se generan los conflictos sociales por los frutos de bien. Cuando se trata de un consumible el uso está incluido en el disfrute del bien, esto es en su consumo. Rospigliosi (2019).

Disposición o ius abutendi, hace referencia a la disposición de bien tanto en lo material como en lo jurídico, por lo que puede disponerse a plena voluntad y libertad del bien por parte del propietario ya sea consumiéndose, afectándolos, desmembrándose o desprendiéndose de ellos a título oneroso o gratuito siempre en marco de la ley. Gonzales (2015)

La reivindicación o ius vindicandi, este atributo faculta al propietario a recurrir a los tribunales para reclamar su propiedad para evitar que un tercero pueda entrometerse. Por la vindicatio se entiende que el propietario tiene como objetivo el retorno del bien de manos extrañas que lo posee sin causa jurídica justa. Los requisitos para la acción de reivindicación son: que el propietario sea el

demandante, que el bien esté individualizado y que el bien esté en posesión del demandado. Rospigliosi (2019).

El derecho de propiedad concierne de manera universal a todo ser humano; los que se encuentran capacitados para usar y disponer con libertad de sus bienes como también transferirlos por herencia o donación. En el histórico caso “Campbell vs Holt” deja sentado la idea de que la propiedad en el ámbito constitucional abarca más que el contenido que le otorga el derecho civil. En el derecho civil la propiedad constituye objetos materiales capaces de ser valorados económicamente, para el orden constitucional se extiende y abarca toda la variedad de bienes materiales e inmateriales, por lo tanto, son aptos de valoración económica. En este sentido el constitucionalista argentino Gregorio Badeni (1997) comenta “la propiedad engloba bienes e intereses de apreciación económica que pueda gozar una persona”.

El artículo 70° de la Constitución señala que la propiedad no puede ser quebrantada en sus aspectos de uso, goce y disposición tanto por terceros como por el Estado Gonzales (2015). El derecho de propiedad a la vez que reconoce el derecho real de la propiedad, también queda comprendido la propiedad inmaterial, esto es para todos los bienes que son susceptibles de apreciación económica de acuerdo a lo dictaminado en la sentencia emitida por el tribunal constitucional en expediente Exp. 00008-2003-AI FJ 26, en la que refiere que el patrimonio de una persona lo integra tanto la propiedad material como inmaterial.

La cuenta bancaria en internet como toda propiedad está facultada por el derecho de uso, disfrute y disposición. Si bien es una propiedad intangible no imposibilita que exista y que pueda ser apreciado económicamente generando derechos sobre estos. Cuando hablamos de propiedad en entornos virtuales, existen nuevos retos que el derecho tiene que enfrentar en torno a internet debido que este en un medio propicio para la violación de los derechos de propiedad. Harvey (2017).

El goce del bien

Entonces se puede entender por protección del patrimonio en internet en apartar del dominio de terceros, información de carácter personal. Tratándose de

información de la cuenta bancaria se debe proteger limitando su acceso solo a los que tienen el derecho de poseerla. Esta acción de limitar el acceso a terceros hace recordar a la confidencialidad como uno de los pilares de la seguridad de la información, la cual limita la intromisión a terceros, contribuyendo a preservar la integridad y disponibilidad de la misma. Boza (2015).

Si la propiedad se encuentra en internet debe implementarse mecanismos de seguridad para gozar del bien con integridad de la información. Se debe proteger la información protegiendo los alojamientos y dominios web en los que se encuentra la información. Mendoza (2018).

En tal sentido, la apropiación de datos de carácter confidencial como el número de la cuenta bancaria de manera fraudulenta, vulnerando medidas de seguridad se entiende como un delito que afecta el goce del patrimonio. Tenorio (2018).

El dinero en el entorno financiero es un bien inmaterial y se constituye como un activo inmaterial. Este dinero inmaterial, es originado a raíz de operaciones crediticias de débito y crédito efectuadas por la banca y el cliente. Las operaciones de estos fondos se realizan a través de las transferencias electrónicas, los cuáles no son en sí una transferencia de recursos sino una creación y extinción de valor monetario. Boada (2019).

La disposición del bien

Es la mayor expresión de poder que ejerce el titular, pues le da la potestad de ceder, destruir, limitar, enajenar o gravar un bien. En este sentido, la propiedad es perpetua debido a que el bien pertenece de forma indefinida a su titular, con excepción que él mismo, haciendo uso de su facultad de disposición, decida desprenderse de él. Rospigliosi (2019)

Es función del Estado proteger la propiedad aun cuando se encuentre en un medio tecnológico, debe garantizar que no se perjudique la información personal que pueda proporcionar los servicios informáticos de naturaleza pública o privada,

salvaguardando información relevante para el ciudadano. Constitución Política del Perú artículo 2, inciso 6.

La jurisprudencia de protección a la propiedad en Perú, se encuentra en la sentencia recaída en el Exp. 00008-2003-AI FJ 26 en la cual referencia al derecho de propiedad en el artículo 2°, inciso 16 de la Constitución, es proyectado como la potestad legal que posibilita a una persona usar, disfrutar, disponer y reivindicar un bien. En este modo podrá aprovechar de manera directa o recibir los frutos de su bien y de acuerdo a su conveniencia darle destino, toda vez que realice estas actividades dentro del bien común y los linderos señalados por la ley; pudiendo recobrarlo si algún tercero se ha apoderado de él sin tener algún derecho. La propiedad no solo comprende el ámbito de lo bienes reales sino también comprende el ámbito de lo inmaterial, en cuanto pueda ser apreciado económicamente.

En la sentencia 00011-2010-PI/TC, invocando al artículo 2°, inciso 16 y el artículo 70 de la constitución, menciona la inviolabilidad del derecho de propiedad y la garantía del Estado para tal fin. Deja sentado que este derecho no se encuentra libre de restricciones, no estamos frente un derecho absoluto, debido que se halla restringido por disposiciones constitucionales taxativas o por restricciones implícitas. Una de las limitaciones del derecho de propiedad es la expropiación.

En la (Tabla 3) se muestra la jurisprudencia de la protección del patrimonio analizados en la presente tesis

Tabla 3

Jurisprudencia protección del patrimonio

Instancia	Expediente	Fundamentos	Recurso	Resolución
Tribunal Constitucional	Exp. 00008-2003-AI FJ 26	Derecho propiedad La propiedad no queda encerrada en el marco de la pertenecía de los derechos reales, sino que abarca la variedad de bienes materiales e inmateriales.	Acción de inconstitucionalidad	fundada
Tribunal Constitucional	Exp. 00011-2010-PI/TC	Derecho propiedad Este derecho no se encuentra liberado de restricciones, por lo que no es un derecho fundamental absoluto	Acción de inconstitucionalidad	fundada

Fuente: Elaboración propia

3.3 Población, Muestra y Muestreo

Población

La Población está constituida por 50 personas de la Distrito Fiscal de Lima Este

Muestra

Se procede con la fórmula de la muestra, con una población de 50.

n = muestra

N = población

E = margen de error (+/- 5%=0.05)

z = nivel de confianza (95% =1.96)

p = probabilidad a favor (0.5)

q = probabilidad en contra (0.5)

$$n = \frac{z^2 p\ q\ N}{(E^2(N-1) + z^2\ p\ q}$$

Este es el tamaño de la muestra

M = Muestra 44 sujetos de estudio.

3.4 Técnicas e instrumentos de recolección de datos

Se usará como técnica la encuesta que tiene como propósito encontrar la información que se requiere y como instrumento un cuestionario de preguntas cerradas para el recojo de datos.

Con los datos obtenidos elaboramos una base de datos que fueron analizados y discutidos para obtener las conclusiones y recomendaciones.

3.5 Procedimientos

Se hará uso de la elaboración de un cuestionario en internet en la aplicación Google Forms Se solicita consentimiento para realizar encuestas a la Presidencia de la Junta de Fiscales Superiores del Distrito Fiscal de Lima Este. Posteriormente el enlace fue enviado por correo a las fiscalías Provinciales.

3.6 Métodos de análisis de datos

Los datos se procesaron en Excel, la presentación de resultados se realizó mediante tablas y gráficos haciendo uso de la estadística descriptiva. El instrumento se validó por juicio de expertos. La confiabilidad se evidenció realizando la prueba de Alfa de Crombach a una encuesta del 30% registrando un valor de 0.88

3.7 Aspectos Éticos

La investigación respeta los derechos fundamentales de la persona, no plantean juicios morales sobre las variables a investigar.

Se ha ceñido a la estructura señalada por la Universidad César Vallejo utilizando las normas APA, séptima edición la que nos permite citar los antecedentes del presente estudio como también las teorías en las que se fundamenta.

De esta manera la investigación cumple con la originalidad y las Políticas anti plagio que promueve esta casa de estudios.

IV. RESULTADOS

El presente estudio tuvo como objetivo principal determinar de qué manera el "fraude informático incide en la protección del patrimonio en tiempos de pandemia" en el Distrito Fiscal de Lima Este, periodo 2021. Se obtiene los resultados de la variable independiente y sus dimensiones y de la misma manera de la variable dependiente.

Variable Fraude Informático

De un total de 30 puntos que puede obtener por cada encuestado como máximo en la valoración de la variable "fraude informático", los 44 encuestados hicieron una media de 24.64 y, una desviación estándar 3.20 unidades. (*Tabla 4*).

En este sentido, se puede anotar un total de 15 puntos por cada una de las dimensiones de esta variable. La media con valor más bajo se encontró en la dimensión transferencias electrónicas fraudulentas y la más alta en la dimensión phishing. Es decir, el phishing es la dimensión que más incide del fraude informático que afecta a la protección del patrimonio en tiempos de pandemia.

Tabla 4

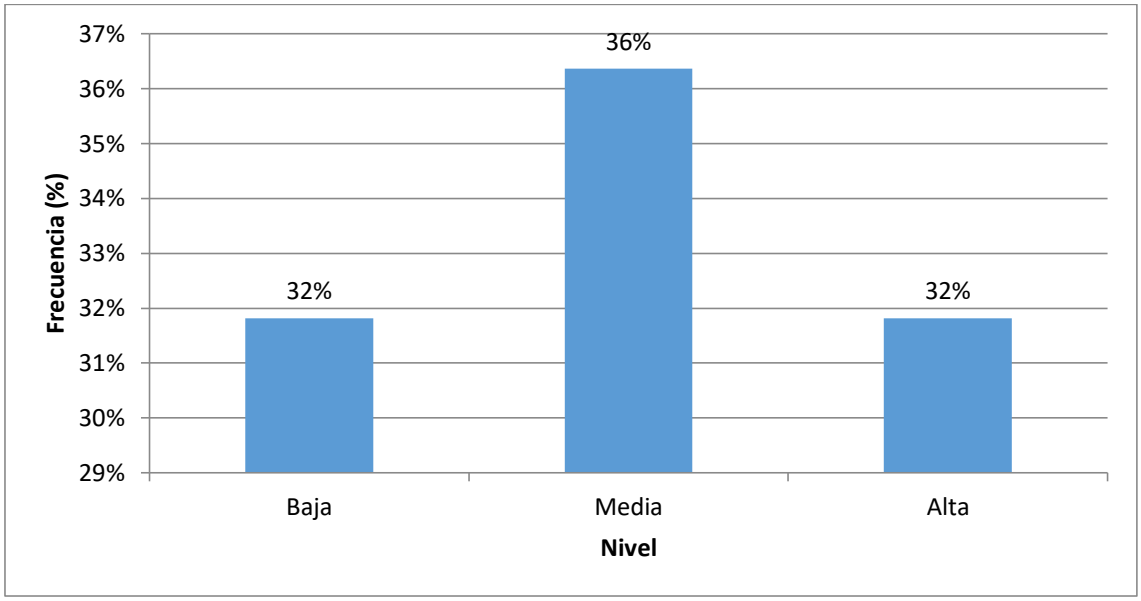
Medidas estadísticas de la variable "fraude informático" y sus dimensiones

Variable/ Dimensión	Promedio	Desviación Estándar	Moda	Máximo	Mínimo	Rango
Fraude informático	24.64	3.20	20	30	18	12
Phishing	12.43	1.69	12	15	8	7
Transferencias electrónicas fraudulentas	12.20	1.82	12	15	9	6

Fuente: Elaboración propia

Figura 3

Frecuencia Porcentual de la Variable Fraude Informático



Nota. Aplicación de escala valorativa o Baremo para presentación de resultados

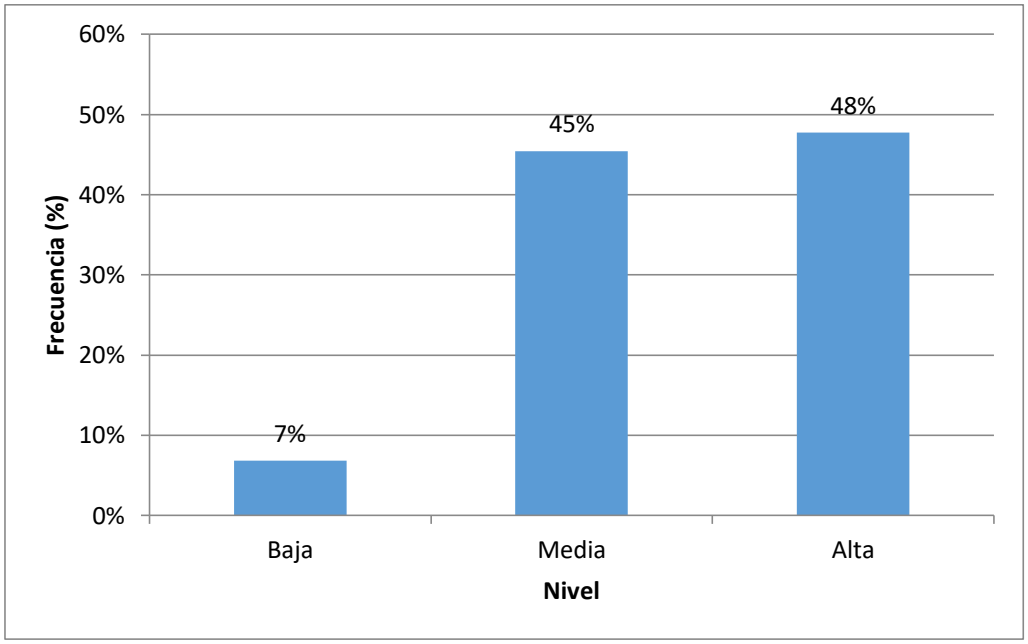
Interpretación

Como podemos observar en la (Figura 3), los encuestados respondieron mayoritariamente que la variable fraude informático incide sobre la variable protección del patrimonio en un nivel medio con una frecuencia del 36%. Además, consideraron los niveles de incidencia tanto alto como bajo con un 32% cada uno.

Dimensión phishing, de la variable fraude informático

Figura 4

Frecuencia Porcentual de la Dimensión Phishing



Nota. Aplicación de escala valorativa o Baremo para presentación de resultados

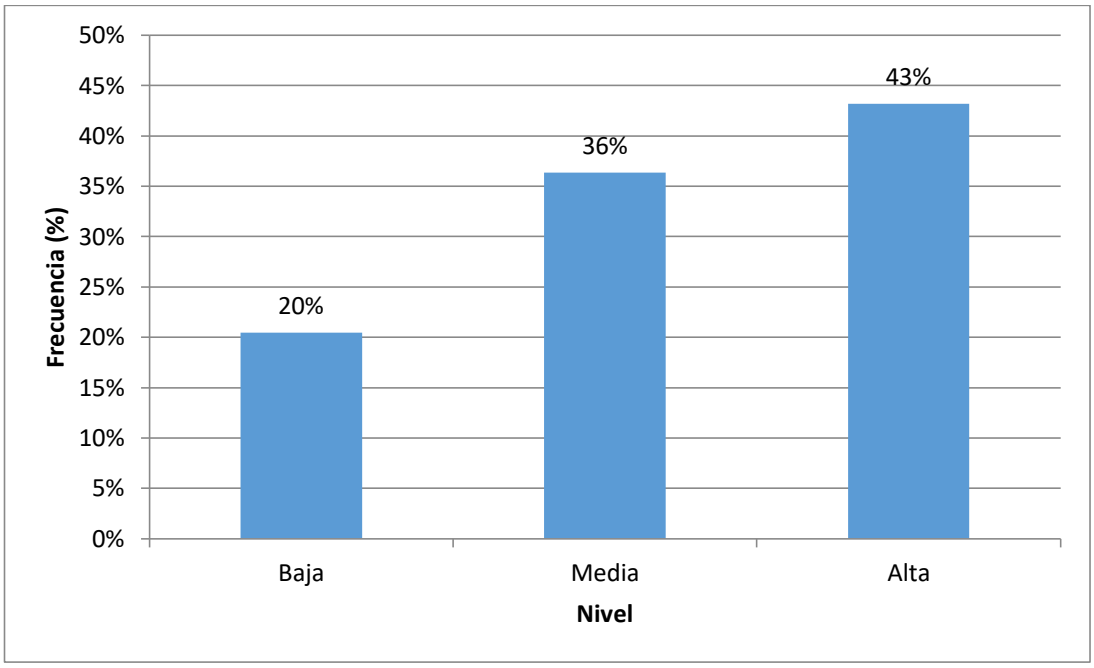
Interpretación

Como podemos observar en la (Figura 4), los encuestados respondieron mayoritariamente que la dimensión phishing de la variable fraude informático inciden es un nivel alto sobre la variable protección del patrimonio con una frecuencia del 48%. Además, consideraron que incide en un nivel medio 45% de los encuestados y finalmente solo un 7% considera una influencia baja.

Dimensión de Transferencias electrónicas fraudulentas, de la variable fraude informático

Figura 5

Frecuencia Porcentual de la Dimensión de Transferencias Electrónicas Fraudulentas



Nota. Aplicación de escala valorativa o Baremo para presentación de resultados

Interpretación

Como podemos observar en la (Figura 5), los encuestados respondieron mayoritariamente que la dimensión Transferencias electrónicas fraudulentas de la variable fraude informático incide sobre la variable protección del patrimonio en un nivel alto con una frecuencia del 43%, Además consideraron que incide en un nivel medio 36% de los encuestados y bajo cada uno con 20%.

Variable Protección del patrimonio en tiempos de pandemia

De un máximo de 30 puntos que puede obtener en el cuestionario por cada encuestado en la “Protección del patrimonio en tiempos de pandemia”, la respuesta de los 44 hicieron una media de 24.57 y, una desviación estándar 3.17 unidades. (*Tabla 5*).

Entonces, se puede conseguir un total de 15 puntos por cada una de las dimensiones de esta variable. La media más baja representó la dimensión disposición del bien y la más alta en la dimensión derecho de goce de bien. Es decir, el derecho de goce de bien es afectado en mayor medida por el fraude informático.

Tabla 5

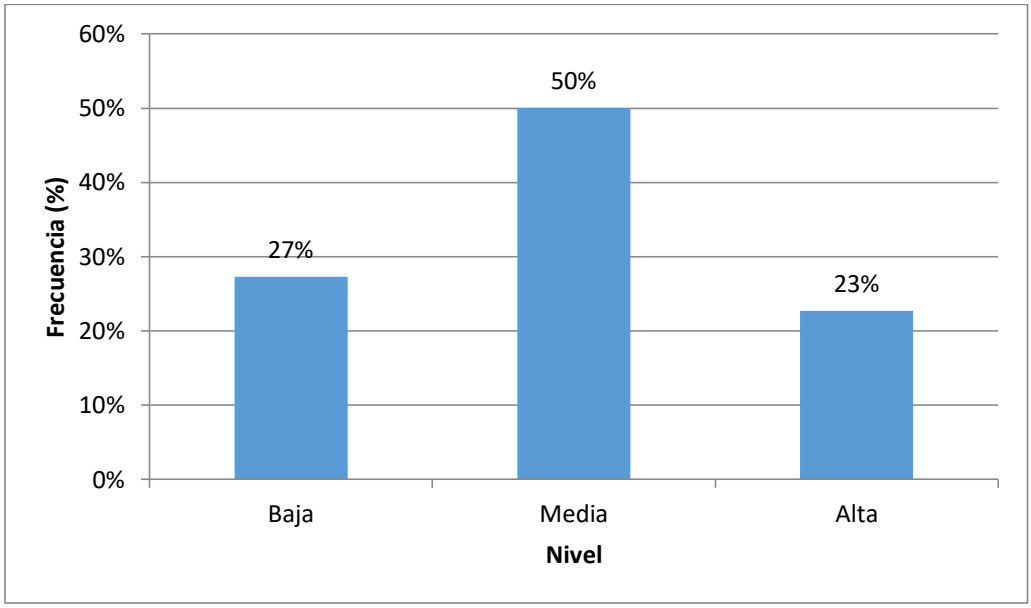
Medidas estadísticas de la variable “Protección del patrimonio en tiempos de pandemia” y sus dimensiones

Variable/ Dimensión	Promedio	Desviación Estándar	Moda	Máximo	Mínimo	Rango
Protección del patrimonio en tiempos de pandemia	24.57	3.17	21	30	18	12
Derecho de goce de bien	12.55	1.44	12	15	9	6
Disposición del bien	12.02	2.03	12	15	9	6

Fuente: Elaboración propia

Figura 6

Frecuencia Porcentual de la variable Protección del Patrimonio en Tiempos de Pandemia



Nota. Aplicación de escala valorativa o Baremo para presentación de resultados

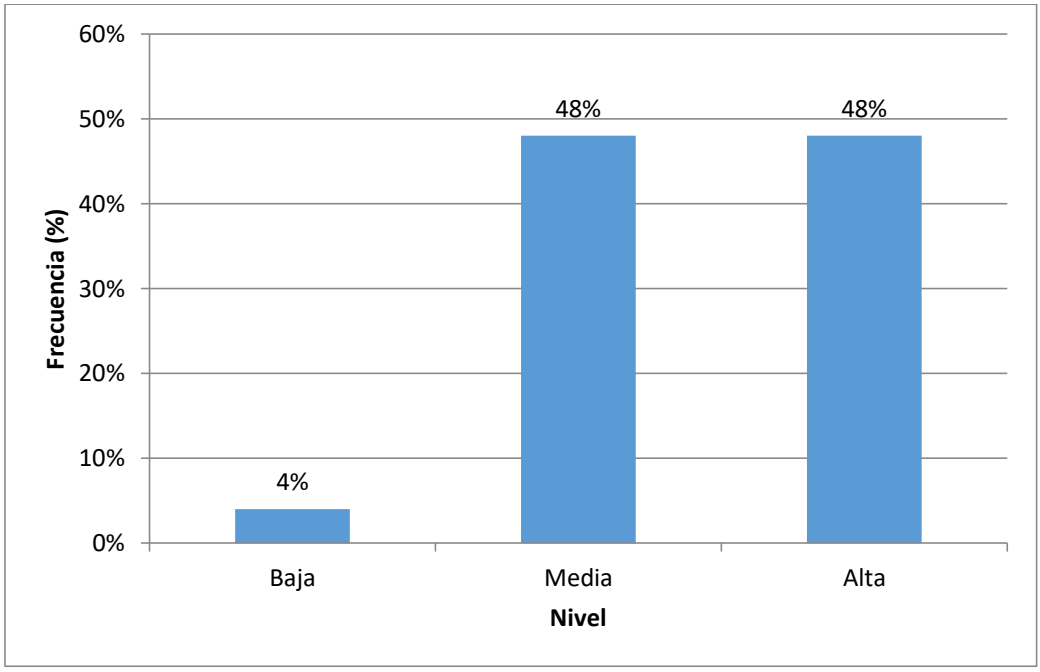
Interpretación

Como podemos observar en la (Figura 6), los encuestados respondieron mayoritariamente que la protección del patrimonio es afectada por la variable fraude informático en un nivel medio con una frecuencia del 50%. Seguido de los niveles de afectación bajo con 27% y del nivel de afectación alto con 23%.

Dimensión “derecho de goce del bien”, de la variable protección del patrimonio en tiempos de pandemia

Figura 7

Frecuencia Porcentual del Derecho de Goce del Bien



Nota. Aplicación de escala valorativa o Baremo para presentación de resultados

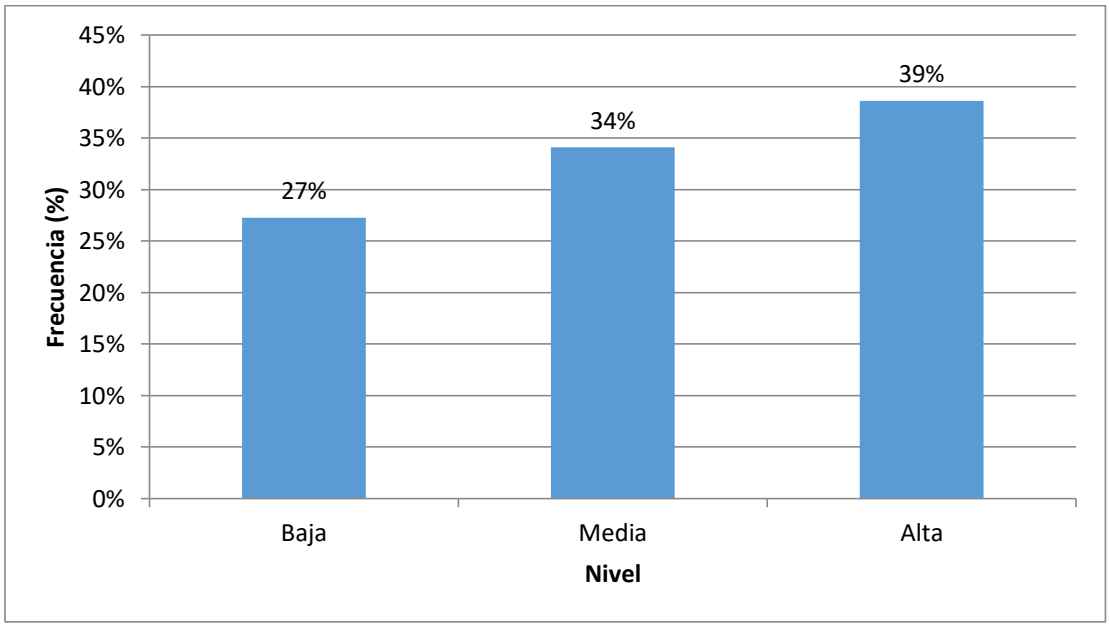
Interpretación

Como podemos observar en la (Figura 7), los encuestados respondieron mayoritariamente que la dimensión derecho de goce del bien de la variable protección del patrimonio en tiempos de pandemia es afectada por la variable fraude informático en el nivel alto y medio con una frecuencia del 48% respectivamente, Además se observa que el nivel bajo es afectado con 4% de las puntuaciones.

Dimensión disposición del bien, de la variable protección del patrimonio en tiempos de pandemia

Figura 8

Frecuencia Porcentual de la Disposición del Bien



Nota. Aplicación de escala valorativa o Baremo para presentación de resultados

Interpretación

Como podemos observar en la (Figura 8), los encuestados respondieron mayoritariamente que la dimensión disposición del bien de la variable protección del patrimonio en tiempos de pandemia es afectada por la variable fraude informático en un nivel alto con una frecuencia del 39%, seguido del nivel intermedio con 34%. Además, se observa que el nivel bajo es afectado con 27% de las puntuaciones.

Prueba de normalidad

Tabla 6

Prueba de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
var1	,113	44	,190	,960	44	,134
var2	**,120**	**44**	**,117**	**,952**	**44**	**,064**

Nota. Corrección de la significación de Lilliefors,

En la (*Tabla 6*) podemos observar el valor del Sig de la prueba de normalidad de Shapiro-wilk (este método es utilizado porque la muestra es menor a 50) es mayor a 0.05, por lo que nos encontramos frente a una distribución paramétrica, en tal sentido corresponde realizar las pruebas correlaciones con la r de Pearson.

Contrastación de hipótesis general

Hipótesis Nula (Ho). El “el fraude informático” no influye significativamente en el “la protección del patrimonio en tiempos de pandemia” en el Distrito Fiscal Lima Este, 2021.

Hipótesis Alternativa (H1). El fraude informático incide negativamente en la protección del patrimonio en tiempos de pandemia en el Distrito Fiscal de Lima Este, periodo 2021.

Tabla 7

Resultados de correlación entre las variables: "fraude informático" y "protección del patrimonio en tiempos de pandemia"

Variable	r de Pearson	Sig. (bilat.)/ P-valor
"fraude informático" y "protección del patrimonio"	.627**	0.000

Nota **. La correlación es significativa al nivel 0,01 (bilateral).

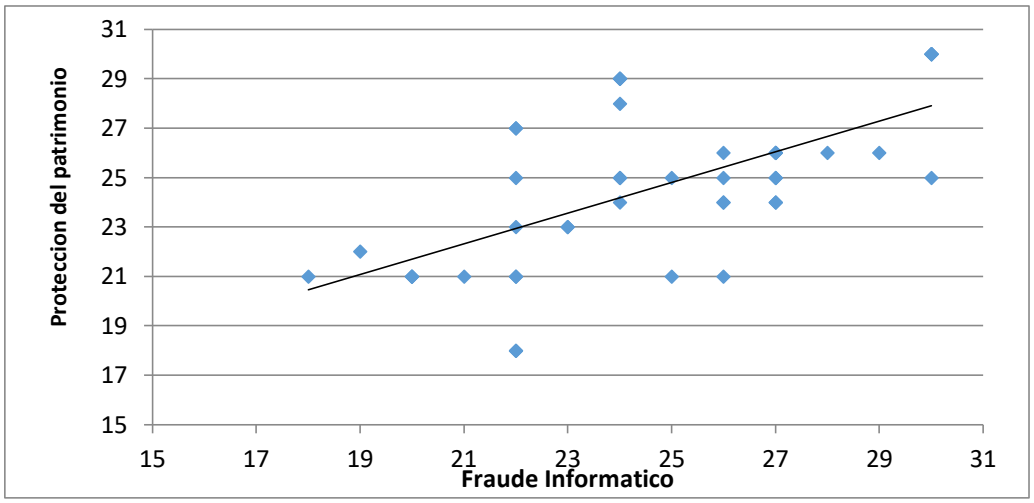
La hipótesis se verificó con el coeficiente de correlación r de Pearson, la cual arrojó un índice r = .627** que corresponde a una correlación positiva alta y muy significativa al determinar el p-valor (p = .000). El cálculo de la regresión lineal arrojó un r cuadrado = .393 entre las variables "fraude informático" y "protección del patrimonio en tiempos de pandemia"; quiere decir que el "fraude informático" influenciará en un 39% en la "protección del patrimonio en tiempos de pandemia".

Por lo que se puede afirmar a un 99% de confianza, que hay una correlación positiva alta entre las variables "fraude informático" y el "protección del patrimonio en tiempos de pandemia", debido a que el valor significancia (bilateral) es de 0.0000, un valor que se encuentra por debajo del 0.01, la correlación es muy significativa.(Tabla 7)

En la (Figura 9) se visualiza el diagrama de dispersión para la correlación entre las variables "fraude informático" y "protección del patrimonio en tiempos de pandemia"

Figura 9

Diagrama de dispersión para la correlación entre las variables "fraude informático" y "protección del patrimonio en tiempos de pandemia"



Nota. La relación lineal de las variables expresada con su línea de tendencia

Decisión: Visto la prueba para la correlación entre las variables "fraude informático" y el "protección del patrimonio en tiempos de pandemia" (*Tabla 7*), existe una correlación positiva alta r = .627 así mismo la significancia es 0.0000<0.01 por lo que se rechaza la hipótesis nula Ho y se acepta la hipótesis general H1.

Contrastación de la primera hipótesis específica

Hipótesis Nula (Ho). El phishing no influye negativamente en el derecho del goce del bien en tiempos de pandemia en el Distrito fiscal de Lima Este, periodo 2021.

Hipótesis Alternativa (H1). El phishing influye negativamente en el derecho del goce del bien en tiempos de pandemia en el Distrito fiscal de Lima Este, periodo 2021.

Tabla 8

Resultados de correlación entre las variables: "El phishing" y "derecho del goce del bien"

Variable	r de Pearson	Sig. (bilat.)/ P-valor
"El phishing" y ""derecho del goce del bien"	.331*	0.028

Nota *. La correlación es significante al nivel 0,05 (bilateral).

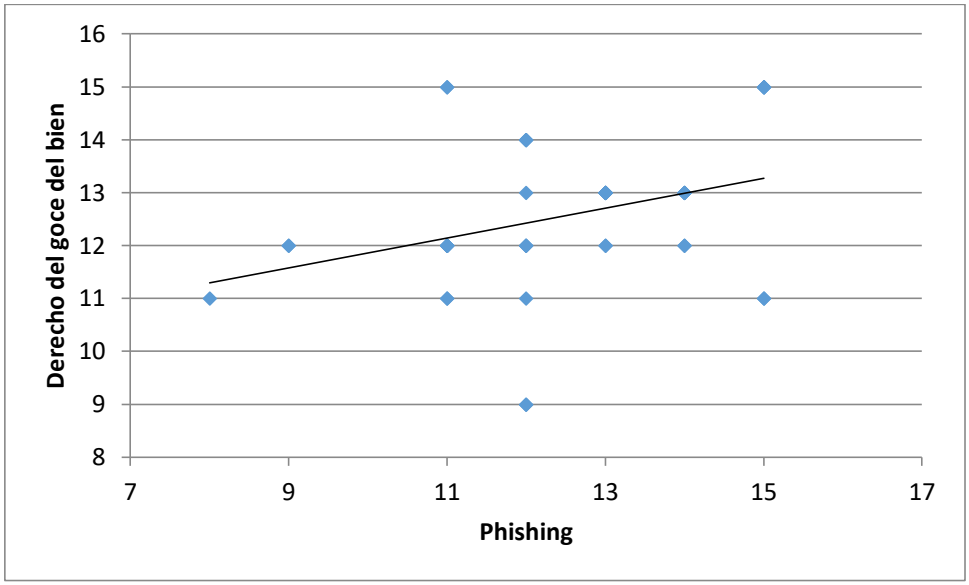
La verificación de la hipótesis se realizó con el coeficiente de correlación r de Pearson, la cual arrojó un índice r = .331* la que corresponde a una correlación positiva baja y significativa al determinar el p-valor (p = .028). El cálculo de la regresión lineal arrojó un r cuadrado = .1096 para la correlación entre el "phishing" y "derecho del goce del bien"; quiere decir que el "phishing" influenciará en un 11% en la "derecho del goce del bien"

Por lo que se puede afirmar a un 95% de confianza, que hay una correlación positiva alta entre las variables "El phishing" y el "derecho del goce del bien", debido a que el valor significancia (bilateral) es de 0.028, un valor que se encuentra por debajo del 0.05, la correlación es significativa. (Tabla 8)

En la (*Figura 10*) se observa la correlación de las variables "phishing" y el "derecho del goce del bien".

Figura 10

Diagrama de Dispersión Variables "Phishing" y "Derecho del Goce del Bien"



Nota. La relación lineal de las variables expresada con su línea de tendencia

Decisión. Visto la prueba para la correlación entre las variables "phishing y el "derecho del goce del bien" (*Tabla 8*), existe una correlación positiva alta r = .331 así mismo la significancia es 0.028<0.05 por lo que se rechaza la hipótesis nula Ho y se acepta la primera hipótesis específica H1..

Contrastación de segunda hipótesis específica

Hipótesis Nula (Ho). Las transferencias electrónicas fraudulentas no afectan negativamente la disposición del bien en tiempos de pandemia en el Distrito Fiscal de Lima Este, periodo 2021.

Hipótesis Alternativa (H1). Las transferencias electrónicas fraudulentas afectan negativamente la disposición del bien en tiempos de pandemia en el Distrito Fiscal de Lima Este, periodo 2021

Tabla 9

Resultados de correlación entre las variables: "trasferencias electrónicas fraudulentas" y "la "disposición del bien"

Variable	r de Pearson	Sig. (bilat.)/ P-valor
"trasferencias electrónicas fraudulentas" y la ""disposición del bien"	.721*	0.000

Nota **. La correlación es significativa al nivel 0,01 (bilateral).

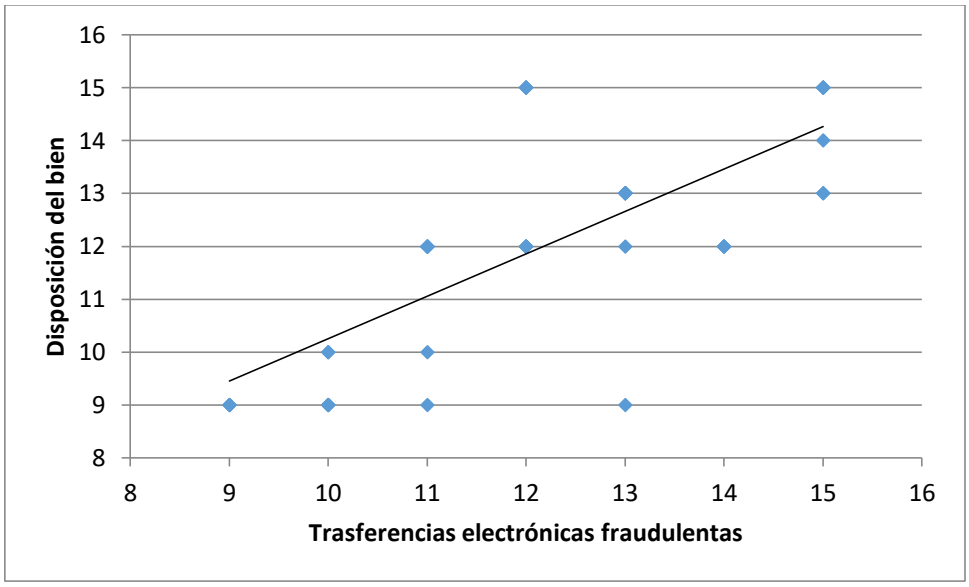
La hipótesis se verificó con el coeficiente de correlación r de Pearson, la cual arrojó un índice r = .721* la que corresponde a una correlación positiva alta y significativa al determinar el p-valor (p = .000). El cálculo de la regresión lineal arrojó un r cuadrado = .564 para la correlación de las variables "transferencias electrónicas fraudulentas" y "disposición del bien"; quiere decir que el "trasferencias electrónicas fraudulentas" influenciará en un 56% en la "disposición del bien"

Por lo que nos permite asegurar a un 99% de confianza, que hay una correlación positiva alta entre las variables "transferencias electrónicas fraudulentas" y la "disposición del bien", debido a que el valor significancia (bilateral) es de 0.000, un valor que se encuentra por debajo del 0.01, la correlación es muy significativa (*Tabla 9*)

En la (Figura 11) se observa la correlación de las variables "transferencias electrónicas fraudulentas" y la "disposición del bien".

Figura 11

Diagrama de dispersión para la correlación entre las variables "trasferencias electrónicas fraudulentas" y la "disposición del bien".



Nota. La relación lineal de las variables expresada con su línea de tendencia

Decisión. Visto la prueba para la correlación entre las variables "transferencias electrónicas fraudulentas" y el "disposición del bien" (**Tabla *1***Tabla 9), existe una correlación positiva alta r = .721 así mismo la significancia es 0.000<0.01 por lo que se rechaza la hipótesis nula Ho y se acepta la segunda hipótesis específica H1.

Análisis e interpretación de los resultados

Al analizar el objetivo general para establecer cómo el fraude informático influye en la protección del patrimonio en tiempos de pandemia en el distrito fiscal de Lima Este, periodo 2021. Se probó la hipótesis general y se demostró que existe una correlación positiva alta (r = .627**) y muy significativa (sig=0. 000) entre la variable fraude informático y la protección del patrimonio en tiempos de pandemia.

Al analizar el primer objetivo específico para establecer cómo el phishing influye en el derecho del goce del bien en tiempos de pandemia en el distrito fiscal de Lima Este, periodo 2021. Se probó la primera hipótesis específica y se demostró que existe una correlación positiva baja (r = .331**) y significativa (sig=0.028) entre la dimensión “phishing” y la dimensión “derecho del goce del bien”.

Al analizar el segundo objetivo específico para establecer cómo las transferencias electrónicas fraudulentas influyen en la disposición del bien en tiempos de pandemia en el distrito fiscal de Lima Este, periodo 2021. Se probó la segunda hipótesis específica y se demostró que existe una correlación positiva alta (r = .721**) y muy significativa (sig=0.000) entre la dimensión “transferencias electrónicas fraudulentas” y la dimensión “disposición del bien”.

De la respuesta de los encuestados se observa que la dimensión “phishing” es la que tiene mayor puntuación alcanzando el 93% de respuestas de nivel medio y alto sobre la afectación del patrimonio. Además, se pudo observar que la dimensión “derecho de goce del bien” es la que mayor afectada por el fraude informático, debido a que el 96% consideró que tiene un nivel de afectación medio y alto.

V. DISCUSIÓN

El objetivo general de este trabajo fue determinar la relación entre el fraude informático y la protección del patrimonio en el Distrito Fiscal de Lima Este. En base a ello se estudió la teoría del bien jurídico como legitimación del Estado para actuar en los delitos de fraude informático y la teoría finalista del patrimonio entendiéndose a este último como un conjunto de relaciones jurídicas que afectan bienes y derechos.

En los resultados muestran un índice r = .627** y un valor muy significativo (p-valor=0.000) < (p-tabular=0.05), a través de la prueba paramétrica de Pearson. Lo que se comprende en una relación existente entre las variables fraude informático y protección del patrimonio. Frente a lo mencionado se rechaza la hipótesis nula y se acepta la hipótesis de investigación que el fraude informático incide negativamente en la protección del patrimonio.

Estos resultados obtenidos guardan relación con lo obtenido por Cangalaya (2020), quien concluye con la incidencia del fraude informático en los bonos en época de pandemia reportando un incremento del fraude informático de 59% lo que genera un perjuicio patrimonial a las personas beneficiarias. De manera similar Gutiérrez (2020) concluye que existe una relación directa entre la afectación del patrimonio y el incremento del phishing en tiempos de pandemia. Sin embargo, en las conclusiones de Hidalgo (2021) no se puede encontrar de manera expresa que este incremento se deba a la pandemia, sino más bien al avance de la tecnología.

Respecto al primer objetivo específico sobre como el phishing influye en el derecho del goce del bien en tiempos de pandemia en el Distrito fiscal de Lima Este. En los resultados se encontró un índice r = .331* y un valor significativo al determinar un (p-valor=0.028) < (p-tabular= 0.05) a través de la prueba paramétrica de Pearson. Lo que se deduce una relación existente entre ambas variables.

Autores como Gutiérrez (2020) señalan que el phishing como parte de los ciberdelitos tienen mayor recurrencia en los tiempos de pandemia, esto concuerda con la presente investigación, donde los encuestados consideran que los links fraudulentos contenidos en los correos, mensaje de textos y redes sociales infuyen negativamente en un nivel medio alto en el derecho del goce del bien.

Urpeque (2019) menciona que el phishing mediante clonación de páginas financieras afecta las cuentas bancarias, con lo que concuerda esta investigación, además señala que este tipo de delitos no está regulado de manera expresa, razón por lo cual propone que se pueda tipificar el phishing en el ordenamiento jurídico peruano al considerarlo como el factor fundamental en el fraude informático.

No obstante Mayer (2020) en una posición contraria al primer objetivo considera que el phishing en sentido estricto no afecta al patrimonio propiamente, sino que es una fase previa o preparatoria de recopilación de información de manera fraudulenta para realizar las transferencias electrónica de las cuentas bancarias, lo que sí ocasiona un perjuicio patrimonial.

El segundo objetivo específico es precisar de qué modo afecta las transferencias electrónicas fraudulentas en la disposición del bien en tiempos de pandemia en el Distrito Fiscal de Lima Este. En los resultados se encontró un índice r = .721** y un valor significativo al determinar un (p-valor=0.000) < (p-tabular= 0.05), a través de la prueba paramétrica de Pearson. Lo que nos da a entender que existe una relación entre ambas variables con un alto índice de afectación.

Pardo (2018) en sus conclusiones de su trabajo del tratamiento jurídico penal de los delitos informáticos contra el patrimonio, establece una relación directa entre las transacciones electrónicas fraudulentas y la afectación al patrimonio, con lo que concuerda los resultados de la presente investigación. En este mismo sentido se pronuncia Mayer (2020), concluyendo que el fraude informático implica un perjuicio en el patrimonio de la víctima la cual se da con unas trasferencias de fondos. Lo que concuerda con nuestro resultado, ya que la correlación entre la variable transferencias electrónicas fraudulentas y la afectación al patrimonio registró un

valor de r = .721** lo cual indica que esta variable tiene un mayor impacto en el patrimonio.

Montoya (2018) señala la necesidad de normar de manera expresa los delito de clonación de tarjetas bancarias para realizar transferencias electrónicas fraudulentas, Sin embargo en la presente investigación se demostró que basta con la obtención de los datos de manera fraudulenta para poder hacer uso de estas tarjeta bancarias para la adquisición de productos, estas transacciones no reconocidas afectan la protección del patrimonio.

VI. CONCLUSIONES

Hemos llegado a las conclusiones siguientes:

PRIMERO. - Se determinó que el fraude informático incide negativamente en la protección del patrimonio en tiempos de pandemia en el Distrito Fiscal de Lima Este, periodo 2021. Existe una correlación positiva media significativa entre las variables en mención. Se ha evidenciado el incremento de denuncias de fraude informático en un 50%

SEGUNDO. - Se estableció que el phishing influye en el derecho del goce del bien en tiempos de pandemia en el distrito fiscal de Lima Este, periodo 2021. Existe una correlación positiva baja significativa entre las variables en mención. El phishing se constituye en el primer paso para la afectación al patrimonio a través de las transferencias electrónicas fraudulentas. También se encontró que la modalidad más frecuente para la obtención de las cuentas bancarias es el envío de links fraudulentos por e-mail.

TERCERO. - Se precisó que las transferencias electrónicas fraudulentas afectan la disposición del bien en tiempos de pandemia en el Distrito Fiscal de Lima Este, periodo 2021. Existe una correlación positiva alta y muy significativa entre las variables en mención. Estas transferencias bancarias son realizadas de manera inmediata, las cuales no son reconocidas por el propietario de la cuenta, afectando el patrimonio. También se pudo encontrar que la adquisición de productos con tarjetas bancarias de manera fraudulenta afecta el patrimonio de la víctima.

VII. RECOMENDACIONES

Recomendamos lo siguiente:

PRIMERO. - Modificar la ley 30096 de delitos informáticos para considerar un nuevo artículo, tipificando el phishing como un delito específico en los siguientes términos: como “La obtención de información confidencial de manera fraudulenta instrumentando dispositivos electrónicos “.

SEGUNDO. - Modificar el artículo del fraude informático de la ley 30096, añadiendo un segundo párrafo sobre las transferencias electrónicas fraudulentas en los siguientes términos: como “La formulación de ofertas engañosas instrumentando dispositivos electrónicos que resulte en transferencias electrónicas fraudulentas que cause perjuicio económico”.

TERCERO. - Descentralizar las fiscalías especializadas en delitos informáticos en el distrito fiscal de Lima Este, proveyéndolos de la logística y procedimientos adecuados que posibiliten una adecuada persecución de estos delitos, además de capacitar a los operadores de justicia.

CUARTO. - Trabajar en una legislación equivalente con los países latinoamericanos para conseguir leyes uniformes y evitar problemas en sus interpretaciones, hecho que favorece la impunidad.

REFERENCIAS

Almeida Minahim, M., & Costa Spínola, L. (2017). *A fraude cometida por meios informáticos sob o prisma da vitimodogmática.* Bahia.

Boada Morales, S. (2019). La naturaleza jurídica de la cuenta bancaria. *Revista de Derecho Privado*, 171-203.

Boza Pró, G. M. (2015). *Tratamiento constitucional ante conflictos entre derechos fundamentales en una relación laboral. El derecho al secreto bancario en una relación laboral.* Lima: PUCP.

Cabrera, P. (2017). *Derecho Penal Parte Especial.* Lima: Moreno.

Camara de Compensación Electrónica. (2020). *Memoria Anual.* Lima.

Candelaria, M., & Pérez, C. (2017). Notas sobre el patrimonio en el derecho venezolano. *Iuris Tantum Revista Boliviana de Derecho*.

Cangalaya, J. (2020). *Fraude informatico en los bonos de subsidio social en epocas de pandemia, en la provincia de chanchamayo, 2020.* Huanuco.

Carrillo, C. (2018). *La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos.* Lima.

Cotrina, S. (2018). *Los factores principales que impiden la aplicación de la ley n°30171- Lima Norte en el año 2016.* Lima-Perú.

Devia, E. (2017). *Estafa Informática del artículo 248.2 del código penal.* Sevilla-España.

Gamio, A. (2018). Límites a la creación voluntaria de patrimonio de afectación para la salvaguarda de bienes. *Revista de derecho de la universidad de Montevideo*, 147.

Gonzales Barrón, G. (2015). Derecho de propiedad y expropiación. *La Constitución comentada*, 3.

Gutierrez, G. S. (2020). *Seguridad de la Información. Phishing y coronavirus.* Lima-Perú: Instituto Nacional de Salud.

Hancco Zapana, E. (2017). *La tipificación del bien jurídico protegido en la estructura del tipo penal informático como causas de su deficiente regulación en la ley 30096, Perú - 2017.* Arequipa.

Harvey, D. (2017). *Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age.* London.

Hernández Sampieri, R., & Mendoza Torres, C. (2018). *Metodología de la Investigación.* Mexico: McGrawHill.

Hernández, D. (2019). *La suplantación de identidad cibernética en el Ecuador.* Colombia.

Hidalgo, c., & Solano, G. (2021). *El phishing como conducta delictiva no regulada en el ordenamiento juridico peruano. propuesta de incorporación del artículo 7-a en la ley de delitos informáticos 30096.* Perú: Universidad Nacional del Santa.

Huayre Torres, G. I. (2021). *El impacto del cibercrimen en delitos de estafa en el Distrito de Lima, 2021.* Lima.

Künsemüller, C. (2017). *Aspectos actuales de los delitos de estafa.* Santiago.

Mayer Lux, L., & Oliver, G. (2020). El delito de fraude informático: Concepto y delimitación. *Revista Chilena de Derecho*, 151-1184.

Mendoza Gurdián , N. (2018). *Las Redes Sociales en el marco del ciberespacio. Consumidores, comercio electrónico y propiedad intelectual a la luz del caso cubano.* Cuba: Universidad de La Habana.

Mesa, A. (2017). *La ciberdelincuencia y sus consecuencias jurídicas.* Colombia.

Ministerio Público, F. d. (2021). *CIberdelincuencia en el Perú: Pautas para una investigación fiscal especializada.* Lima: OFAEC - Oficina de analisis estrategico contra la criminalidad.

Montoya, F. (2018). *Regulación expresa del delito informático de clonación de tarjetas - sede divindat, 2017.* Lima.

Mori, F. (2019). *Los delitos informaticos y la protección penal de la intimidad en el distrito judicial de lima periodo 2008 al 2012.* Lima.

Novoa, I. (2020). *Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional.* Santiago de Chile.

Pardo, A. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018.* Lima.

Pazos, J. (2017). *La persona jurídica de derecho privado en el sistema juridico peruano: ensayo de una teoría general.* Sevilla.

Posada Maya, R. (2017). *Los cibercrímenes: Un nuevo paradigma de criminalidad.* Colombia: Ediciones Uniandes.

Rospigliosi, V. (2019). *Propiedad y Derechos reales Analisis jurídico.* Lima.

Schlack, A. (2008). *El concepto de patrimonio y su contenido en el delito de estafa.* Santiago Chile.

Tellez Valdés, J. (2008). *Derecho Informático.* México: Editorial Graw Hill.

Tenorio Pereyra, J. E. (2018). *Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest.* Lima.

Urpeque, C. (2019). *Análisis de la adecuación de la Ley N°30096, al marco del convenio internacional de Budapest 2001, y su incidencia en la reducción de los delitos informáticos. Huaura 2018.* Huacho.

Vilca, G. (2018). *Los hackers: "Delito informatico frente al codigo penal peruano".* Huaraz.

Villavicencio Terreros, F. (2014). Delitos informáticos. *IUS ET VERITAS*.

Villegas Paiva, E. (2017). *Como se aplica realmente la teoría del delito. Un enfoque a partir de los análisis de los casos jurisprudenciales.* Lima: Gaceta Jurídica S.A.

Vinelli, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Universidad de Lima*.

Zorrilla, K. (2018). *Inconsistencias y ambigüedades en la ley de delitos informáticos ley nº 30096 y su modificatoria ley nº 30171, que imposibilitan su eficaz cumplimiento.* Ancash-Perú.

ANEXOS

Anexo 1: Matriz de operacionalización de variables

TÍTULO: FRAUDE INFORMÁTICO Y LA PROTECCIÓN DEL PATRIMONIO EN TIEMPOS DE PANDEMIA DISTRITO FISCAL LIMA ESTE, PERIODO 2021

ANEXO 1: MATRIZ DE OPERACIONALIZACIÓN DE LAS VARIABLES

Variables	Definición conceptual	Definición operacional	Dimensiones	Indicadores (MIDE LA VARIABLE)	Escala de medición
FRAUDE INFORMÁTICO	Es toda acción dolosa que provoca un perjuicio a personas o entidades utilizando de forma activa dispositivos informáticos afectando el patrimonio. Mayer (2020)	La variable será analizada mediante la aplicación de un cuestionario (escala de likert) en Distrito Fiscal Lima Este. A través del cual se podrá analizar el phishing y la transferencia electrónica fraudulenta	El phishing	Links enviados por e-mail Links enviados por Mensaje de texto Links en redes sociales	Totalmente en desacuerdo En desacuerdo Ni de acuerdo ni en desacuerdo De acuerdo Totalmente De acuerdo
			Trasferencias electrónicas fraudulentas	Trasferencia bancaria inmediata Trasferencias por aplicativo móvil Adquisición de productos con tarjeta bancarias	
PROTECCIÓN DEL PATRIMONIO EN ÉPOCA DE PANDEMIA	El patrimonio económico es un conjunto de bienes o por derechos propios a la persona. Candelaria (2017)	La variable será analizada mediante la aplicación de un cuestionario (escala de likert) en Distrito Fiscal Lima Este. A través del cual se podrá analizar	Derecho de goce de bien	Acceso a cuenta bancaria disponibilidad del saldo Integridad del saldo	

		el derecho de goce y disposición del dinero			
			Disposición del dinero	Colocación a plazo fijo Colocación fondos mutuos Cuenta de ahorros	

Anexo 2: Matriz de consistencia

MATRIZ DE CONSISTENCIA

TÍTULO: FRAUDE INFORMÁTICO Y LA PROTECCIÓN DEL PATRIMONIO EN TIEMPOS DE PANDEMIA DISTRITO FISCAL LIMA ESTE, PERIODO 2021

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES
Problema General ¿De qué manera el fraude informático incide en la protección del patrimonio en tiempos de pandemia en el distrito fiscal de Lima Este, periodo 2021?	**Objetivo general:** Determinar de qué manera el fraude informático incide en la protección del patrimonio en tiempos de pandemia en el Distrito Fiscal de Lima Este, periodo 2021	**Hipótesis general**. El fraude informático incide negativamente en la protección del patrimonio en tiempos de pandemia en el Distrito Fiscal de Lima Este, periodo 2021	Fraude informático	El phishing	Links enviados por e-mail Links enviados por mensaje de texto Links en redes sociales

Primer Problema específico ¿De qué manera el phishing influye en el derecho del goce del bien en tiempos de pandemia en el distrito fiscal de Lima Este, periodo 2021? **Segundo problema específico** ¿De qué manera las trasferencias electrónicas fraudulentas afectan la disposición del bien en tiempos de pandemia en el Distrito Fiscal de Lima Este, periodo 2021?	**Primer objetivo específico. –** Establecer cómo el phishing influye en el derecho del goce del bien en tiempos de pandemia en el distrito fiscal de Lima Este, periodo 2021 **Segundo objetivo específico.** Precisar de qué modo las trasferencias electrónicas fraudulentas afecta la disposición del bien en tiempos de pandemia en el Distrito Fiscal de Lima Este, periodo 2021.	**Primera hipótesis específica.** El phishing influye negativamente en el derecho del goce del bien en tiempos de pandemia en el Distrito fiscal de Lima Este, periodo 2021 **Segunda hipótesis específica.** Las trasferencias electrónicas fraudulentas afectan negativamente la disposición del bien en tiempos de pandemia en el Distrito Fiscal de Lima Este, periodo 2021.		Trasferencias electrónicas no reconocidas	Trasferencia bancaria inmediata Trasferencias por aplicativo móvil Adquisición de productos con tarjeta bancarias

			Protección del patrimonio	Derecho de goce del dinero	Acceso a cuenta bancaria Disponibilidad del saldo Integridad del saldo
				Disposición del dinero	Colocación a plazo fijo Colocación fondos mutuos Cuenta de ahorros

Anexo 3: Instrumento de recolección de datos

Cuestionario sobre "FRAUDE INFORMÁTICO Y LA PROTECCIÓN DEL PATRIMONIO EN TIEMPOS DE PANDEMIA EN EL DISTRITO FISCAL LIMA ESTE, PERIODO 2021"

INSTRUCCIONES: Estimado encuestado a continuación, tienes 12 preguntas sobre "fraude informático incide negativamente en la protección del patrimonio en época de pandemia", para lo cual debes marcar con el número de la tabla la opción que consideras correcta.

Totalmente de acuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Totalmente en desacuerdo
5	4	3	2	1

N°	**ÍTEMS**	**ESCALA**				
		5	4	3	2	1
	Phishing					
1	Los links enviados por e-mail como parte del fraude informático afectan la protección del patrimonio.					
2	Los links enviados por mensaje de texto como parte del fraude informático afectan la protección del patrimonio.					
3	Los links en redes sociales como parte del fraude informático afectan la protección del patrimonio.					
	Transferencias electrónicas fraudulentas					
4	Las transferencias bancarias inmediatas no reconocidas afectan la protección del patrimonio.					
5	Las trasferencias por aplicativo móvil no reconocidas afectan la protección del patrimonio.					
6	La adquisición de productos con tarjeta bancarias no reconocidas afectan la protección del patrimonio.					

	Derecho de goce de bien					
7	El fraude informático afecta el acceso a la cuenta bancaria como parte de la protección del patrimonio					
8	El fraude informático afecta la disponibilidad del saldo como parte de la protección del patrimonio					
9	El fraude informático afecta la integridad del saldo como parte de la protección del patrimonio					
	Disposición del bien					
10	El fraude informático afecta la disposición del dinero para colocarlo a plazo fijo					
11	El fraude informático afecta la disposición del dinero para colocarlo en fondos mutuos.					
12	El fraude informático afecta la disposición del dinero para colocarlo en cuenta de ahorros.					

Anexo 4: Validación de instrumento

HOJA VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

- Apellidos y Nombres: Ginés aliaga Rocío rosario
- Cargo e institución donde labora: Juez poder judicial
- Nombre del instrumento: Instrumento de recolección de datos
- Autor de Instrumento: Juan Carlos Linares Vila

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE					MÍNIMO 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	X
- El Instrumento no cumple con Los requisitos para su aplicación	

IV. PROMEDIO DE VALORACIÓN:

79

Lima, 1 de diciembre del 2022

.

HOJA VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

- Apellidos y Nombres: Cueva Travesaño Mario
- Cargo e institución donde labora: Especialista poder judicial
- Nombre del instrumento: Instrumento de recolección de datos
- Autor de Instrumento: Juan Carlos Linares Vila

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE					MÍNIMO 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	X
- El Instrumento no cumple con Los requisitos para su aplicación	

IV. PROMEDIO DE VALORACIÓN:

95

Lima, 1 de diciembre del 2022

.

FIRMA DEL EXPERTO
DNI No. 06811674

HOJA VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

- Apellidos y Nombres: Kristhel Myrell Palza Bernuy
- Cargo e institución donde labora: Analista Informática Banco Ripley
- Nombre del instrumento: Instrumento de recolección de datos
- Autor de Instrumento: Juan Carlos Linares Vila

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE					MÍNIMO 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	X
- El Instrumento no cumple con Los requisitos para su aplicación	

IV. PROMEDIO DE VALORACIÓN:

85

Lima, 1 de diciembre del 2022

.

FIRMA DEL EXPERTO
DNI No. 40480466
CIP: 89005

Anexo 5: Información Distrito Fiscal Lima Este

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN

Decenio de la Igualdad de Oportunidades para Mujeres y Hombres
Año del Bicentenario del Perú: 200 Años de Independencia
PRESIDENCIA DE LA JUNTA DE FISCALES SUPERIORES
DELDISTRITO FISCAL DE LIMA ESTE

Santa Anita 7 Julio del 2021

Firma Digital
Firmado digitalmente por HERNANDEZ MIRANDA Edith FAU 20131370301 soft
Presidente De La Junta De Fiscales Superiores Del Df Li
Motivo: Soy el autor del documento
Fecha: 07.07.2021 12:31:52 -05:00

CARTA N° 000224-2021-MP-FN-PJFS-DFLE

Señor
Linares Vila Juan Carlos
DNI: 10819370
Correo Electrónico :
juancalina@gmail.com
Presente.-

Referencia: Solicitud información delitos informáticos **(**MUPDFL20210005734)

Tengo el agrado de dirigirme a usted en relación a su solicitud de información, a fin de remitirle el PROVEÍDO N°173-2021-MP-FN-PJFS-DFLE, mediante el cual se dispone la remisión de la información solicitada, para su conocimiento y fines pertinentes.

Sin otro particular, hago propicia la ocasión para expresarle mi consideración. Atentamente,

EDITH HERNANDEZ MIRANDA
PRESIDENCIA DE LA JUNTA DE FISCALES SUPERIORES DEL DISTRITO FISCAL DE LIMA ESTE

EHM/msg

PROVEÍDO N°173-2021-PJFS-DFLE

Lima Este, siete de julio de dos mil veintiunos. -

DADO CUENTA: la solicitud de información presentada por el ciudadano Juan Carlos Linares Vila, ante la Presidencia de la Junta de Fiscales Superiores del Distrito Fiscal de Lima Este, registrada como el Expediente CEA N°5734-2021, mediante la cual peticiona lo siguiente:

"INFORMACIÓN DE DENUNCIAS DE DELITOS INFORMATICOS EN LIMA ESTE"; y

ATENDIENDO:

Que, a fin de atender el presente requerimiento se ha recabado de las Fiscalías Corporativas Penales del Distrito Fiscal de Lima Este, la información solicitada; en consecuencia, SE DISPONE: REMITIR la información cursada por las citadas Fiscalías, al ciudadano Juan Carlos Linares Vila, a través del correo electrónico proporcionado en su solicitud: juancalina@gmail.com, a efecto que tome conocimiento de la misma, concluyéndose así, el proceso de atención a la presente solicitud. Notificándose. -

EDITH HERNANDEZ MIRANDA
PRESIDENCIA DE LA JUNTA DE FISCALES
SUPERIORES DEL DISTRITO FISCAL DE LIMA ESTE

PERÚ | Ministerio del Interior

Firmado digitalmente por: RAMIREZ ESCARATE Rose Mary FAU 20131366966 soft
Motivo: Soy el autor del documento
Fecha: 30/07/2021 14:39:14-0500

"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES""AÑO DEL BICENTENARIO DEL PERÚ: 200 AÑOS DE INDEPENDENCIA"

San Isidro, 30 de Julio de 2021

CARTA N° 001268-2021/IN/SG/OACGD

Señor
JUAN CARLOS LINARES VILA
E-mail:
juancalina@gmail.com
La Era Mz. C, Lt. 11 -
Chosica Lurigancho.-

Asunto: Pedido de información amparada en la Ley N° 27806

Referencia: Solicitud virtual registrada el 30JUL2021

Tengo el agrado de dirigirme a usted en mi calidad de Responsable de atender las solicitudes de acceso a la información pública que corresponda al Ministerio del Interior, con relación al documento de la referencia, a través del cual solicita *"(…) información estadística de los delitos informáticos del periodo 2020-2021 del tipo penal (fraude informático, contra la fe pública, contra datos y sistemas informáticos), y de estar archivadas el motivo del archivo (no se puede identificar al autor, otros) (…)";* pedido que se ampara en la Ley de Transparencia y Acceso a la Información Pública.

Al respecto, preciso a usted que mediante Decreto Supremo Nº 123-2021-PCM, se establece entre otros, prorrogar el Estado de Emergencia Nacional declarado mediante Decreto Supremo Nº 044-2020-PCM, ampliado temporalmente mediante los Decretos Supremos N^{OS} 058, 051, 064, 075, 083, 094, 116, 135, 146, 156, 174, 184, 201-2020-PCM, 008, 023, 036, 076, 105-2021-PCM;

y precisado o modificado por los Decretos Supremos N^{OS} 045, 046, 051, 053, 057, 058, 061, 063,

064, 068, 072, 083, 094, 116, 129, 135, 139, 146, 151, 156, 162, 165, 170, 177, 178 y N° 180-

2020-PCM, por el plazo de treinta y un (31) días calendario, a partir del jueves 1 de julio de 2021, por las graves circunstancias que afectan la vida de las personas a consecuencia de la COVID-19.

Sin perjuicio de ello, hago de su conocimiento que mediante Oficio N° 001192-2021/IN/SG/OACGD, que en copia se adjunta, su pedido de información estará siendo trasladado al Funcionario Responsable de Acceso a la Información Pública de la Policía Nacional del Perú, para su atención directa en el ámbito de su competencia.

En caso requiera más información respecto a su pedido o conocer sobre el estado de su trámite, podrá usted dirigirse al correo electrónico: utd@policia.gob.pe

Sin otro particular, quedo de

usted. Atentamente,

Documento firmado digitalmente

ROSE MARY RAMIREZ ESCARATE
DIRECTORA
OFICINA DE ATENCIÓN AL CIUDADANO Y GESTIÓN DOCUMENTAL MINISTERIO DEL INTERIOR

RMRE/pcp

BICENTENARIO PERÚ 2021

RUD: 20210004062128

PERÚ | Ministerio del Interior

Firmado digitalmente por: RAMIREZ ESCARATE Rose Mary FAU 20131366966 soft
Motivo: Soy el autor del documento
Fecha: 30/07/2021 14:39:14-0500

"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES""AÑO DEL BICENTENARIO DEL PERÚ: 200 AÑOS DE INDEPENDENCIA"

San Isidro, 30 de Julio de 2021

OFICIO N° 001192-2021/IN/SG/OACGD

Señor Coronel PNP
EDUAN DIZ DIAZ
Funcionario Responsable de Acceso a la Información Pública
Policía Nacional del Perú - PNP
Jefe de la Unidad de Trámite Documentario
Secretaría Ejecutiva - Policía Nacional del Perú
Presente.-

Asunto: Traslado de pedido de información amparada en la Ley Nº 27806

Referencia: Solicitud virtual registrada el 30JUL2021

Tengo el agrado de dirigirme a usted en mi calidad de Responsable de atender las solicitudes de acceso a la información pública que corresponda al Ministerio del Interior, con relación al documento de la referencia, a través del cual el ciudadano JUAN CARLOS LINARES VILA solicita *"(…) información estadística de los delitos informáticos del periodo 2020-2021 del tipo penal (fraude informático, contra la fe pública, contra datos y sistemas informáticos), y de estar archivadas el motivo del archivo (no se puede identificar al autor, otros) (…)";* pedido que se ampara en la Ley de Transparencia y Acceso a la Información Pública.

Al respecto, en virtud de lo establecido en el literal b) del artículo 11° del TUO de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, aprobado con Decreto Supremo N° 021-2019-JUS, se traslada a su Despacho la petición de información para su evaluación pertinente y trámite de atención en su calidad de Funcionario Responsable de Acceso a la Información Pública de la Policía Nacional del Perú, por corresponder al ámbito de su competencia, agradeciendo dar respuesta directamente al administrado dentro de los plazos previstos en la Ley.

Sin otro particular, hago propicia la ocasión para reiterarle los sentimientos de mi consideracióny estima.

Atentamente,

Documento firmado digitalmente

ROSE MARY RAMIREZ ESCARATE
DIRECTORA
OFICINA DE ATENCIÓN AL CIUDADANO Y GESTIÓN DOCUMENTALMINISTERIO DEL INTERIOR

RMRE/pcp

BICENTENARIO PERÚ 2021

Anexo 7: Guía de análisis documental

GUÍA DE ANÁLISIS DOCUMENTAL

EXP:	: 4106014502-2019-293-0
SALA/JUZGADO:	: Primera Fiscalía provincial penal corporativa Santa Anita Cuarto despacho
MATERIA	: Patrimonio-Fraude Informático
IMPUTADO/DEMANDADO	: Laidy Mar Rivera Cruz
FECHA	: 23/10/2019

HECHOS:

Con fecha 04 de diciembre de 2018 al promediar las 17:39 horas, Grecia Esther Baldeón Soto, denuncia haber recibido una llamada telefónica del Banco Falabella, indicándole que la llamada correspondía para realizar la validación de un par de zapatilla que realizo vía internet, para lo cual le dijeron que llegaría un mensaje de texto con un código el cual debía proporcionales. Refiere que al término de la llamada ingreso a la página del banco para verificar su estado de cuenta y ver si habían efectuado el cobro del monto de las zapatillas, percatándose que además de las compras de las zapatilla, había un depósito de 2150, dinero que luego fue transferido a una cuenta del Banco de la Nación a nombre de Leidy Mar Rivera Cuz, motivo por el cual llamo al banco y preguntó sobre dichos movimientos, sin embargo le refirieron que el Banco no tenía registrada ninguna llamada a su persona, ante ello y por seguridad la denunciante bloqueo su tarjeta de crédito.

DECISIÓN

Falta o deficit de elementos. No se ha individualizado al presunto autor (es) y participe (s) del hecho delictivo, por lo que no acredita la existencia del delito.

ANÁLISIS DE LOS RESUELTO

Y SU RELACIÓN CON LAS VARIABLES O CATEGORIAS

Conforme a la versión del denunciante, los hechos denunciados han sido atribuidos como presunto delito contra el patrimonio, en la modalidad de fraude informático previsto en el artículo 8 de la Ley 30096.

La información que se cuenta es básica para dar con la ubicación y captura de los responsables del delito, lo cual no contribuye para iniciar un proceso penal, más aún so la prosecución del proceso penal se requiere.

La individualización del sujeto activo del delito, pues para la configuración de cualquier tipo penal, el legislador ha comprendido al sujeto como un requisito sine qua non, cuya ausencia conllevaría a la falta de un elemento sustancial del tipo penal, imposibilitando material y jurídicamente ejercitar una acción penal valida.

El actuar objetivo del ministerio público, siendo que no puede iniciar la persecución penal si no se cuenta con una prognosis o pronostico positivo, dado que, conforme lo prescribe el principio de selectividad, se ha de dar prioridad a aquellos casos con futuro, es decir, a aquellos casos que permitirán viabilizar la acción

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Autenticidad del Asesor

Yo, VILDOSO CABRERA ERICK DANIEL, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ATE, asesor de Tesis titulada: "FRAUDE INFORMÁTICO Y LA PROTECCIÓN DEL PATRIMONIO EN TIEMPOS DE PANDEMIA EN EL DISTRITO FISCAL LIMA ESTE, PERIODO 2021", cuyo autor es LINARES VILA JUAN CARLOS, constato que la investigación tiene un índice de similitud de %, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

ATE VITARTE, 26 de Diciembre del 2022

Apellidos y Nombres del Asesor:	**Firma**
VILDOSO CABRERA ERICK DANIEL **:** 09949028 **ORCID:** 0000-0002-0803-9415	Firmado electrónicamente por: EVILDOSOC el 26-12-2022 22:31:45

Código documento Trilce: INV - 0998854

INVESTIGA UCV