FACULTAD DE DERECHO Y HUMANIDADES

**ESCUELA PROFESIONAL DE DERECHO**

# Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:**

Abogado


**AUTORES:**

De la Cruz Cherres, Wendy Aracely (orcid.org/0000-0002-8365-1356)

Lulli Caceres, Juan Antonio (orcid.org/0000-0001-9213-7968)

**ASESOR:**

Dr. Mucha Paitan, Angel Javier (orcid.org/0000-0003-1411-8096)


**LÍNEA DE INVESTIGACIÓN:**

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

**LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:**

Fortalecimiento de la democracia, liderazgo y ciudadanía

**TRUJILLO – PERÚ**

**2023**

## DEDICATORIA

A Dios, por ser mi guía y fortaleza.
A mi padre, Walter De La Cruz, por su sabiduría y amor incondicional.
A mi madre, Susana Cherres, por su motivación y apoyo absoluto.
A mi pareja, Miguel Guzmán, por creer en mí desde el primer momento.

***Wendy Aracely De La Cruz Cherres***

A Dios, por bendecir mi camino.
A mis padres, por su amor infinito y apoyo incondicional durante toda mi formación profesional.
A mis hijos, por alegrar mi existencia y motivarme a ser mejor cada día.
A mi hermano, que estuvo presente para guiarme ante los problemas y adversidades.

***Juan Antonio Lulli Cáceres***

**AGRADECIMIENTO**

A nuestro asesor metodológico, Dr. Ángel Javier Mucha Paitán, por sus enseñanzas, consejos y acompañamiento. A la Universidad César Vallejo, por abrirnos las puertas de su casa de estudios y permitirnos realizarnos como profesionales. Y a todos aquellos que contribuyeron en la presente investigación.

UNIVERSIDAD CÉSAR VALLEJO

**FACULTAD DE DERECHO Y HUMANIDADES**

**ESCUELA PROFESIONAL DE DERECHO**

# Declaratoria de Autenticidad del Asesor

Yo, MUCHA PAITAN ANGEL JAVIER, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - TRUJILLO, asesor de Tesis Completa titulada: "Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022", cuyos autores son LULLI CACERES JUAN ANTONIO, DE LA CRUZ CHERRES WENDY ARACELY, constato que la investigación tiene un índice de similitud de 18.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

TRUJILLO, 22 de Noviembre del 2023

| **Apellidos y Nombres del Asesor:** | **Firma** |
|---|---|
| MUCHA PAITAN ANGEL JAVIER<br>**DNI:** 17841314<br>**ORCID:** 0000-0003-1411-8096 | Firmado electrónicamente por: AMUCHAP el 22-11-2023 21:23:25 |

Código documento Trilce: TRI - 0659405



INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

**FACULTAD DE DERECHO Y HUMANIDADES**

**ESCUELA PROFESIONAL DE DERECHO**

## Declaratoria de Originalidad de los Autores

Nosotros, DE LA CRUZ CHERRES WENDY ARACELY, LULLI CACERES JUAN ANTONIO estudiantes de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - TRUJILLO, declaramos bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022", es de nuestra autoría, por lo tanto, declaramos que la Tesis:

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

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

| **Nombres y Apellidos** | **Firma** |
|---|---|
| LULLI CACERES JUAN ANTONIO<br>**DNI:** 40999379<br>**ORCID:** 0000-0001-9213-7968 | Firmado electrónicamente por: JLULLIC el 22-11-2023 20:29:01 |
| DE LA CRUZ CHERRES WENDY ARACELY<br>**DNI:** 70127055<br>**ORCID:** 0000-0002-8365-1356 | Firmado electrónicamente por: WCRUZCH5 el 22-11-2023 20:34:39 |

Código documento Trilce: INV - 1376735

INVESTIGA UCV

## Índice de contenidos

## Índice de tablas

## RESUMEN

En la presente investigación se planteó como objetivo general; analizar el tratamiento de los casos de delitos informáticos contra el patrimonio que se investigaron en el Distrito Fiscal del Santa, durante el periodo 2022.

Por tal razón, la investigación se ha ceñido al enfoque cualitativo, de tipo básica, nivel descriptivo y diseño jurídico - propositivo. Como técnicas de recolección de datos se empleó la entrevista, la encuesta y el análisis documental, con sus respectivos instrumentos contenidos en las guías de entrevista, cuestionario y de análisis documental.

Concluyendo así que, el tratamiento de los casos sobre delitos informáticos contra el patrimonio investigados en el Distrito Fiscal del Santa, durante el periodo 2022 fue deficiente, toda vez que los principales supuestos de hecho, tales como: las compras fraudulentas por internet y los fraudes en operaciones y transferencias electrónicas, no están contemplados taxativamente en la regulación actual, siendo menester modificarla con una nueva fórmula legal; asimismo, los fiscales carecen de recursos tecnológicos, personal especializado y conocimiento sobre técnicas sofisticadas de investigación en la lucha contra la ciberdelincuencia.



**Palabras clave:** Tratamiento de los casos, delitos informáticos, patrimonio.

## ABSTRACT

In the present investigation, the general objective was raised; to analyze the treatment of cases of computer crimes against property that were investigated in the Santa Fiscal District, during the period 2022. Therefore, the research has been based on a qualitative approach, of a basic type, descriptive level and legal-propositive design. The interview, survey and document analysis were used as data collection techniques, with their respective instruments contained in the interview guides, questionnaire and document analysis. Concluding that the treatment of cases related to computer crimes against property investigated in the Fifth Corporate Criminal Prosecutor's Office of Santa during the period 2022 was deficient, since the main alleged acts were committed, such as: fraudulent purchases over the Internet and fraud in operations and electronic transfers are not exhaustively contemplated in the current regulations, since they must have been modified with a new legal formula; Consequently, inspectors lack technological resources, specialized personnel, and knowledge of sophisticated investigative techniques in the fight against cybercrime.



**Keywords:** Treatment of cases, computer crimes, patrimony.

## I. **INTRODUCCIÓN**

Hoy en día, es inevitable hablar de progreso y desarrollo sin resaltar el papel predominante que han desempeñado las nuevas tecnologías relacionadas a la información y comunicación en esta última era, el acceso a las mismas ha generado una mejora extraordinaria en la economía, ciencia, salud, transporte y otros; sin embargo, también han sido utilizadas como medios de perpetración de diversos actos punibles llamados por su modus operandi, delitos informáticos que afectan principalmente el patrimonio de las víctimas, dado su elemento configurativo de animus lucrandi.

Esta nueva facilidad para delinquir mediante el acceso a dispositivos inteligentes y la gran libertad para conectarse a un servidor desde cualquier parte del mundo ha causado zozobra en nuestra sociedad, y es que, por diversos motivos y circunstancias, las personas a diario plasman su información personal y financiera en los dispositivos electrónicos que utilizan, sin ser conscientes que ésta puede ser usada por los sujetos denominados ciberdelincuentes para su propio provecho y beneficio.

De esta manera, observamos como a nivel internacional son cada vez más frecuentes las noticias acerca de ciberataques que se realizan de forma masiva en agravio de empresas de todo rango e inclusive de entidades estatales, así por ejemplo en el país del Ecuador, específicamente en la ciudad de Milagro, Zuña et al. (2019), evidenciaron la poca relevancia que le dan las Pymes a los métodos de ciberseguridad, pese a que gracias a su significativo crecimiento en los últimos años, son objetos de múltiples ataques cibernéticos, tales como phishing o malware (p. 492).

Frente a ese contexto, han emergido en el mercado variadas técnicas sofisticadas de ciberseguridad, tales como el Modelo de Auditoría de Seguridad Cibernética presentado por Sabillón (2018), el cual tiene como función valorar y estimar el grado de seguridad, formalidad y previsión cibernética de cualquier institución y/u organismo; de igual modo, es capaz de cuantificar la eficacia de los parámetros de ciberseguridad implementados por los Estados, relacionados a sus tácticas nacionales de seguridad informática (p. 21).

Así tenemos que, según el Centro de Estudios Estratégicos e Internacionales (CSIS), los estados pioneros en brindar mayor ciberseguridad a sus ciudadanos gracias a su legislación vanguardista y su tecnología de punta son Bélgica, Finlandia y España.

Ante lo expuesto, surge la cuestión si estamos verdaderamente preparados para afrontar una amenaza global como tal, al respecto, Echevarría et al. (2020), teniendo como muestra de estudio universitarios del Ecuador, señalan que, si bien los jóvenes son conscientes de los potenciales ciber-hackeos que sus dispositivos pueden sufrir, no le brindan la seriedad del caso ni resultan tomar las medidas de prevención necesarias, mostrándose reacios a resguardar sus datos mediante la descarga de antivirus en sus ordenadores (p. 82).

Por otro lado, apreciamos como en el ámbito nacional, los ciberdelitos se han manifestado de modo alarmante mediante suplantaciones, operaciones fantasmas en cuentas bancarias, utilización de tarjetas de crédito en compras por internet no reconocidas, reflejando dichas modalidades la falta de herramientas y competitividad de nuestras autoridades para hacerle frente a este fenómeno social, económico y jurídico. Pues, si bien el Ministerio Público dispuso convenientemente la conformación de una Unidad Fiscal Especializada en Ciberdelincuencia, la cual contaría con el apoyo de la División de Investigación de delitos de alta tecnología (DIVINDAT) perteneciente a la Policía Nacional del Perú en su labor persecutora del delito, aún se espera su implementación en todo el territorio peruano.

Siendo que, a nivel del Distrito Fiscal del Santa advertimos un incremento progresivo de las denuncias por fraude informático a raíz de la Pandemia por la Covid19, dado que, ante el aislamiento obligatorio implantado por el gobierno central, los ciudadanos se vieron forzados a efectuar sus actividades laborales y económicas desde casa, siendo blancos fáciles de la ciberdelincuencia dada su inexperiencia y pobre o nula educación cibernética sobre estafas informáticas; de allí que, salta a la palestra la cuestión de cómo a pesar del tiempo transcurrido, este tipo de delito sigue en ascenso; por lo que, nos formulamos la siguiente interrogante: ¿Cómo fue el tratamiento de los casos de delitos

informáticos contra el patrimonio en el Distrito Fiscal del Santa durante el periodo 2022?

Por consiguiente, justificamos teóricamente esta investigación con la contribución al desarrollo doctrinal sobre delitos informáticos contra el patrimonio, dado el desglosamiento que se efectuó del tipo penal para un mejor entendimiento e interpretación por parte de los agentes del derecho y de los ciudadanos de a pie.

Además, en cuanto a la justificación metodológica, al ser una investigación cualitativa, tipo básica, se empleó como técnica la entrevista, la encuesta y el análisis documental, con sus respectivos instrumentos: la guía de entrevista, el cuestionario y la guía de análisis de documentos, correspondientemente.

Asimismo, como justificación práctica, tenemos que la presente tesis buscó evidenciar las deficiencias existentes en el tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, durante el periodo 2022; proponiendo a partir de ello una nueva tipificación que permita abordar de manera clara y eficaz el delito en mención; simultáneamente, plantear recomendaciones que de ser ejecutadas coadyuvará a las Fiscalías del Distrito Fiscal del Santa y de los demás distritos fiscales en el ejercicio de sus funciones.

En esa misma línea, tenemos que el objetivo general de esta investigación fue analizar cómo fue el tratamiento de los casos de delitos informáticos contra el patrimonio que se presentaron en el Distrito Fiscal del Santa durante el periodo 2022, mientras que los objetivos específicos se disgregaron en examinar el tratamiento de los casos de compras fraudulentas por internet que se investigaron en el Distrito Fiscal del Santa; además, distinguir el tratamiento de los casos de fraude en las operaciones y transferencias electrónicas que se investigaron en el Distrito Fiscal del Santa, y plantear un proyecto de ley donde se especifique la tipificación de los delitos informáticos contra el patrimonio en el ordenamiento jurídico penal peruano.

Finalmente, se planteó como supuesto de este referido estudio de investigación que el tratamiento de los casos de delitos informáticos contra del patrimonio en

el Distrito Fiscal del Santa durante el periodo 2022 fue deficiente principalmente por su fórmula legal generalizada.

## II. MARCO TEÓRICO

En el plano nacional consideramos la tesis de grado de Pardo (2018) titulada: Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018; la cual se desarrolló desde un enfoque cualitativo, tipo básica, diseño de teoría fundamentada, empleando la técnica de la entrevista con su respectiva guía de entrevista, llegando a la conclusión que la actual normativa de los delitos informáticos contra el patrimonio en el Perú, dista de llegar a ser la más apropiada para combatir sus múltiples modalidades, tales como: el fraude, estafa, sabotaje y hurto informático, pues, al no adecuarse la conducta humana al tipo penal descrito en el artículo 8° de la Ley N°30096, se imposibilita la imposición de una sanción efectiva a los sujetos agentes de este ilícito penal.

Luego, contamos con la investigación aplicada de Gómez (2020) denominada: El tratamiento jurídico penal por parte del fiscal en los delitos informáticos contra el patrimonio, distrito judicial de Lima Norte 2019, realizada desde un enfoque cualitativo, diseño de teoría fundamentada, empleando las técnicas de entrevista y análisis de documentos, para arribar a la siguiente conclusión: el alarmante incremento de la criminalidad informática se dio a partir de la pandemia por la Covid 19, durante la cual las personas para comercializar y obtener artículos de primera necesidad han recurrido al empleo de las redes sociales y páginas webs, sin prever los fraudes informáticos a los que estaban expuestos. Siendo que, a pesar de que en nuestro ordenamiento jurídico penal se tipifica este tipo de delitos, lo hace de forma muy genérica, por lo que, no resulta eficaz frente al panorama que en la práctica se presenta.

Por otra parte, en el plano internacional, encontramos la tesis de Ortiz (2019), titulada: Investigación de fraude digital: Pueblo de Puerto Rico Vs. Luz María Soto Barreto, en cuyas conclusiones se evidencia la vulnerabilidad de una

empresa ante la falta de implementación de políticas y procedimientos de seguridad cibernética, puesto que ante la inexistencia de controles, es susceptible de fraudes informáticos que generan ingentes pérdidas económicas que afectan directamente a clientes y proveedores, provocando la inestabilidad de la persona jurídica y por consiguiente, la economía de sus trabajadores.

De igual importancia, aparece la tesis de Celli (2019), nombrada: Las nuevas tecnologías y los delitos informáticos. Análisis de la ley 26.388. Modificación del Código Penal argentino, elaborada desde un enfoque cualitativo, método descriptivo, empleando la técnica de análisis documental para llegar a la conclusión que, la regulación argentina en relación a los delitos informáticos resulta insuficiente, dada la aparición de nuevas conductas delictivas y la carencia de instrumentos que permitan controlar las mismas, por lo que resta, invitar a los ciudadanos a guardar mayor precaución en su interacción con la tecnología para evitar así ser sujetos pasivos de los ciberdelincuentes.

A continuación, procedemos a desarrollar las categorías del presente trabajo, empezando por los delitos informáticos, cuyo origen se remonta al siglo XXI, en el cual se viralizó a nivel global el empleo de la internet, trayendo consigo ciertos riesgos para las personas naturales y jurídicas, por lo que surge la necesidad para los Estados de regular este tipo de conductas, así como, facilitar a sus ciudadanos estrategias para ejercer un control efectivo de sus datos personales (Rodríguez et al., 2017, p. 70).

Al respecto, Mayer y Vera (2022) refieren que este trascendente comercio de productos y servicios mediante herramientas digitales y pagos virtuales ha generado un mayor movimiento del dinero; sin embargo, también ha propiciado la aparición del ciber-fraude que atenta contra el patrimonio de múltiples individuos y empresas, ocasionando una fluctuante en la economía nacional e internacional que perturba la paz en la sociedad dada la inseguridad informática.

Por lo que, según Santillán et al. (2021), la ausencia de medidas de ciberseguridad, auditorías continuas e inspección de los sistemas de información brinda campo abierto a los piratas informáticos para que puedan alterar,

modificar y manipular los datos que allí encuentren, facultando así la realización de ilícitos penales, en provecho propio o de terceros (pp. 21-22).

En este orden de pensamiento, podemos observar que los móviles para la ciberdelincuencia basados en el sujeto activo son en un primer grupo de ideas: motivaciones intrínsecas, las definidas como la satisfacción o premio que obtiene el actor ante la comisión del ilícito penal, bien pudiera ser por simple curiosidad, por una actividad de autoaprendizaje, un reto personal, o simplemente por salir de la rutina que lo aburre, todo ello relacionado a una edad media de joven o joven adulto. En un segundo grupo de ideas: encontramos las motivaciones extrínsecas, directamente vinculadas al resultado finalista del delito cometido, el cual podría ser por lucrar o beneficiarse económicamente como también por la satisfacción de obtenerlo o conseguirlo utilizando los medios digitales (Alves et al., 2016, pp. 545-546).

En la misma línea, advertimos que producto de la Pandemia por la Covid19, se concretizó la transformación digital, ante la recomendación de contacto físico cero, aumentando los riesgos de sufrir fraudes, estafas, sabotajes y hurtos informáticos, los mismos que siguen innovando en sus modalidades de ejecución, siempre que no se plantee la creación de organismos especializados capaces de hacerle frente. En relación con ello, reparamos que, en países desarrollados tales como España, ya se viene implementando métodos de ciberseguridad en todo su territorio nacional aptos para afrontar los retos que supone operar en el ciberespacio.

Estos delitos también llamados fraudes informáticos por su modus operandi, Saltos et al. (2021), nos señalan que, se basan en sustraer información de aquellas personas que plasman sus datos personales y de sus tarjetas en la internet, en mérito a las aplicaciones innovadoras que se presentan para agilizar trámites, pagos de servicios, compras online y otros, buscando lograr así un beneficio de carácter pecuniario, en detrimento del patrimonio de su víctima (p. 345).

En nuestro ordenamiento jurídico peruano este tipo de ilícito penal lo hallamos previsto en el artículo 8° de la Ley N° 30096, y su posterior modificación en la

Ley N°30171, donde se sanciona al sujeto que, a través del uso de las TIC (Tecnologías de la Información y Comunicaciones) logra apropiarse con conocimiento e intención de la información financiera de cualquier persona natural o jurídica, causando una afectación ilegal en su esfera patrimonial, agravándose dicha conducta, si se vulnera el patrimonio estatal revestido de una finalidad social y/o asistencial.

Con todo, las cuestiones surgen también alrededor de la circunscripción del bien jurídico tutelado en los delitos informáticos, puesto que según Mayer (2017) es la internet dado que cuenta en la actualidad con un estatus de autónomo, debido a las peculiaridades de su uso. Es así que, al ser utilizada a nivel global de manera desmesurada, por sus múltiples beneficios y su libre accesibilidad, se propone como un elemento esencial del sistema democrático moderno, siendo que su acceso debe ser regulado como un derecho fundamental (pp. 254-255).

No obstante, Mayer y Viera (2020) señalan que, si los delitos de fraude informático son perpetrados en stricto sensu de manera online, estarían vulnerando la funcionalidad informática, por lo cual ésta debe ser concebida como el bien jurídico tutelado para este tipo de ilícitos penales (p. 224). Siendo el phishing, la ciber-amenaza más usual por medio del cual, se roban datos personales a través de páginas webs falsas, denominadas páginas phishing, creadas para que los usuarios ingresen sus datos para certificar su identidad teniendo los ciberdelincuentes libre acceso a esta información para efectivizar los fraudes informáticos (García, 2018, p. 654).

Respecto al sujeto activo, doctrinariamente se ha denominado, como los delitos de cuello blanco, al ser una condición especial de la que el actor está revestido, al poseer un dominio especial respecto al manejo de las TICs, debido a que ninguna persona promedio tendría la posibilidad siquiera de cometer tales delitos que requieren un conocimiento necesario acerca del modo de funcionamiento de los diferentes sistemas informáticos. En cambio, el sujeto pasivo puede ser cualquier persona natural o jurídica, órgano del estado o instituciones del sistema financiero que empleen en su gestión sistemas automatizados o (IAS)

inteligencias artificiales de manejo de datos que se encuentran conectados a sistemas computarizados (Warikandwa, 2021, p. 5).

Sin embargo, se ha determinado la complejidad de individualizar al sujeto activo del ilícito penal en comento dado que, existe la viabilidad de realizar estas fechorías mediante el uso de la internet en el total anonimato y sin dejar rastro.

Al respecto, Condori (2020) indica que, si bien la estipulación del delito de fraude informático en el Perú busca sancionar penalmente el comportamiento doloso de los ciberdelincuentes, a condición de que vulneren el patrimonio de sus víctimas; tales penas no alcanzan su efectividad sancionadora, dado que, por su intrincado modo de obrar, los sujetos activos no logran ser identificados con facilidad, requiriéndose para ello, de tecnología vanguardista y normas penales específicas.

Además, Cisneros (2022) resalta que en nuestro país hay una alta demanda de agraviados de delitos informáticos que, por lo dilatorio del proceso, los gastos que acarrea y el tiempo que requiere desisten y no continúan asistiendo a las diligencias donde se solicita su presencia. Aunado a ello tenemos que, incluso las entidades bancarias entorpecen el proceso penal requiriendo para el levantamiento del secreto bancario, orden judicial, burocracia que obstaculiza el pronto esclarecimiento de los hechos en los procesos penales seguidos por la supuesta comisión de los delitos informáticos contra el patrimonio, en su modalidad de fraude informático (pp. 40-41).

Ante lo expuesto, cabe resaltar que los sujetos activos de delitos informáticos suelen recurrir a terceros, para que sus cuentas bancarias sean utilizadas para el depósito y transferencias de las cantidades defraudadas, las que posteriormente son enviadas a cuentas internacionales para perder el hilo de su paradero; del mismo modo, no necesitan acceder desde su propio ordenador, ya que lo pueden hacer desde las llamadas direcciones IP (protocolo de internet) dinámicas, por lo que, no dejarán ni huella de su accionar ilícito. Por consiguiente, al carecer de claridad respecto al lugar donde se perpetuó el ilícito penal, se obstaculiza la investigación y disminuye la posibilidad de llegar a la verdad de los hechos materia de denuncia.

Por otro lado, pueden presentarse inconvenientes relacionados a la elaboración y actuación de los medios probatorios en los procesos penales. Dentro de ese marco, aquella probabilidad de ocultar datos informáticos, aunada a su volatilidad, deviene en ineludible la utilización de técnicas forenses de mayor sofisticación, lo cual debe garantizar la recuperación, preservación y presentación frente a autoridades jurisdiccionales. Conjuntamente, tenemos que, pese a que actualmente se cuenta con herramientas tecnológicas para la captura y evaluación de medios probatorios, su empleo dista de ser normalizado (Mayer, 2018, p. 194).

Es así que, hasta la fecha con respecto al tema tratado, la más óptima propuesta del derecho internacional ha sido la celebración del Convenio sobre la Ciberdelincuencia en Budapest, cuyos estados suscritos se comprometen a aprobar normas que sancionen y regulen estas prácticas ilícitas, mediante la subsunción en un tipo penal de acuerdo a su contexto relacionado a los actos efectuados en agravio patrimonial de algún sujeto, a través de la inserción, modificación, borrado, eliminación de datos informáticos de índole personal mediante sistemas de interferencia o procesamiento de manera dolosa y con el animus de obtener un beneficio económico (Mejía et al., 2023, p. 360).

Empero, resulta criticable que, dado los años transcurridos a partir de la celebración del Convenio mencionado, no se halla actualizado ni innovado la legislación y mecanismos de salvaguarda de las víctimas, con respecto a los delitos informáticos, siendo que los mismos han adoptado una serie de nuevas modalidades que sobrepasan al Derecho, motivo por el cual, resulta sostenible el argumento que debe concretarse una nueva regulación internacional (Rodas y Loor, 2018, p. 75).

Puesto que, tal acuerdo legal de suma relevancia apunta al logro de la aplicación de una política penal mejorada con rango de cobertura hacia todos los miembros suscritos con la finalidad de tener una suerte de sociedad protegida por esta nueva legislación de carácter informático no quitando importancia a la cooperación internacional para lograr mecanismos mejorados pro detención,

prevención y sanción de todo delito informático (Convenio sobre la Ciberdelincuencia, 22 de setiembre de 2019).

En tanto, en nuestro país se ha implementado órganos especializados de apoyo, tales como: la Unidad Fiscal Especializada en Ciberdelincuencia, cuyo objetivo específico es la de brindar y ofrecer soporte y orientación técnica jurídica a los fiscales de las corporativas penales en el desarrollo de las investigaciones de delitos cibernéticos. Asimismo, regularizar las normas técnicas y las formas de investigar los delitos informáticos, coordinando con el titular del Consejo Superior del Ministerio Público sobre el apoyo que requieren para el conveniente desarrollo de sus labores; y, gestionando con los organismos públicos y privados vinculados con la ciberdelincuencia.

Dicha Unidad Fiscal cuenta con el órgano de apoyo de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), creada el 08 de agosto de 2005, bajo la Dirección de Investigación Criminal de la Policía Nacional del Perú (DIRINCRI - PNP), cuyas funciones se centran en prevenir e investigar los delitos informáticos, efectuar indagaciones forenses y pesquisas que conlleven a identificar y localizar los dispositivos móviles o electrónicos que se utilizaron para la perpetración del ilícito penal y hacer efectiva la cooperación internacional.

Esta división tiene competencia a nivel nacional; no obstante, solo cuenta con sede central en Lima y otra a partir del año 2018 en Arequipa, por lo que aún se espera su implementación en todo el territorio peruano. Asimismo, se advierte según el informe emitido por la Defensoría del Pueblo a principios del 2023, que solo el 40% del personal fue instruido en investigación de delitos informáticos sobre la base del NCPP, lo cual resulta alarmante, máxime si consideraciones que asumen la indagación de casi la mitad de las denuncias de parte ingresadas por ciberdelitos en la PNP y aquellas derivadas por la Fiscalía en función a su complejidad.

De allí que, coincidamos con lo manifestado por López (2018), sobre los principales flagelos detectados en los procesos de enjuiciamiento por fraude y estafa informática, siendo estos: i) la alta demanda de víctimas y la dispersión de estas, ii) la carencia de recursos tecnológicos para localizar al autor del ilícito

y iii) la ausencia de una legislación acorde con las nuevas modalidades de ataques cibernéticos que se efectúan a diario (p. 46).

De igual forma, Delgado (2022) resalta la exigencia de una modificatoria para la Ley de Delitos Informáticos N° 30096, que brinde seguridad a las empresas y ciudadanos en general, cuya interpretación no genere mayor incertidumbre en su aplicación y permita salvaguardar el patrimonio de las potenciales víctimas.

Es así que, en el país vecino de Chile, donde según Mayer y Oliver (2020), pese haber provocado revuelo la regulación del delito de fraude informático, aún no se ha llegado a un consenso en la doctrina penal relacionado a sus implicancias jurídicas, por lo que, resaltan la conveniencia de precisar algunos parámetros de su tipificación orientados a una mejor interpretación y aplicación por parte de los agentes del derecho (p. 179).

Ahora bien, respecto a la segunda categoría tenemos los delitos contra el patrimonio que transgreden o vulneran el caudal de las personas, a fin de generar un beneficio propio o de terceros. Estos delitos que anteriormente eran cometidos por los delincuentes en las calles mediante el uso de la fuerza o amenaza, para obtener las pertenencias de las personas, se encuentran previstos en el Código Penal peruano vigente, bajo los tipo penales de hurto, hurto agravado, robo, robo agravado, abigeato, apropiación ilícita, apropiación irregular, receptación, estafa y otras defraudaciones, son perpetrados en la actualidad a través del uso de las nuevas tecnologías, vulnerando la seguridad privada de los sujetos, siendo comunes las suplantaciones, operaciones fantasmas en cuentas bancarias, utilización de tarjetas de crédito en compras por internet no reconocidas, reflejando la falta de herramientas y competitividad de nuestras autoridades para hacerle frente a este fenómeno social.

# III. METODOLOGÍA

## 3.1 Tipo y diseño de investigación

La presente investigación fue elaborada desde un enfoque cualitativo, donde el investigador inicia explorando los hechos, luego procede a describirlos, para culminar planteando una conjetura congruente con lo observado (Hernández, 2014, p. 190).

Asimismo, fue estimada básica, dado que nace de la curiosidad y su principal objetivo es revelar nuevos saberes que sirvan de base fundamental para indagaciones futuras; dentro de su nivel fue de índole descriptivo, puesto que se enfoca en recopilar información sobre las peculiaridades, atributos y propiedades de las categorías y subcategorías que conecta el examinador.

Por otro lado, consideramos el diseño jurídico propositivo, el cual parte del estudio de leyes y casos para lograr precisar las insuficiencias en la puesta en práctica de las normas durante los procesos judiciales.

Finalmente, tenemos que se empleó la teoría fundamentada, que radica en aplicar un método comparativo permanente, antecedido por la compilación de información, con el propósito de plantear posibles soluciones a los cuestionamientos que surgen en el tema a tratar (Páramo, 2015, párr. 4).

## 3.2 Categorías, Subcategorías y matriz de categorización

Tabla 1: Matriz de Categorización.

| Categorías | Subcategorías | Descripción |
|---|---|---|
| **Delitos informáticos** | – Concepto | - Descripción |
| | – Ciberdelincuencia | - Preceptos<br>- Convención sobre la Ciberdelin-cuencia |

| | | |
|---|---|---|
| | – Ordenamiento Jurídico | - Nacional e internacional |
| | – El bien jurídico penal | - Norma |
| | - Órganos especializados | - Unidad Fiscal Especializada en Ciberdelincuencia<br>- DIVINDAT (PNP) |
| **Delitos contra el patrimonio** | – Concepto | - Descripción |
| | – Base Legal | - Código penal |

*Fuente: elaboración propia*

.

## 3.3 Escenario de estudio

El desarrollo de la actual investigación se circunscribió al Distrito Fiscal del Santa; no obstante, los agentes del derecho entrevistados y personal policial encuestados, laboran en distintas partes del Perú, ello en atención, a que aún en el Distrito Fiscal del Santa no se han implementado órganos como la DIVINDAT y otros.

## 3.4 Participantes

La investigación en mención contó con la participación de 03 magistrados de la Corte Superior de Justicia del Santa, 07 fiscales del Ministerio Público del Distrito Fiscal del Santa, 05 abogados especializados en lo penal y 05 agentes de la División de Investigación de delitos de alta tecnología (DIVINDAT); en virtud del grado de conocimiento que poseen y al papel que desempeñan en el tratamiento jurídico penal de los delitos informáticos contra el patrimonio.

## 3.5 Técnicas e instrumentos de recolección de datos

Para efectos de la recopilación de datos se empleó la técnica de la entrevista con su instrumento, la guía de entrevista, la cual según Piza et al. (2019) facilita la obtención de información mediante terceros cualificados, cuya experiencia y conocimientos aportan significativamente; asimismo, se tiene que en la formulación de las interrogantes se debe tener en cuenta que se debe partir de lo más general a lo más específico.

En la misma línea, se usó la técnica de la encuesta y como herramienta el cuestionario, el cual fue aplicado a los a agentes policiales de la DIVINDAT.

Finalmente, se efectuó un estudio documentario aplicando la guía de análisis documental, con el propósito de despejar los diferentes cuestionamientos doctrinarios que surgieron en el trascurso de la presente investigación.

## 3.6 Procedimientos

Para la presente investigación, se redactó una entrevista de 12 preguntas, en función a las categorías y subcategorías en estudio; asimismo, para su aplicación se tuvo que contar primero con el consentimiento de los participantes y la institución en la que laboran.

Además, se usó un cuestionario con 11 interrogantes, las cuales fueron planteadas en consideración a los objetivos propuestos en la presente investigación.

Paralelamente, se profundizó en el análisis de documentos jurídicos relacionados al tratamiento de los delitos informáticos contra el patrimonio.

## 3.7 Rigor científico

El rigor científico según puntualizan Casadevall y Fang (2016) sirve para medir la calidad de una investigación, la cual debe seguir ciertos criterios; por lo que, la presente investigación tiene como fuente libros, tesis y artículos jurídicos confiables para acentuar la credibilidad de la misma; además, dicha

información obtenida fue contrastada con los casos fiscales estudiados; finalmente, sirve de base para futuras investigación en la misma área u otros.

## 3.8 Método de análisis de la información

Se consideró como método de estudio el jurídico - propositivo, debido a que se buscó hallar una solución legislativa a la controversia planteada a través de una propuesta legal, que permita un mejor entendimiento y aplicación de las normas en función de los delitos informáticos contra el patrimonio. Al respecto, Alarcón (2014) indica que este método tiene como propósito identificar los flagelos en la norma, en aras de garantizar la eficacia y eficiencia de la ley; es por ello, que, para concretar los objetivos propuestos, se utilizaron técnicas como la entrevista, la encuesta y el análisis documental. Del mismo modo, se utilizó el método hermenéutico, característico de las investigaciones de carácter cualitativo, pues nos permitió interpretar y entender la exégesis del precepto jurídico cuestionado.

## 3.9 Aspectos éticos

De acuerdo con lo señalado por la académica Tracy (2021), la calidad de una investigación cualitativa se mide conforme a la ética en ella. Por ello, es menester desde el inicio del procedimiento de indagación, salvaguardar la privacidad de los participantes, así como la integridad de los datos obtenidos; de igual manera, se debe reflexionar sobre la idoneidad y proporcionalidad de los métodos a utilizar en base a nuestros principios y valores de formación (pp. 192-193).

Por consiguiente, la presente investigación se ciñó a los lineamientos establecidos por nuestra casa de estudio en la Guía de Elaboración de Productos de Investigación; asimismo, la redacción fue elaborada en aplicación de las normas APA 7$^{ma}$ edición, respetando los derechos de autor y demás reglas; finalmente, se procedió a proteger la identidad de los participantes.

## IV. RESULTADOS Y DISCUSIÓN

Descripción de resultados de la técnica de Entrevista:

En cuanto a la descripción de resultados obtenidos de la guía de entrevista se tiene que se formularon un total de doce preguntas. Estando a que, el objetivo general abarcó cuatro interrogantes**,** el objetivo específico 1) contuvo tres interrogantes, el objetivo específico 2) englobó dos interrogantes y el objetivo específico 3) contó con tres interrogantes.

Es así que, en la primera ronda de interrogantes concernientes al objetivo general, el cual fue analizar el tratamiento de los casos de delitos informáticos contra el patrimonio que se presentaron en el Distrito Fiscal del Santa durante el periodo 2022, se plantearon cuatro preguntas: 1. ¿Considera Ud. que, el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096 regula eficazmente el delito de fraude informático? SI – NO ¿Por qué?, 2. ¿Considera Ud. que, en nuestro ordenamiento jurídico peruano se prevé mecanismos para poder detener, prevenir y sancionar los delitos informáticos contra el patrimonio? SI – NO ¿Por qué?, 3. ¿Qué opinión le merece el aumento progresivo de las denuncias por la presunta comisión del delito de fraude informático, durante el periodo 2022? y 4. ¿Considera Ud. que, los fiscales y funcionarios de las Fiscalías Corporativas Penales deben ser capacitados para abordar e investigar eficientemente los delitos informáticos contra el patrimonio? SI - NO ¿Por qué?

- En atención a la primera pregunta, los entrevistados por unanimidad coincidieron en que el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096 no regula eficazmente el delito de fraude informático, dado que su redacción no abarca todos los supuestos de hecho que en la realidad se presentan; por lo que resulta desfasada e inidónea, generando poca efectividad en cuanto a su aplicación.
- Con respecto a la segunda pregunta, los entrevistados Silva, Núñez, Paredes, Alva, Zavaleta, Ramos, Torres y Huertas (2023) refieren que

en nuestro ordenamiento jurídico peruano sí se prevé mecanismos para poder detener, prevenir y sancionar los delitos informáticos contra el patrimonio, sin embargo, no son suficientes y algunos resultan ineficaces para la identificación de los posibles autores del ilícito penal, lo que evidentemente impide la imposición de una sanción. En contraposición, los entrevistados Martínez, Corcuera, Velásquez, Valdez, Olivares, Saldaña y Díaz (2023) manifiestan que el Perú carece de una regulación legal apropiada y de políticas de prevención orientadas a afrontar este tipo de delitos informáticos contra el patrimonio,

- En consideración a la tercera pregunta, los entrevistados Silva, Zavaleta, Hurtado y Torres (2023) indicaron que el aumento progresivo de las denuncias por la presunta comisión del delito de fraude informático durante el periodo 2022 se debió a la pandemia por la Covid 19, ya que se intensificó el uso de las TICs para las transacciones financieras y en contrapartida se incrementó la cantidad de ciberdelincuentes por las múltiples formas que se generó para delinquir mediante el uso de la internet. Adicionalmente, los entrevistados Martínez, Velásquez, Valdez y Corcuera (2023) señalan que este aumento también responde a la falta de políticas criminales por parte del Estado.
- Referente a la cuarta pregunta, todos los entrevistados convinieron en que los fiscales y funcionarios de las Fiscalías Corporativas Penales deben ser capacitados para abordar e investigar eficientemente los delitos informáticos contra el patrimonio, ya que el uso de herramientas informáticas de las cuales se valen los autores de este tipo de delitos requiere de una permanente actualización.

Para la segunda ronda de interrogantes asociadas con el objetivo específico 1), el cual fue examinar el tratamiento de los casos de compras fraudulentas por internet que se investigaron en el Distrito Fiscal del Santa durante el periodo 2022, se formularon tres preguntas: 5. ¿Cuál cree Ud. que, es la principal razón por la cual se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet?, 6. ¿Considera Ud. que, existen otras razones por las cuales se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet? y 7. ¿Cuál considera Ud. que, sería el aporte de los

miembros de la Unidad Fiscal especializada en Ciberdelincuencia del Ministerio Público en la persecución de los presuntos autores del ilícito penal de compras fraudulentas por internet?

- En relación con la quinta pregunta, los entrevistados Silva, Martínez, Corcuera y Paredes (2023) manifestaron que la principal razón por la cual se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet es la dificultad que se presenta para identificar plenamente a los autores o partícipes del hecho delictivo en cuestión, dado que estos actos ilícitos son ejecutados desde la clandestinidad y el anonimato, utilizando muchas veces para sus fines los datos personales y bancarios de terceras personas. Por otra parte, el resto de entrevistados señalaron que este archivamiento se debe a la ineficaz regulación del tipo penal de fraude informático, por lo que, en muchas ocasiones los supuestos de hecho quedan como atípicos.
- En cuanto a la sexta pregunta, los entrevistados Silva y Saldaña (2023) indicaron que las investigaciones por compras fraudulentas por internet se archivan también a nivel preliminar por la demora de los órganos jurisdiccionales para autorizar el levantamiento del secreto bancario y de las comunicaciones, generando el vencimiento de los plazos; igualmente, por el caso omiso que hacen las entidades de telefonía y financieras para proporcionar la información requerida dentro de los plazos establecidos. Asimismo, Corcuera, Huertas y Olivares (2023) refieren que se debe a la falta de un sistema integrado de seguridad digital. Al respecto, Paredes, Valdez y Torres (2023) agregaron que es debido a la falta de interés de las víctimas en continuar con el proceso al aceptar que fueron ellos quienes brindaron sus datos personales. Y finalmente, Velásquez (2023) precisa que es a causa de la insuficiencia de capacitaciones de los operadores fiscales, quienes desconocen las estrategias de investigación para perseguir el delito y lograr capturar a los delincuentes informáticos.
- Referente a la sétima pregunta, todos los entrevistados coincidieron en lo primordial que resultaría el aporte de los miembros de la Unidad Fiscal especializada en Ciberdelincuencia del Ministerio Público en la

persecución de los presuntos autores del ilícito penal de compras fraudulentas por internet, ya que cuentan con acceso a las fuentes de información telefónica y bancaria, lo que les permitiría rastrear con mayor facilidad la dirección IP desde la cual se efectuó el delito; además que, al estar capacitados en técnicas de investigación sofisticadas permitirían ampliar el abanico de posibilidades de indagación.

En la tercera ronda de interrogantes vinculadas con el objetivo específico 2), el cual fue distinguir el tratamiento de los casos de fraude en las operaciones y transferencias electrónicas que se investigaron en el Distrito Fiscal del Santa, durante el periodo 2022, se interpusieron dos preguntas: 8. ¿Considera Ud. que, es necesaria la actuación de los agentes policiales de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) en las investigaciones aperturadas por la presunta comisión del delito de fraude en las operaciones o transferencias electrónicas? SI - NO ¿Por qué? y 9. ¿Considera Ud. que, las entidades financieras aplican eficientemente sus métodos de seguridad para proteger las cuentas de sus usuarios de fraudes realizados mediante operaciones o transferencias electrónicas? SI – NO ¿Por qué?

- En relación a la octava pregunta, los entrevistados por unanimidad coincidieron en la imperiosa necesidad de la intervención y actuación de los agentes policiales de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) en las investigaciones aperturadas por la presunta comisión del delito de fraude en las operaciones y transferencias electrónicas, para el rastreo de los equipos informáticos empleados por los autores o partícipes de este tipo de delitos, ello en atención a que dicha División está altamente capacitada en estrategias especializadas para la obtención de resultados óptimos en las investigaciones cibernéticas ya que cuentan con equipos de última generación para las pesquisas informáticas que realizan. Adicionalmente, tenemos que el propio sistema procesal penal prevé a la Policía Nacional del Perú (PNP) como órgano de apoyo al Ministerio Público en la persecución de los hechos delictivos.

- Concerniente a la novena interrogante, los entrevistados Paredes, Alva, Zavaleta, Ramos, Torres, Olivares, Saldaña, Velásquez, Valdez, Corcuera y Huertas (2023) refieren que las entidades financieras no aplican eficientemente sus métodos de seguridad para proteger las cuentas de sus usuarios de fraudes realizados mediante operaciones o transferencias electrónicas, por cuanto son fáciles de vulnerar por los ciberdelincuentes ya que no implementan medidas de seguridad sofisticadas en el acceso a la base de datos de sus clientes: del mismo modo, no cuentan con un adecuado filtro de seguridad en la selección de su personal viéndose comprometidos posteriormente en la comisión de estos delitos, y no están dispuestos a denunciar la comisión de estos actos ilícitos por proteger su imagen corporativa. Por otro lado, desde otra arista, los entrevistados Silva, Núñez, Martínez y Díaz (2023) refirieron que en el Perú las entidades financieras ya han implementados seguros de protección frente a fraudes para sus usuarios; sin embargo, los mismos por los costos extras que acarrean no optan por comprarlos y salvaguardar su patrimonio.

Finalmente, en la cuarta ronda de interrogantes concordantes con el objetivo específico 3), el cual fue plantear un proyecto de Ley donde se especifique la tipificación de los delitos informáticos contra el patrimonio en el ordenamiento jurídico penal peruano, se propusieron tres preguntas: 10. ¿Qué deficiencias legislativas advierte Ud. en la tipificación del delito de fraude informático en el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096?, 11. ¿Considera Ud. que, se debe modificar el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096 que regula el delito de Fraude Informático en aras de una mejor aplicación? SI - NO ¿Por qué? y 12. Finalmente, ¿tiene Ud. alguna propuesta de solución o anotación que aportar con relación al delito de fraude informático?

- Referente a la décima pregunta, los entrevistados Silva, Núñez, Saldaña, Díaz y Velásquez (2023) señalaron que la tipificación del delito de fraude informático en el artículo 8° de la Ley de Delitos Informáticos – Ley N°30096, urge de una actualización, ya que no incluye todos los supuestos de hecho que se vienen presentando en la realidad;

asimismo, incurre en demasiado tecnicismo jurídico al describir los verbos rectores. Por otro lado, Valdez, Huertas y Torres (2023) indicaron que el tipo penal adolece de redundancia al especificarse que la conducta debe ser deliberada e ilegítima cuando se sobreentiende que es así por cuanto es un delito doloso. Además, Martínez, Corcuera, Paredes, Valdez, Alva (2023) refirieron que la tipificación de los verbos rectores deber ser mejorada incluyendo los aplicativos con los que se ha innovado nuestro sistema informático y bancario desde el año 2020 a la fecha.

- En consideración a la décimo primera pregunta, los entrevistados Silva, Núñez, Paredes, Alva, Zavaleta, Ramos, Torres, Huertas, Corcuera, Velásquez, Valdez, Olivares, Saldaña y Díaz (2023) manifestaron que se debe modificar el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096 que regula el delito de Fraude Informático en aras de una mejor aplicación; a fin de que, se incluya los supuestos de hecho que actualmente se presenta, en atención a la evolución constante del derecho en torno a regular las relaciones entre las entidades financieras, usuarios y ciberdelincuentes; además que se debe mejorar la técnica narrativa con el propósito de llenar los vacíos legales y posibles deficiencias. Desde otro punto de vista, la entrevistada Martínez (2023) alega que no hay necesidad de modificar el artículo 8° de la Ley N°30096, sino solamente basta añadir nuevos artículos más específicos y con algunas agravantes.
- Para culminar, en relación a la décimo segunda pregunta, los entrevistados Silva, Saldaña y Díaz (2023) propusieron incluir en la nueva narrativa legal definiciones claras de las conductas ejecutadas por los sujetos activos de este tipo de delitos, tales como la clonación de tarjetas de crédito, el Phishing, el Spear Phishing o Phishing segmentado, las transferencias electrónicas fraudulentas, las compras por internet mediante información de tarjetas de crédito o débito, el Cishing, el Ransomware y el Smishing. De igual manera, los entrevistados Paredes, Alva, Valdez, Zavaleta y Ramos (2023) plantearon establecer en el articulado circunstancias agravantes para

incrementar las penas y poder solicitar la medida de prisión preventiva que actualmente el tipo penal no permite. Por último, los entrevistados Torres, Huertas, Corcuera, Martínez, Velásquez y Olivares (2023) hicieron hincapié en que las transacciones realizadas desde dispositivos móviles e informáticos deben realizarse mediante huella digital y grabación incorporada.

Descripción de resultados de la técnica de la Encuesta:

Para la presente investigación se obtuvo los siguientes resultados de la encuesta aplicada a 20 participantes, entre ellos: 3 magistrados, 7 fiscales, 5 abogados especialistas en lo penal y 5 agentes de la DIVINDAT.

La primera interrogante de la encuesta en mención estuvo inclinada a conocer si en el Perú se regula eficazmente el delito de fraude informático, en función a la imperante necesitad de leyes que sancionen tal ilícito penal cuyo aumento en la práctica resulta alarmante en nuestro país.

Al respecto, la segunda tabla nos muestra que el 80% de los participantes, conocedores del derecho e involucrados en la regulación del delito de fraude informático, fueron de la opinión que dicho ciberdelito no se encuentra normado eficazmente en el Perú. En tanto, el 10% difirieron y consideraron que su regulación es eficaz, mientras que el 10% restante del total de los participantes no precisaron.

Tabla 2: Regulación eficaz del delito de fraude informático en nuestra legislación peruana.

1. ¿Considera Ud. que, en el Perú se regula eficazmente el delito de fraude informático?

| | FRECUENCIA | PORCENTAJE |
|---|---|---|
| SI | 2 | 10% |
| NO | 16 | 80% |

| | | |
|---|---|---|
| NO PRECISA | 2 | 10% |
| TOTAL | 20 | 100% |

*Fuente: elaboración propia*

La segunda pregunta estuvo orientada a discriminar si en nuestro ordenamiento jurídico peruano existen mecanismos para detener, prevenir y/o sancionar los delitos informáticos.

Así, tenemos que la tercera tabla refleja que el 60% de los participantes han referido que en nuestro ordenamiento jurídico sí existen mecanismos para detener, prevenir y/o sancionar los delitos informáticos. En tanto, el 30% convergieron y refirieron que no existen dichos mecanismos y el otro 10% restante del total de los encuestados no precisaron.

Tabla 3: Existencia de mecanismos para detener, prevenir y/o sancionar los delitos informáticos en nuestro ordenamiento jurídico peruano.

2. ¿Considera Ud. que, en nuestro ordenamiento jurídico peruano existen mecanismos para detener, prevenir y/o sancionar los delitos informáticos?

| | FRECUENCIA | PORCENTAJE |
|---|---|---|
| SI | 12 | 60% |
| NO | 6 | 30% |
| NO PRECISA | 2 | 10% |
| TOTAL | 20 | 100% |

*Fuente: elaboración propia*

La tercera interrogante estuvo inclinada a conocer si el aumento progresivo de denuncias por fraude informático se debe a la insuficiente regulación de este delito.

La tabla cuarta nos muestra que el 80% de los participantes concordaron en que efectivamente dicho aumento se debe a la insuficiente regulación del ilícito penal en mención. En tanto, el 10% refirieron que tal aumento no responde a la fórmula legislativa establecida para regular el delito de fraude informático y el 10% restante de los participantes no precisaron.

Tabla 4: Insuficiente regulación de fraude informático como causa de aumento progresivo de denuncias.

| 3. ¿Considera Ud. que, el aumento progresivo de denuncias por fraude informático se debe a la insuficiente regulación de este delito? | | |
|---|---|---|
| | FRECUENCIA | PORCENTAJE |
| SI | 16 | 80% |
| NO | 2 | 10% |
| NO PRECISA | 2 | 10% |
| TOTAL | 20 | 100% |

*Fuente: elaboración propia*

La cuarta pregunta estuvo direccionada a determinar si los fiscales y funcionarios de las Fiscalías Corporativas Penales están capacitados para investigar eficientemente los delitos informáticos.

La tabla quinta nos muestra que el 100% de los participantes conocedores del derecho e involucrados en la regulación del delito de fraude informático, fueron de la opinión que los fiscales y funcionarios de las Fiscalías Corporativas Penales no están capacitados para investigar eficientemente los delitos informáticos. En tanto que, ninguno de los participantes difirió.

Tabla 5: Capacitación de fiscales y funcionarios de las Fiscalías Corporativas Penales para investigar eficientemente los delitos informáticos.

4. ¿Estima Ud. que, los fiscales y funcionarios de las Fiscalías Corporativas Penales están capacitados para investigar eficientemente los delitos informáticos?

| | FRECUENCIA | PORCENTAJE |
|---|---|---|
| SI | 0 | 0% |
| NO | 20 | 100% |
| NO PRECISA | 0 | 0% |
| TOTAL | 20 | 100% |

*Fuente: elaboración propia*

.

La quinta interrogante estuvo orientada a conocer si el motivo principal de archivamiento a nivel preliminar de compras fraudulentas por internet es la deficiente regulación del delito de fraude informático.

La tabla sexta nos muestra que el 80% de los participantes refirieron que si consideran que el motivo principal de archivamiento a nivel preliminar de compras fraudulentas por internet es la deficiente regulación del delito de fraude informático. En tanto que, el 20% de los participantes de nuestra investigación que laboran en el ámbito del delito de fraude informático manifestaron que consideran que el motivo principal de archivamiento a nivel preliminar de compras fraudulentas por internet no es la deficiente regulación del delito de fraude informático.

Tabla 6: La deficiente regulación del delito de Fraude Informático como motivo principal de archivamiento a nivel preliminar de compras fraudulentas por internet.

5. ¿Considera Ud. qué, el motivo principal de archivamiento a nivel preliminar de compras fraudulentas por internet es la deficiente regulación del delito de fraude informático?

| | FRECUENCIA | PORCENTAJE |
|---|---|---|
| SI | 16 | 80% |
| NO | 4 | 20% |
| NO PRECISA | 0 | 0% |
| TOTAL | 20 | 100% |

*Fuente: elaboración propia*

La sexta pregunta estuvo inclinada a establecer si existen otros motivos por los cuales se archiva a nivel preliminar las investigaciones por compras fraudulentas por internet.

La tabla sétima nos muestra que el 80% de los participantes manifestaron que sí consideran que existen otros motivos por los cuales se archiva a nivel preliminar las investigaciones por compras fraudulentas por internet. En tanto que, el 20% de los participantes de nuestra investigación que laboran en el ámbito del delito de fraude informático consideraron que no existen otros motivos por los cuales se archiva a nivel preliminar las investigaciones por compras fraudulentas por internet.

Tabla 7: Otros motivos por los cuales se archiva a nivel preliminar las investigaciones por compras fraudulentas por internet.

6. ¿Considera Ud. que, existen otros motivos por los cuales se archiva a nivel preliminar las investigaciones por compras fraudulentas por internet?

| | FRECUENCIA | PORCENTAJE |
|---|---|---|
| SI | 16 | 80% |
| NO | 4 | 20% |
| NO PRECISA | 0 | 0% |

| | | |
|---|---|---|
| TOTAL | 20 | 100% |

*Fuente: elaboración propia*

La sétima interrogante estuvo direccionada a conocer si es determinante la participación de la Unidad Especializada en ciberdelincuencia del Ministerio Publico para la eficaz persecución del ilícito penal de compras fraudulentas por internet.

La tabla octava nos muestra que el 90% de los participantes conocedores del derecho e involucrados en la regulación del delito de fraude informático, señalaron que sí consideran determinante la participación de la Unidad Especializada en ciberdelincuencia del Ministerio Publico para la eficaz persecución del ilícito penal de compras fraudulentas por internet. En tanto que, el 10% de los participantes de nuestra investigación difirieron e indicaron que no es determinante la participación de la Unidad Especializada en ciberdelincuencia del Ministerio Publico para la eficaz persecución del ilícito penal de compras fraudulentas por internet.

Tabla 8: Participación de la Unidad Especializada en ciberdelincuencia del Ministerio Publico para la eficaz persecución del ilícito penal de compras fraudulentas por internet.

7. ¿Considera Ud. determinante la participación de la Unidad Especializada en ciberdelincuencia del Ministerio Publico para la eficaz persecución del ilícito penal de compras fraudulentas por internet?

| | FRECUENCIA | PORCENTAJE |
|---|---|---|
| SI | 18 | 90% |
| NO | 2 | 10% |
| NO PRECISA | 0 | 0% |
| TOTAL | 20 | 100% |

*Fuente: elaboración propia*

La octava pregunta estuvo orientada a determinar si es necesaria la actuación de los agentes policiales de la DIVINDAT en las investigaciones por fraude mediante operaciones o transferencias electrónicas.

La tabla novena nos muestra que el 90% de los participantes refirieron que sí es necesaria la actuación de los agentes policiales de la DIVINDAT en las investigaciones por fraude mediante operaciones o transferencias electrónicas. En tanto que, el 10% de los participantes consideraron que no es necesaria su actuación en dichas investigaciones.

Tabla 9: Actuación de los agentes policiales de la DIVINDAT en las investigaciones por fraude mediante operaciones y transferencias electrónicas.

8. ¿Considera Ud. que, es necesaria la actuación de los agentes policiales de la DIVINDAT en las investigaciones por fraude mediante operaciones o transferencias electrónicas?

| | FRECUENCIA | PORCENTAJE |
|---|---|---|
| SI | 18 | 90% |
| NO | 2 | 10% |
| NO PRECISA | 0 | 0% |
| TOTAL | 20 | 100% |

*Fuente: elaboración propia*

La novena interrogante estuvo inclinada a conocer si se considera que las entidades financieras brindan seguridad jurídica a sus usuarios ante posibles fraudes informáticos.

La tabla décima nos muestra que el 100% de los participantes que laboran en el ámbito de aplicación del delito de fraude informático indicaron que las entidades financieras no brindan seguridad jurídica a sus usuarios ante posibles fraudes

informáticos. En tanto que, ninguno de los participantes de nuestra investigación difirió de lo antes mencionado.

Tabla 10: Seguridad jurídica que las entidades financieras brindan a sus usuarios ante posibles fraudes informáticos.

9. ¿Considera Ud. que, las entidades financieras brindan seguridad jurídica a sus usuarios ante posibles fraudes informáticos?

| | FRECUENCIA | PORCENTAJE |
|---|---|---|
| SI | 0 | 0% |
| NO | 20 | 100% |
| NO PRECISA | 0 | 0% |
| TOTAL | 20 | 100% |

*Fuente: elaboración propia*

La décima pregunta estuvo direccionada a determinar si existen vacíos legales en el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096.

La tabla décimo primera nos muestra que el 90% de los participantes conocedores del derecho e involucrados en la regulación del delito de fraude informático manifestaron que si existen vacíos legales en el Artículo 8° de la Ley de Delitos Informáticos - Ley N°30096. En tanto que, el 10% de los participantes de nuestra investigación no consideraron que existan vacíos legales en el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096.

Tabla 11: Existencia de vacíos legales en el Artículo 8° de la Ley de Delitos Informáticos - Ley N°30096.

10. ¿Considera Ud. que, existen vacíos legales en el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096?

| | FRECUENCIA | PORCENTAJE |
|---|---|---|

| | | |
|---|---|---|
| SI | 18 | 90% |
| NO | 2 | 10% |
| NO PRECISA | 0 | 0% |
| TOTAL | 20 | 100% |

*Fuente: elaboración propia*

La onceava interrogante estuvo orientada a establecer si se debe modificar el artículo 8° de la Ley N°30096 referente al delito de fraude informático.

La tabla décimo segunda nos muestra que el 90% de los participantes que laboran en el ámbito del delito de fraude informático señalaron que sí se debe modificar el Art. 8 de la Ley N°30096 referente al ilícito penal de fraude informático. En tanto que, el 10% de los participantes de nuestra investigación difirieron considerando que no se debe modificar el Art. 8 de la Ley N°30096 referente al delito en mención.

Tabla 12: Necesidad de modificar el Art. 8 de la Ley N°30096 referente al delito de fraude informático.

11. ¿Considera Ud. que, se debe modificar el artículo 8° de la Ley N°30096 referente al delito de fraude informático?

| | FRECUENCIA | PORCENTAJE |
|---|---|---|
| SI | 18 | 90% |
| NO | 2 | 10% |
| NO PRECISA | 0 | 0% |
| TOTAL | 20 | 100% |

*Fuente: elaboración propia*

**Discusión:**

En cuanto a la discusión, se consideraron los resultados obtenidos en los diferentes instrumentos de recolección de datos empleados, tales como: las guías de entrevista, los cuestionarios y las guías documentales; asimismo, se tuvo en cuenta los resultados de las investigaciones citadas en el marco teórico a fin de desarrollar una postura en concordancia con los objetivos establecidos en la presente investigación.

De dicha manera, en relación al objetivo general que fue analizar el tratamiento de los casos de delitos informáticos contra el patrimonio que se presentaron en el Distrito Fiscal del Santa, durante el periodo 2022; tenemos que, el progreso acelerado de las TIC y el aumento de las operaciones y transacciones financieras por la internet han motivado una serie de conductas delictivas fraudulentas en todo el mundo, no siendo ajeno nuestro país, donde según el diario El Peruano (2023), se registró 2 382 denuncias por fraude informático en todo el Perú, convirtiéndolo en el ilícito penal más denunciado durante el periodo 2022. Tal es el caso que, al extrapolar dichas cifras, se presume un crecimiento del 10% en la próxima década.

Al respecto, surgen muchas interrogantes en torno a las causas que producen que estos delitos se multipliquen en la práctica. De acuerdo con el informe publicado por la Defensoría del Pueblo (2023), se tiene conocimiento que el 73% de la población peruana de 6 años de edad a más, llegando al 86% en el caso de la ciudad de Lima Metropolitana tienen acceso frecuente a la internet, lo que los hace blancos fáciles de los ciberdelincuentes (p. 12).

Sobre ello, los investigadores Herrero et al. (2022), sustentan la teoría de que los sujetos pasivos de esta clase de delitos informáticos no son vulnerables por sus características personales, sino por su forma de vida y actividades diarias, siendo que, estos ilícitos penales se materializan cuando la víctima potencial y el ciberdelincuente motivado concurren en tiempo y espacio en ausencia de un tutor apto; sumado a ello, tenemos que las diferentes circunstancias que se han presentado en los últimos años, tales como: la pandemia y otros, han propiciado el uso desmesurado de los teléfonos inteligentes que no solo perjudica la salud

psicosocial de los usuarios sino también los coloca en una situación de vulnerabilidad extrema ante la ciberdelincuencia (pp. 60-64).

No obstante, la interacción constante con la tecnología no debería ser vista únicamente como un flagelo de la sociedad sino como un punto a favor que utilizándolo adecuadamente puede contribuir con la detección y eliminación de estos delitos cibernéticos. Verbigracia, en Sudáfrica se planteó a modo de tesis la implementación de la inteligencia artificial y la tecnología de quinta generación (5G) para empoderar a los dispositivos y estos puedan actuar en respuesta a determinados patrones y/o transacciones, de modo que desalienten y prevengan pertinentemente los fraudes informáticos (Chitimira y Ncube, 2021, p. 23).

Por otro lado, se determinó de los resultados de las entrevistas y encuestas aplicadas que, otra razón que motiva el aumento de denuncias por delitos informáticos contra el patrimonio es la falta de políticas criminales por parte del Estado, y es que, pese a que se han activado mecanismos para poder detener, prevenir y sancionar estos ciberdelitos en el Perú, tales herramientas no son suficientes y algunas resultan ineficaces para la identificación de los posibles autores del ilícito penal, razón por la cual se archivan a menudo las investigaciones fiscales.

Tal es el caso, de las carpetas fiscales sobre delitos informáticos contra el patrimonio que se investigaron durante el periodo 2022 en el Distrito Fiscal del Santa, de cuyo estudio se llegó al supuesto que su tratamiento fue deficiente, dado que el principal argumento que se empleó para archivarlos liminarmente y en etapa preliminar fue la ausencia de elementos de convicción que permitieran individualizar plenamente al autor/es y/o partícipes del delito, no habiéndose agotado todos los medios para la identificación de los mismos, pues, según se tiene de los instrumentos recogidos, los fiscales y funcionarios de las Fiscalías Corporativas Penales no están capacitados para investigar eficientemente los delitos informáticos, ameritando para ello, capacitaciones continuas sobre el marco legal y estrategias de investigación que pueden hacer uso y coadyuven con su labor persecutoria.

Asimismo, se detectó que dicha posición se agrava con los vacíos e imprecisiones legales existentes en nuestra regulación de delitos informáticos que solo salvaguardan situaciones específicas y omiten las nuevas modalidades con las que se presentan esta clase de ilícitos, cayendo en cuenta en la veracidad del axioma: la realidad supera la legalidad.

Por ello, es necesario además de una reforma legislativa, sensibilizar a la población sobre los riesgos reales que acarrea el uso de la internet y las posibles estrategias de protección en una fase temprana y de forma vasta desde las escuelas u otros centros de aprendizaje.

En correspondencia, el profesor Herzog (2009) señala la opción de poner en marcha un programa mediante el cual, los ciudadanos para tener acceso general a la internet tengan que cumplir con una serie de exámenes orientados a la obtención de un certificado de permiso semejante a la licencia de conducir. Por otra parte, sugiere que aquellas personas que incumplan con los códigos de conducta impuestos en las salas de chat y foros sean sometidas a sanciones previamente establecidas para delitos menores en la internet, de modo que sugestivamente el resto comprenda las repercusiones que puede generar el mal uso de las plataformas online (pp. 483-484).

Es así que, se tiene que si bien nuestro país fue uno de los primeros de la región latinoamericana en adherirse al Convenio de Budapest, adecuando su ya existente legislación interna sobre delitos informáticos a los estándares exigidos por dicho Convenio, mediante la promulgación de la Ley N°30171 que modifica la Ley N°30096 – Ley de Delitos Informáticos; hasta el día de hoy no se ha visibilizado políticas para la colaboración e intercambio de conocimientos, experiencias y recursos con los más de setenta Estados Partes del Convenio en mención, desaprovechando información relevante relacionada con las nuevas herramientas sofisticadas con las que otros países ya cuentan para la recopilación de pruebas y seguimiento de los posibles autores.

Por su parte, en referencia al primer objetivo específico de la investigación que fue examinar el tratamiento de los casos de compras fraudulentas por internet que se investigaron en el Distrito Fiscal del Santa, durante el periodo 2022,

tenemos que acorde con los datos publicados por la Organización Mundial del Comercio (2021) el intercambio de productos y servicios ha ingresado a una nueva era, donde se vienen efectuando de forma masiva compras y ventas a través de medios digitales por las múltiples ventajas que brindan en los procesos de producción, propaganda, transacción y distribución. Verbigracia, tenemos que, en el año 2017 el comercio electrónico ha generado un incremento del 13% en las ventas en el mercado europeo, asiático y norteamericano produciendo ganancias de hasta 29 billones de dólares (Gonzáles, 2020, p. 54).

Empero, este innovador comercio online trajo consigo también nuevos riesgos para los que evidentemente no estamos preparados y nuestra regulación legislativa es deficiente, de allí la necesidad de un marco legal ajustado a la realidad para prevenir y sancionar los ilícitos cibernéticos que se presenten.

Tal es la situación que, en el Distrito Fiscal del Santa se determinó que del total de denuncias ingresadas por fraude informático durante el periodo 2022, una gran cantidad correspondía a compras fraudulentas por internet, en las que las víctimas ingresaron a paginas clonadas, adulteradas o no oficiales.

Asimismo, se procedió a identificar las modalidades de ciberfraude aplicadas, resaltando entre ellas: el E-Skimming o clonación de página web, el phishing o envío de correos no deseados y el Sim Swapping, a través del cual dejan al usuario fuera de la red celular para efectuar compras no reconocidas.

Cabe resaltar que, estas compras fraudulentas también se pueden realizar por medio de las POS (terminales punto de venta) y plataformas de e-commerce, por lo que Domínguez y Vera (2022) enfatizan en la urgencia de que dichas plataformas dispongan de medios de seguridad extras para la autentificación de sus cibernautas (p. 28). Además, se pueden comprar datos de tarjetas bancarias por internet, motivo por el cual suele complicarse la identificación del autor y/o partícipes.

Ante lo expuesto, procedimos a contrastar con los datos obtenidos en nuestros instrumentos, apreciando que la mayoría de los participantes coincidieron al considerar que la principal razón por la cual se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet es la dificultad que se

presenta para identificar plenamente a los autores o partícipes del hecho delictivo en cuestión, puesto que, estos actos ilícitos son ejecutados desde la clandestinidad y el anonimato, aunado a la ineficaz regulación del tipo penal de fraude informático, por lo que, en muchas ocasiones los supuestos de hecho quedan como atípicos.

De igual manera, hicieron hincapié en el cambio que generaría el aporte global de los miembros de la Unidad Fiscal especializada en Ciberdelincuencia del Ministerio Público, en la persecución del delito de fraude informático, dado su vasto acceso a las fuentes de información de telefonía y entidades bancarias, y el conocimiento cualificado de técnicas de investigación sofisticadas que ostentan.

Bajo estas premisas, es posible determinar que los sujetos agentes de esta clase de delitos pueden ser personas comunes, especializadas o técnicas, además, pueden operar solas o como parte de una organización. Siendo que, lo que se debe diferenciar es que al efectuar compras fraudulentas por internet solo se deja un rastro volátil, intangible y de breve permanencia en el espacio, por lo que es más complejo de investigar.

Tal es el caso que, es menester destacar la funcionalidad de la auditoría forense como disciplina de impacto para el rastreo de los ciberdelincuentes mediante la detección, preservación y análisis de la evidencia digital en las investigaciones de delitos cibernéticos. Entendiéndose la evidencia digital como los registros únicos que dejan los sujetos activos en un equipo informático y que posibilita confirmar la ejecución de una acción por un usuario o intruso en un determinado sistema informático. Adicionalmente, puede revelar la correspondencia online entre los imputados y la víctima que permita enlazarlos y desvirtuar la presunción de inocencia que reviste todo investigado (Díaz, 2021, pp. 320 - 329).

Por otro lado, respecto al segundo objetivo específico de la presente investigación que fue distinguir el tratamiento de los casos de fraude en las operaciones y transferencias electrónicas que se investigaron en el Distrito Fiscal del Santa, durante el periodo 2022, tenemos que desde que surgieron las World Wide Web, Cerezo y García (2020) refieren que las personas han adaptado sus

vidas a las nuevas corrientes digitales, desarrollando con el tiempo una codependencia con las tecnologías de la información y comunicación, plasmando sus datos biográficos y financieros en sus dispositivos móviles para agilizar movimientos bancarios con el propósito de pagar servicios básicos, efectuar compras online, transferir dinero, cobrar remuneraciones y otros, a expensas de los múltiples riesgos a los que se exponen, tales como por ejemplo: el ciberfraude (p. 2).

No obstante, en los fraudes en operaciones o transferencias electrónicas, los ciberdelincuentes requieren necesariamente una cuenta de destino correspondiente a una persona natural o jurídica a diferencia de las compras fraudulentas, lo que a grandes rasgos pareciera beneficiaría su rápida identificación; empero, éstas no suelen pertenecer a los propios sujetos agentes, sino a terceras personas que, mediante engaño, coacción, intimidación y/o manipulación retiran el dinero transferido.

Motivo por el cual, al proceder analizar los casos de fraude en operaciones o transferencias electrónicas ingresados en el Distrito Fiscal del Santa durante el periodo 2022, se distinguió dos situaciones: i) aperturas de investigación preliminar por fraude informático contra el titular de la cuenta de destino y ii) aperturas de investigación preliminar por fraude informático contra los que resulten responsables, disponiendo como primer acto de investigación la declaración testimonial del titular de la cuenta de destino.

En relación con ello, cabe resaltar que en la mayoría de los casos los titulares de dichas cuentas son personas que han sido víctimas de hurto o robo de sus documentos de identidad, tarjetas de crédito o débito y/o celulares y que, por desidia o ignorancia no han denunciado ni bloqueado sus tarjetas, conllevando a que estos ciberdelincuentes les den un mal uso desde la clandestinidad.

Al respecto, Paz (2018) señala que las entidades bancarias no han cumplido con su rol de garante monetario, pues no cuentan con medidas de ciberseguridad idóneas que protejan el patrimonio de sus clientes, asumiendo un comportamiento culposo al ofrecer alternativas de solución sesgadas frente a la comisión de un fraude informático (p. 285).

Además, tales instituciones financieras se muestran reacias a denunciar estos ciberdelitos por la mala propaganda, el menoscabo a su nombre y la disminución de la confianza en la ciudadana que eso les causaría; por lo que, solo proceden a incrementar las tasas de interés a pagar por los usuarios víctimas de fraude informático (Cassim, 2015, p. 75)

Lo que deja al Ministerio Público en una posición compleja como ente persecutor del delito, pues pese que conforme la Ley N°27697 los fiscales están facultados para intervenir y controlar las comunicaciones y documentos privados en caso excepcional, estos solo limitan su accionar a la presentación de un requerimiento al Juzgado de Investigación Preparatoria de turno respecto al levantamiento del secreto bancario de las cuentas de destino, siendo que cuando son declaradas fundadas y se prosigue a remitir los escritos a los bancos adjuntando la resolución concesora, los mismos son atendidos posterior a la preclusión de los plazos establecidos para la investigación preliminar.

En virtud de lo expuesto, los participantes entrevistados coincidieron en la imperiosa necesidad de la intervención y actuación de los agentes policiales de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), dado que están altamente capacitados en estrategias especializadas para la obtención de resultados óptimos en las investigaciones cibernéticas ya que cuentan con equipos de última generación para las pesquisas informáticas que realizan.

Adicionalmente, Jones y Guzmán (2019) postulan las técnicas del machine learning como métodos líderes en la detección de fraudes bancarios, pues bajo el concepto de que los ordenadores aprenden de sí y de los datos que en ellos se plasman, mediante algoritmos pueden identificar patrones en la conducta de los sujetos agentes, contribuyendo en la prevención y erradicación de la ciberdelincuencia.

Finalmente, en relación al tercer objetivo específico que fue plantear un proyecto de Ley donde se especifique la tipificación de los delitos informáticos contra el patrimonio en el ordenamiento jurídico penal peruano, tenemos que en la actualidad, resulta alarmante el incremento de modalidades en las que se ejecutan los delitos informáticos contra el patrimonio, dificultando la identificación

e individualización de los sujetos agentes y acarreando grandes pérdidas económicas para las víctimas, siendo que tal situación ha generado una sensación de inseguridad informática en los usuarios al navegar por la internet.

En consecuencia, surge la preocupación sobre qué medidas podemos emprender para hacerle frente a este fenómeno de la ciberdelincuencia, es así que en concordancia con lo planteado por Alves et al. (2017) tenemos las siguientes alternativas: i) actualizar periódicamente la legislación interna, ii) implementar sistemas de navegación seguras, iii) enseñar a la población como detectar de forma temprana las amenazas, iv) fomentar y promocionar la investigación sobre ciberseguridad e v) incentivar la cooperación institucional e internacional (p. 99).

Respecto al primer punto, nuestro ordenamiento jurídico penal peruano regula los delitos informáticos contra el patrimonio en el artículo 8 de la Ley N°30096, modificada el 10 de marzo del 2014 por la Ley N°30171; referente a ello, los participantes entrevistados manifestaron que dicha tipificación urge de una reforma legislativa, ya que no incluye los principales supuestos de hecho que se vienen presentando a diario en la práctica; asimismo, incurre en excesivos tecnicismos jurídicos al describir los verbos rectores y adolece de redundancia al especificarse que la conducta debe ser deliberada e ilegítima cuando se sobreentiende que es así por cuanto es un delito doloso.

En consecuencia, salta a la palestra la necesidad de una nueva fórmula legal que permita prevenir, sancionar y erradicar los delitos informáticos contra el patrimonio, albergando las modalidades de compras fraudulentas por internet y fraude en operaciones y transferencias electrónicas, que del estudio de casos de fraude informático investigados en el Distrito Fiscal del Santa durante el periodo 2022, se identificó en mayor cantidad.

Asimismo, según lo sostenido por Mabeka y Cassim (2023), se debe incluir sanciones no penales en sus acápites, tales como, la posibilidad para la víctima de interponer acciones civiles simultáneas al proceso penal en curso, con el propósito de garantizar la reparación del daño sufrido producto del delito informático cometido en su contra (p. 32).

En la misma línea, los investigadores Silva de García et al. (2018) señalan que el estudio de los delitos cibernéticos debe ser abordado de forma holística y multidisciplinaria, ya que la motivación delictiva varía de acuerdo con el contexto en el que se ejecuta, tal es la situación que en muchos casos los ciberdelincuentes suelen ser trabajadores de las mismas entidades bancarias, empresas o instituciones, cuya conducta motivada por una percepción de injusticia organizacional los inclina a cometer estos ilícitos penales.

En suma, al quedar demostrado que la actual normativa que tipifica los delitos informáticos contra el patrimonio es ineficaz, por cuanto no aborda las diversas modalidades delictivas y su redacción genera confusión en su aplicación por los agentes del derecho, urge un proyecto de Ley donde se adecúe los supuestos de hecho más frecuentes; por ello, en la presente investigación adjuntamos un proyecto de Ley acorde con las necesidades de la población peruana ávida de justicia social y seguridad informática.

De igual manera, tenemos que se comprobó el supuesto del presente estudio de investigación, el cual afirma que el tratamiento de los casos de delitos informáticos contra del patrimonio en el Distrito Fiscal del Santa durante el periodo 2022 fue deficiente, en primer lugar, por la regulación tan general de los delitos informáticos contra el patrimonio en nuestro ordenamiento jurídico penal, en segundo lugar, por no contar con la tecnología necesaria y en tercer lugar, ante la falta de implementación de oficinas descentralizadas de la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional (DIVINDAT) en el Distrito Fiscal del Santa.

Para concluir, resaltamos los principales aportes que tuvo la presente investigación en relación al desarrollo doctrinal y procesal de los delitos informáticos contra el patrimonio; tales como la identificación de las deficiencias en la investigación a nivel fiscal, así como la propuesta de una nueva fórmula legal que permita abordar de manera clara y eficaz los delitos en mención; además, de servir de base para futuras investigaciones en otros distritos fiscales y/o judiciales.

## V. **CONCLUSIONES**

1. El tratamiento de los casos sobre delitos informáticos contra el patrimonio investigados en el Distrito Fiscal del Santa durante el periodo 2022 fue deficiente, toda vez que los principales supuestos de hecho, tales como: las compras fraudulentas por internet y los fraudes en operaciones y transferencias electrónicas, no están contempladas taxativamente en la regulación actual; asimismo, los fiscales carecen de recursos tecnológicos, personal especializado y conocimiento sobre técnicas sofisticadas de investigación en la lucha contra la ciberdelincuencia.

2. Las denuncias por compras fraudulentas por internet, fueron aperturadas en el Distrito Fiscal del Santa durante el periodo 2022, por el delito de estafa agravada o fraude informático; sin embargo, fueron archivadas en la etapa preliminar por atipicidad, así como por falta de elementos de convicción que permitan identificar e individualizar a los autores o partícipes del ilícito penal. Dado que, los fiscales en su labor persecutoria del delito no cuentan con personal especializado en la detección, preservación y análisis de la evidencia digital, toda vez que, en esta modalidad de fraude informático, los ciberdelincuentes solo se dejan un rastro volátil, intangible y de breve permanencia en el espacio, por lo que es más complejo de investigar.

3. Las denuncias por fraude en las operaciones y transferencias bancarias, fueron aperturadas en el Distrito Fiscal del Santa durante el periodo 2022, por el delito de estafa agravada, apropiación irregular o fraude informático; no obstante, fueron archivadas en la etapa preliminar por atipicidad y falta de elementos de convicción para desvirtuar la presunción de inocencia de los investigados que en su mayoría son los titulares de las cuentas de destino que, mediante engaño, coacción, intimidación y/o manipulación retiraron el dinero transferido. Así es que, si bien los ciberdelincuentes dejaron un rastro o huella, el único acto de investigación aplicado por los fiscales fue la solicitud del levantamiento del secreto bancario, omitiendo

su facultad de intervenir y controlar las comunicaciones y documentos privados en caso excepcional.

4. Si bien, en nuestro ordenamiento jurídico penal peruano se regula los delitos informáticos contra el patrimonio en el artículo 8° de la Ley N°30096 – Ley de Delitos Informáticos, posteriormente modificada por la Ley N°30171, dicha fórmula legal es muy global, lo que dificulta su aplicación y por ende, la sanción a los ciberdelincuentes como la protección del bien jurídico lesionado que estaría constituido por el patrimonio de las víctimas. Siendo el caso que, al no responder a las necesidades actuales de la sociedad, amerita una modificación urgente.

## VI. RECOMENDACIONES

1. Se recomienda al Congreso de la República modificar la fórmula legal empleada en la tipificación de los delitos informáticos contra el patrimonio, con el fin de contemplar las nuevas modalidades de fraude informático, entre ellas las compras fraudulentas por internet y los fraudes en las operaciones y transferencias electrónicas; asimismo, endurecer las penas con el propósito de disuadir al potencial sujeto agente de cometer este ilícito penal en cualquiera de sus formas.

2. Se sugiere al Ministerio de Relaciones Exteriores, concretar reuniones virtuales con los demás Estados Parte del Convenio sobre Ciberdelincuencia, con la finalidad de pactar conferencias internacionales para el intercambio de conocimientos sobre las nuevas herramientas y técnicas de investigación que han surgido en la lucha contra el fraude informático.

3. Se aconseja a la Fiscalía de la Nación, sumar esfuerzos para terminar de implementar en todo el territorio peruano, Fiscalías especializadas en Ciberdelincuencia y oficinas descentralizadas de la DIVINDAT, ante el aumento alarmante de denuncias. Asimismo, contratar personal cualificado en auditoría forense y demás disciplinas que coadyuven a los fiscales en su labor persecutoria del delito; abasteciéndolos con equipos de última generación para sus pesquisas informáticas.

4. Se sugiere al Ministerio de Educación incorporar en la malla curricular de educación primaria, secundaria y universitaria, cursos y talleres sobre navegación segura en la internet y el uso adecuado de las Tics; asimismo, proponga políticas públicas que incentiven la investigación desde las escuelas sobre métodos de ciberseguridad.

## REFERENCIAS


Alarcón, A. (2014). La investigación en la enseñanza del derecho para la formación de abogados. Caso universidad de Cartagena de Indias periodo 1994 – 2014. *Revista Saber, ciencia y libertad,* 8(2). https://www.researchgate.net/publication/312874510_La_investigacion_en_la_enseñanza_del_derecho_para_la_formación_de_abogados_Caso_universidad_de_Cartagena_de_indias_periodo_1994_-_2014

Alves, P. M. y Andrade de Jesús, I. O. (2016). Combate às transferências bancárias ilegítimas pela Internet no direito português:entre as experiências domésticas e políticas globais concertadas. *Revista direito GV,* 12(2). https://www.scielo.br/j/rdgv/a/6CjnmkZgQkkqZC7XVkrDXrv/?lang=pt#

Alves, P., Santos da Silva, S. y Bilhim de Faria, J. (2017). Proposta de modelo explicativo das perceções sobre gestão e políticas públicas em matéria de cibersegurança e cibercrime. *Sociologia*, *33*, 95-113. http://www.scielo.pt/scielo.php?script=sci_arttext&pid=S0872-34192017000100006&lang=es

Casadevall, A. y Fang, F (2016). Rigorous Science: A How-To Guide. *mBio, 7(6).* https://journals.asm.org/doi/10.1128/mbio.01902-16

Cassim, F. (2015). Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves? *Potchefstroom Electronic Law Journal (PELJ)*, *18*(2), 69-110 http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1727-37812015000200003&lang=es

Celli, S. (2019). *"Las nuevas tecnologías y los delitos informáticos. Análisis de la ley 26.388. Modificación del Código Penal argentino"* [Tesis de grado, Universidad Siglo XXI – CAU Salta] Archivo Digital. https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/16861/CELLI%20TRIUNFETTI%20Sebastian.pdf?sequence=1

Cerezo, A. y García, R. (2020). La ciberdelincuencia en España. *Revista Electrónica de Estudios Penales y de la Seguridad, 6*, 1-20. https://dialnet.unirioja.es/servlet/articulo?codigo=7468453

Chitimira, H y Ncube, P. (2021). The regulation and use of artificial intelligence and 5G technology to combat cybercrime and financial crime in South African banks. *Potchefstroom Electronic Law Journal (PELJ)*, *24* (1), 1-33. http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1727-37812021000100041&lang=es

Cisneros, R. (2022). Factores de identificación del imputado de fraude informático en un despacho de la fiscalía de ciberdelincuencia, año 2021. https://alicia.concytec.gob.pe/vufind/Record/UCVV_2ffccfdbc3d60062dbad707a197ed5f8

Condori, R. (2020). Implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020. https://alicia.concytec.gob.pe/vufind/Record/UCVV_149385237f8f917c703e8db75952a324

Convenio sobre la Ciberdelincuencia (22 de setiembre de 2019). Serie de Tratados Europeos – N° 185. Diario Oficial El Peruano. https://cdn.www.gob.pe/uploads/document/file/1671758/Convenio%20de%20Budapest.pdf.pdf

Díaz, G. (2021). La auditoría forense como fundamento metodológico en la detección de casos de fraudes informáticos. *Revista Gestión I+D, 6*(2), 315-351. https://dialnet.unirioja.es/servlet/articulo?codigo=8737229

Delgado, F. (2022). El tratamiento penal de los delitos informáticos contra el patrimonio de las personas naturales y jurídicas en la Corte Superior de Justicia del Santa - Chimbote. https://alicia.concytec.gob.pe/vufind/Record/USSS_096176a6634cd48bae1b38db275cb45a

Domínguez, R. y Vera, R. (2022). Análisis espacial del ciberfraude al comercio electrónico: consideraciones en agenda política Tamaulipeca. *Podium, (41),* 21-40. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2588-09692022000100021&lang=es

Echeverría, M., Garaycoa, M., y Tusev, A. (2020). Are Ecuadorian Millennials prepared against a cyberattacj? *Revista Chakiñan de Ciencias Sociales y Humanidades, (10),* 73-86. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2550-67222020000100073&lang=es

García, D. (2018). El Phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (1402/2016). *Revista Bolivariana de Derecho,* (25), 650-659. https://dialnet.unirioja.es/servlet/articulo?codigo=6263417

Gómez, J. (2020). El tratamiento jurídico penal por parte del fiscal en los delitos informáticos contra el patrimonio, Distrito Judicial de Lima Norte 2019. https://alicia.concytec.gob.pe/vufind/Record/UCVV_5a763a62ab78eb7062003ac9bc69d112

González, J. (2020). Comercio electrónico en China y México: surgimiento, evolución y perspectivas. *México y la cuenca del pacífico*, *9*(27), 53-84. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-53082020000300053

Hernández, R. (2014). La investigación cualitativa a través de entrevistas: su análisis mediante la teoría fundamentada. *Revista de ciencias de la educación.* 187-210. https://dialnet.unirioja.es/servlet/articulo?codigo=4909706

Herrero, J., Torres, A., Vivas, P. y Urueña, A. (2022). Smartphone addiction, social support, and cybercrime victimization: a discrete survival and growth mixture model. *Psychosocial Intervention*, *31(1),* 59-66.

http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1132-05592022000100005&lang=es

Herzog, F. (2009). Straftaten im Internet, Computerkriminalitat und die Cybercrime Convention. *Política criminal*, *4(8)*, 475-484. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-33992009000200006&lang=es

Jones, C. y Guzmán, J. (2022). Análisis de las técnicas de machine learning aplicadas en la detección de fraudes bancarios. *Ciencia y Tecnología Revista Científica Muldisciplinar, 22*(33), 114-122. https://dialnet.unirioja.es/servlet/articulo?codigo=8591813

López, B. (2018). El delito de estafa cometido a través de las redes sociales: problemas de investigación y enjuiciamiento. *Revista de Internet, derecho y política,* (27), 42-51. https://dialnet.unirioja.es/servlet/articulo?codigo=7329022

Mabeka, N. y Cassim, F. (2023). Interpreting the provisions of the Cybercrimes Act 19 of 2020 in the context of civil procedure: a future journey Obiter. *44 (1),* 19-32. http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1682-58532023000100002&lng=en&tlng=en.

Mayer, L. (2017). El bien jurídico protegido en los delitos informáticos. *Revista chilena de derecho y tecnología. 44*(1), 261-285. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-34372017000100011&lang=es

Mayer, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Ius et Praxis*, *24*(1), 159-206. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122018000100159&lang=es

Mayer, L. y Oliver, G. (2020). El delito de fraude informático: Concepto y delimitación. *Revista chilena de derecho y tecnología*, *9*(1), 151-

184. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000100151

Mayer, L. y Vera, J. (2020). El delito de espionaje informático: Concepto y delimitación. *Revista chilena de derecho y tecnología, 9*(2), 221-256. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000200221&lang=es

Mayer, L y Vera, J. (2022). La falsificación informática: ¿un delito necesario?. *Revista chilena de derecho y tecnología, 11*(1), 261-286. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842022000100261&lang=es

Mejía, M., Hurtado, S. y Grisales, A. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones. *Revista de ciencias sociales, 29*(2), 356-372. https://dialnet.unirioja.es/servlet/articulo?codigo=8920556

Ortiz, R. (2019). *Investigación de fraude digital: Pueblo de Puerto Rico Vs. Luz María Soto Barreto* [Tesis de maestría, EDP University of Puerto Rico, INC] PRC Repositorio. https://prcrepository.org/xmlui/handle/20.500.12475/1240

Organización Mundial del Comercio (OMC, 2021). *Entender la OMC: cuestiones transversales y cuestiones nuevas.* https://www.wto.org/spanish/thewto_s/whatis_s/tif_s/tif_s.htm

Páramo, D. (2015). La teoría fundamentada (Grounded Theory), metodología cualitativa de investigación científica. *Pensamiento & Gestión*, (39), 1-7. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1657-62762015000200001&lng=en&tlng=es.

Pardo, A. (2018). Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018. https://alicia.concytec.gob.pe/vufind/Record/UCVV_4d4beb28faf17510d395af8ea626dca2

Paz, A. (2018). La culpa del consumidor en la responsabilidad financiera y su proyección causar en el daño por fraude electrónico. Una mirada a la jurisprudencia de la Delegatura para Funciones Jurisdiccionales de la Superintendencia Financiera de Colombia. *Revista de Derecho Privado, 35*, 261-289. https://dialnet.unirioja.es/servlet/articulo?codigo=7013328

Piza, N., Amaiquema, F. y Beltrán, G. (2019). Métodos y Técnicas en la Investigación cualitativa. Algunas precisiones necesarias. *Conrado*, *15*(70), 455-459. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442019000500455

Rodas, P. y Loor, E. (2018). Proceso de formación en tipificación en el código orgánico integral penal para los delitos cibernéticos. *Revista Iberoamericana de la Educación, 1*(1), 42-79. https://dialnet.unirioja.es/servlet/articulo?codigo=8489061

Rodríguez, J., Oduber, J. y Mora, E. (2017). Actividades rutinarias y cibervictimización en Venezuela. *URVIO Revista Latinoamericana de Estudios de Seguridad, (20),* 63-79. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-42992017000200063&lang=es

Sabillon, R. (2018). A Practical Model to Perform Comprehensive Cybersecurity Audits. *Enfoque UTE, 9(1),* 127-137. https://dialnet.unirioja.es/servlet/articulo?codigo=8314336

Saltos, M., Robalino, J. y Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. *Conrado*, *17*(78), 343-351. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442021000100343&lng=es&tlng=es.

Santillán, A., Vinueza, N. y Benavides, C. (2021). Derecho, informática y corrupción. Un enfoque a la realidad ecuatoriana. *Dilemas contemporáneos: educación, política y valores, 9(1).* https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-78902021000800106&lang=es

Tracy, S. (2021). Calidad cualitativa: ocho pilares para una investigación cualitativa de calidad. *Márgenes, Revista de Educación de la Universidad de Málaga, 2*(2), 173-201. https://dialnet.unirioja.es/servlet/articulo?codigo=8049668

Silva de García, P. y Edimara, L. (2018). A influência da injustiça organizacional na motivação para a prática de crimes cibernéticos. *JISTEM J.* https://www.scielo.br/j/jistm/a/3Qj7Xvdg9Sd3T6RFNHvSbWB/?lang=pt#

Warikandwa, T. V. (2021). Personal Data Security in South Africa's Financial Services Market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation Compared. *Potchefstroom Electronic Law Journal (PELJ)*, *24*(1), 1-32. http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1727-37812021000100033&lang=es

Zuña, E. R., Arce, A., Romero, W. y Soledispa, C. (2019). Análisis de la seguridad de la información en las PYMES de la ciudad de Milagro. *Revista Universidad y Sociedad, 11*(4), 487-492. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000400487&lng=es&tlng=es.

# ANEXOS

## ANEXO I – MATRIZ DE COHERENCIA INTERNA

| TÍTULO | FORMULACIÓN DEL PROBLEMA | OBJETIVO GENERAL | OBJETIVOS ESPECÍFICOS | SUPUESTO | TIPO | DISEÑO DE INVESTIGA-CIÓN | PARTICIPANTES | TÉCNICAS E INSTRUMEN-TOS |
|---|---|---|---|---|---|---|---|---|
| Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022. | ¿Cómo fue el tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, durante el periodo 2022? | Analizar el tratamiento de los casos de delitos informáticos contra el patrimonio que se presentaron en el Distrito Fiscal del Santa, durante el periodo 2022. | - Examinar el tratamiento de los casos de compras fraudulentas por internet que se investigaron en el Distrito Fiscal del Santa.<br>- Distinguir el tratamiento de los casos de fraude en las operaciones y transferencias electrónicas que se investigaron en el Distrito Fiscal del Santa.<br>- Plantear un proyecto de ley donde se especifique la tipificación de los delitos informáticos contra el | El tratamiento de los casos de delitos informáticos contra del patrimonio en el Distrito Fiscal del Santa durante el periodo 2022 fue deficiente, en primer lugar, por la regulación tan general de los delitos informáticos contra el patrimonio en nuestro ordenamiento jurídico penal, en segundo lugar, por no contar con la tecnología necesaria y en tercer lugar, ante la falta de implementación de oficinas descentralizadas | - Enfoque o Paradigma: Cualitativo<br>- Tipo de investigación: Básica | Jurídico propositivo | - 03 Magistrados de la Corte Superior de Justicia del Santa<br>- 07 Fiscales del Ministerio Público del Distrito Fiscal del Santa<br>- 05 Abogados especializados en lo penal<br>- 05 Agentes de la División de investigación de delitos de alta tecnología (DIVINDAT) | Técnicas:<br>- Entrevista<br>- Encuesta<br>-Análisis documental<br>Instrumentos:<br>- Guía de entrevista<br>- Cuestionario<br>- Guía de análisis documental |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | patrimonio en el ordenamiento jurídico penal peruano. | de la división de investigación de delitos de alta tecnología de la policía nacional (DIVINDAT) en el Distrito Fiscal del Santa | | | | |

## ANEXO 2 - TABLA DE CATEGORIZACIÓN

| Categorías | Subcategorías | Descripción |
|---|---|---|
| **Delitos informáticos** | – Concepto | – Descripción |
| | – Ciberdelincuencia | – Preceptos<br>– Convención sobre la Ciberdelincuencia |
| | – Ordenamiento Jurídico | - Nacional e internacional |
| | – El bien jurídico penal | – Norma |
| | - Órganos especializados | – Unidad Fiscal Especializada en Ciberdelincuencia<br>– DIVINDAT (PNP) |
| **Delitos contra el patrimonio** | – Concepto | – Descripción |
| | – Base Legal | - Código penal |

## ANEXO 3 - GUÍA DE ENTREVISTA

UNIVERSIDAD CÉSAR VALLEJO

**DATOS PERSONALES DEL ENTREVISTADO**

- **NOMBRE COMPLETO:** ……
- **LUGAR DE TRABAJO:** ……
- **FUNCIÓN DESEMPEÑADA:** ……
- **FECHA DE ENTREVISTA:** ……

**TÍTULO: TRATAMIENTO DE LOS CASOS DE DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO EN EL DISTRITO FISCAL DEL SANTA, 2022**

**Objetivo General:** Analizar el tratamiento de los casos de delitos informáticos contra el patrimonio que se presentaron en el Distrito Fiscal del Santa durante el periodo 2022.

1. ¿Considera Ud. que, el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096 regula eficazmente el delito de fraude informático? SI - NO ¿Por qué?

   ……

   ……

   ……

   ……

2. ¿Considera Ud. que, en nuestro ordenamiento jurídico peruano se prevé mecanismos para poder detener, prevenir y sancionar los delitos informáticos contra el patrimonio? SI - NO ¿Por qué?

   ……

   ……

   ……

   ……

3. ¿Qué opinión le merece el aumento progresivo de las denuncias por la presunta comisión del delito de fraude informático, durante el periodo 2022?

……..…
……...
……...
..……..

4. ¿Considera Ud. que, los fiscales y funcionarios de las Fiscalías Corporativas Penales deben ser capacitados para abordar e investigar eficientemente los delitos informáticos contra el patrimonio? SI- NO ¿Por qué?

……..…
……...
……...
..……..…

| |
|---|
| **Objetivo Específico 1:** Examinar el tratamiento de los casos de compras fraudulentas por internet que se investigaron en el Distrito Fiscal del Santa, durante el periodo 2022. |

5. ¿Cuál cree Ud. que, es la principal razón por la cual se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet?

……..…
……...
……...
..……..…

6. ¿Considera Ud. que, existen otras razones por la cuales se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet?

……
……

7. ¿Cuál considera Ud. que, sería el aporte de los miembros de la Unidad Fiscal especializada en Ciberdelincuencia del Ministerio Público en la persecución de los presuntos autores del ilícito penal de compras fraudulentas por internet?

……...…
……...
……...
..……..…

**Objetivo Específico 2:** Distinguir el tratamiento de los casos de fraude en las operaciones y transferencias electrónicas que se investigaron en el Distrito Fiscal del Santa, durante el periodo 2022.

8. ¿Considera Ud. que, es necesaria la actuación de los agentes policiales de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) en las investigaciones aperturadas por la presunta comisión del delito de fraude en las operaciones y transferencias electrónicas? SI - NO ¿Por qué?

……...…
……...
……...
..……..…

9. ¿Considera Ud. que, las entidades financieras aplican eficientemente sus métodos de seguridad para proteger las cuentas de sus usuarios de fraudes realizados mediante operaciones o transferencias electrónicas? SI – NO ¿Por qué?

……...…
……...
……...
..……..…

**Objetivo Específico 3:** Plantear un proyecto de Ley donde se especifique la tipificación de los delitos informáticos contra el patrimonio en el ordenamiento jurídico penal peruano.

10. ¿Qué deficiencias legislativas advierte Ud. en la tipificación del delito de fraude informático en el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096?

……..…
……...
……...
..……..…

11. ¿Considera Ud. que, se debe modificar el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096 que regula el delito de Fraude Informático en aras de una mejor aplicación? SI - NO ¿Por qué?

……..…
……...
……...
..……..…

12. Finalmente, ¿tiene Ud. alguna propuesta de solución o anotación que aportar con relación al delito de fraude informático?

……..…
……...
……...
..……..…
……...
..……..…

**ANEXO 4 – CUESTIONARIO**

UNIVERSIDAD CÉSAR VALLEJO

**TÍTULO: TRATAMIENTO DE LOS CASOS DE DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO EN EL DISTRITO FISCAL DEL SANTA, 2022.**

**INSTRUCCIONES:**

Señor encuestado se le solicita que conteste el siguiente cuestionario en forma anónima y con honestidad para así desarrollar la investigación señalada, se agradece de antemano por su colaboración.

**CONDICIÓN:**

Juez ☐ Fiscal ☐ Abogado ☐

Agente policial de la DIVINDAT ☐

**PREGUNTAS:**

1. ¿Considera Ud. que, en el Perú se regula eficazmente el delito de fraude informático?

   SI ☐ NO ☐ NO PRECISA ☐

2. ¿Considera Ud. que, en nuestro ordenamiento jurídico peruano existen mecanismos para detener, prevenir y/o sancionar los delitos informáticos?

   SI ☐ NO ☐ NO PRECISA ☐

3. ¿Considera Ud. que, el aumento progresivo de denuncias por fraude informático se debe a la insuficiente regulación de este delito?

SI ☐ NO ☐ NO PRECISA ☐

4. ¿Estima Ud. que, los fiscales y funcionarios de las Fiscalías Corporativas Penales están capacitados para investigar eficientemente los delitos informáticos?

SI ☐ NO ☐ NO PRECISA ☐

5. ¿Considera Ud. que, el motivo principal de archivamiento a nivel preliminar de las investigaciones por compras fraudulentas por internet es la deficiente regulación del delito de fraude informático?

SI ☐ NO ☐ NO PRECISA ☐

6. ¿Considera Ud. que, existen otros motivos por los cuales se archiva a nivel preliminar las investigaciones por compras fraudulentas por internet?

SI ☐ NO ☐ NO PRECISA ☐

7. ¿Considera Ud. determinante la participación de la Unidad Especializada en ciberdelincuencia del Ministerio Publico para la eficaz persecución del ilícito penal de compras fraudulentas por internet?

SI ☐ NO ☐ NO PRECISA ☐

8. ¿Considera Ud. que, es necesaria la actuación de los agentes policiales de la DIVINDAT en las investigaciones por fraude mediante operaciones o transferencias electrónicas?

SI ☐ NO ☐ NO PRECISA ☐

9. ¿Considera Ud. que, las entidades financieras brindan seguridad jurídica a sus usuarios ante posibles fraudes informáticos?

SI ☐ NO ☐ NO PRECISA ☐

10. ¿Considera Ud. que, existen vacíos legales en el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096?

SI ☐ NO ☐ NO PRECISA ☐

11. ¿Considera Ud. que, se debe modificar el artículo 8° de la Ley N°30096 referente al delito de fraude informático?

SI ☐ NO ☐ NO PRECISA ☐

## ANEXO 5 – GUIA DE ANÁLISIS DE FUENTE DOCUMENTAL

**Título:** Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022.

**Objetivo General:** Analizar el tratamiento de los casos de delitos informáticos contra el patrimonio que se presentaron en el Distrito Fiscal del Santa, durante el periodo 2022.

**AUTORES:** Wendy Aracely De La Cruz Cherres
Juan Antonio Lulli Cáceres

**FECHA:** 25 de julio de 2023

| | |
|---|---|
| Fuente documental | Ley de delitos informáticos N°30096, con modificatoria posterior en la Ley N°30171. |
| Contenido de la fuente a analizar | Artículo 8. Fraude Informático.<br>El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de la libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa.<br>La pena será privativa de libertad no menor de cinco ni mayo de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o programas de apoyo social. |
| Análisis de contenido | La actual regulación de fraude informático no incluye los principales supuestos de hecho que se vienen presentando a diario en la práctica; asimismo, incurre en excesivos tecnicismos jurídicos al describir los verbos rectores y adolece de redundancia al especificarse que la conducta debe ser deliberada e ilegítima cuando se sobreentiende que es así por cuanto es un delito doloso. |
| Conclusión | Hoy en día, es meritorio modificar la tipificación de los delitos informáticos contra el patrimonio, por cuanto no aborda las diversas modalidades delictivas y su redacción genera confusión en su aplicación por los agentes del derecho. |

## ANEXO 6 – GUIA DE ANÁLISIS DE FUENTE DOCUMENTAL

**Título:** Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022.

**Objetivo Específico 1:** Examinar el tratamiento de los casos de compras fraudulentas por internet que se investigaron en el Distrito Fiscal del Santa, durante el periodo 2022.

**AUTORES:** Wendy Aracely De La Cruz Cherres
Juan Antonio Lulli Cáceres

**FECHA:** 25 de julio de 2023

| | |
|---|---|
| Fuente documental | Díaz, G. (2021). La auditoría forense como fundamento metodológico en la detección de casos de fraudes informáticos. *Revista Gestión I+D,* *6*(2), 315-351. https://dialnet.unirioja.es/servlet/articulo?codigo=8737229 |
| Contenido de la fuente a analizar | La evidencia digital se define como cualquier dato almacenado o transmitido mediante una computadora que respalda o refuta una teoría de cómo ocurrió un delito o que aborda elementos críticos del delito, como la intención o la coartada; los datos referidos en esta definición son esencialmente una combinación de números que representan información de varios tipos, incluidos texto, imágenes, audio y video. |
| Análisis de contenido | De lo antes referido, se desprende que la evidencia digital está constituida por los rastros que deja el sujeto agente en un equipo informático y que posibilita confirmar la ejecución de una acción por un usuario o intruso en un determinado sistema informático. Adicionalmente, puede revelar la correspondencia online entre los imputados y la víctima. |
| Conclusión | La evidencia digital coadyuva en la investigación por fraude informático, permitiendo enlazar al imputado con las víctimas puesto que los registros únicos que dejan en un equipo informático posibilitan desvirtuar la presunción de inocencia que le asiste a todo investigado |

## ANEXO 7 – GUIA DE ANÁLISIS DE FUENTE DOCUMENTAL

**Título:** Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022.

**Objetivo Específico 2:** Distinguir el tratamiento de los casos de fraude en las operaciones y transferencias electrónicas que se en el Distrito Fiscal del Santa, durante el periodo 2022.

**AUTORES:** Wendy Aracely De La Cruz Cherres
Juan Antonio Lulli Cáceres

**FECHA:** 25 de julio de 2023

| | |
|---|---|
| Fuente documental | Jones, C. y Guzmán, J. (2022). Análisis de las técnicas de machine learning aplicadas en la detección de fraudes bancarios. *Ciencia y Tecnología Revista Científica Muldisciplinar, 22*(33), 114-122. https://dialnet.unirioja.es/servlet/articulo?codigo=8591813 |
| Contenido de la fuente a analizar | Se considera al aprendizaje automático o de máquinas (machine learning en inglés), como un subárea en el campo de la computación e informática, además de estar estrechamente ligada a la inteligencia artificial; el objetivo de esta técnica es lograr que los ordenadores aprendan, siendo un agente que mejore la experiencia; ha sido muy útil sobre todo para el análisis de investigaciones y procesos que generan grandes cantidades de datos. |
| Análisis de contenido | Las técnicas del machine learning soy hoy en día los métodos líderes en la detección de fraudes bancarios, pues bajo el concepto de que los ordenadores aprenden de sí y de los datos que en ellos se plasman, mediante algoritmos pueden identificar patrones en la conducta de los sujetos agentes, contribuyendo en la prevención y erradicación de la ciberdelincuencia. |
| Conclusión | Es menester resaltar la importancia de incluir las técnicas del machine learning en la detección de fraudes informáticos, ya que estos métodos sofisticados permiten plasmar patrones en los ordenadores que evidencien previamente la acción ilegal de un usuario. |

## ANEXO 8 – GUIA DE ANÁLISIS DE FUENTE DOCUMENTAL

**Título:** Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022.

**Objetivo Específico 3:** Plantear un proyecto de Ley donde se especifique la tipificación de los delitos informáticos contra el patrimonio en el ordenamiento jurídico penal peruano.

**AUTORES:** Wendy Aracely De La Cruz Cherres
Juan Antonio Lulli Cáceres

**FECHA:** 25 de julio de 2023

| | |
|---|---|
| Fuente documental | Convenio sobre la Ciberdelincuencia. Budapest, 23.XI.2001 |
| Contenido de la fuente a analizar | Título 2: delitos informáticos:<br><br>"Artículo 8 – Fraude Informático. Las partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a) La introducción, alteración, borrado o supresión de datos informáticos; b) Cualquier interferencia en el funcionamiento de un sistema informático,<br>Con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona. |
| Análisis de contenido | El Perú suscribió el Convenio sobre la Ciberdelincuencia en noviembre del 2001, por ende, está obligado a tipificar los delitos informáticos; sin embargo, recién en el año 2013 promulgó la Ley N°30096, con su posterior modificatoria en la Ley N°30171. Aceptando así las pautas que menciona dicho convenio sobre las que debe apoyarse las normas de derecho interno que vendrán a regular estos actos ilícitos. |
| Conclusión | Nuestro ordenamiento jurídico penal peruano regula los delitos informáticos; empero, resulta desfasada respecto a las nuevas modalidades que se presentan en la práctica, de allí la necesidad de modificar su fórmula legal en aras de coadyuvar a la labor fiscal y lograr la función de prevención y sanción efectiva de la norma. |

## ANEXO 9 – MATRIZ EVALUACIÓN POR JUICIO DE EXPERTOS

UNIVERSIDAD CÉSAR VALLEJO

**DATOS PERSONALES DEL ENTREVISTADO**

- **NOMBRE COMPLETO:** ……
- **LUGAR DE TRABAJO:** ……
- **FUNCIÓN DESEMPEÑADA:** ……
- **FECHA DE ENTREVISTA:** ……

**TÍTULO: TRATAMIENTO DE LOS CASOS DE DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO EN EL DISTRITO FISCAL DEL SANTA, 2022**

**Objetivo General:** Analizar el tratamiento de los casos de delitos informáticos contra el patrimonio que se presentaron en el Distrito Fiscal del Santa durante el periodo 2022.

1. ¿Considera Ud. que, el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096 regula eficazmente el delito de fraude informático? SI - NO ¿Por qué?

   ……

   ……

   ……

   ……

2. ¿Considera Ud. que, en nuestro ordenamiento jurídico peruano se prevé mecanismos para poder detener, prevenir y sancionar los delitos informáticos contra el patrimonio? SI - NO ¿Por qué?

   ……

   ……

   ……

   ……

3. ¿Qué opinión le merece el aumento progresivo de las denuncias por la presunta comisión del delito de fraude informático, durante el periodo 2022?

……...…
……...
……...
..……..

4. ¿Considera Ud. que, los fiscales y funcionarios de las Fiscalías Corporativas Penales deben ser capacitados para abordar e investigar eficientemente los delitos informáticos contra el patrimonio? SI- NO ¿Por qué?

……...…
……...
……...
..……..…

| |
|---|
| **Objetivo Específico 1:** Examinar el tratamiento de los casos de compras fraudulentas por internet que se investigaron en el Distrito Fiscal del Santa, durante el periodo 2022. |

5. ¿Cuál cree Ud. que, es la principal razón por la cual se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet?

……...…
……...
……...
..……..…

6. ¿Considera Ud. que, existen otras razones por la cuales se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet?

……
……

7. ¿Cuál considera Ud. que, sería el aporte de los miembros de la Unidad Fiscal especializada en Ciberdelincuencia del Ministerio Público en la persecución de los presuntos autores del ilícito penal de compras fraudulentas por internet?

……...…
……...
……....
..……..…

**Objetivo Específico 2:** Distinguir el tratamiento de los casos de fraude en las operaciones y transferencias electrónicas que se investigaron en el Distrito Fiscal del Santa, durante el periodo 2022.

8. ¿Considera Ud. que, es necesaria la actuación de los agentes policiales de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) en las investigaciones aperturadas por la presunta comisión del delito de fraude en las operaciones y transferencias electrónicas? SI - NO ¿Por qué?

……...…
……...
……....
..……..…

9. ¿Considera Ud. que, las entidades financieras aplican eficientemente sus métodos de seguridad para proteger las cuentas de sus usuarios de fraudes realizados mediante operaciones o transferencias electrónicas? SI – NO ¿Por qué?

……...…
……...
……....
..……..…

**Objetivo Específico 3:** Plantear un proyecto de Ley donde se especifique la tipificación de los delitos informáticos contra el patrimonio en el ordenamiento jurídico penal peruano.

10. ¿Qué deficiencias legislativas advierte Ud. en la tipificación del delito de fraude informático en el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096?

    ……..…
    ……...
    ……....
    ..……..…

11. ¿Considera Ud. que, se debe modificar el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096 que regula el delito de Fraude Informático en aras de una mejor aplicación? SI - NO ¿Por qué?

    ……..…
    ……...
    ……....
    ..……..…

12. Finalmente, ¿tiene Ud. alguna propuesta de solución o anotación que aportar con relación al delito de fraude informático?

    ……..…
    ……...
    ……....
    ..……..…
    ……....
    ..……..…

# EVALUACIÓN POR JUICIO DE EXPERTOS

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento Guía de entrevista, a fin de conocer como se viene ejecutando el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022. La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente. Agradecemos su valiosa colaboración.

**1. Datos generales del juez:**

| | |
|---|---|
| **Nombre del juez:** | Maggye Gabriela López Agüero. |
| **Grado profesional:** | Maestría **( X )** Doctor ( ) |
| **Área de formación académica:** | Pregrado Universidad Privada del Norte<br>Posgrado Universidad César Vallejo |
| **Áreas de experiencia profesional:** | Derecho Civil, Administrativo, Penal, Conciliación Extrajudicial. |
| **Institución donde labora:** | Gerente de Asesoría Jurídica de la Municipalidad Distrital de Jesús - Cajamarca. |
| **Tiempo de experiencia profesional en el área:** | 2 a 4 años ( ) Más de 5 años ( X ) |
| **Experiencia en Investigación /Temática** (si corresponde) | Título de estudio realizado. |

**2. Propósito de la evaluación:**

Validar el contenido del instrumento guía de entrevista por juicio de expertos, conocedores del tema.

**3. Datos del instrumento**

Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022.

| | |
|---|---|
| Nombre de la Prueba: | Guía de entrevista para analizar el tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022. |
| Autores: | De la Cruz Cherres, Wendy Aracely<br>Lulli Cáceres, Juan Antonio |
| Procedencia: | Chimbote. |
| Administración: | Abogados especialistas de manera presencial. |
| Tiempo de aplicación: | 30 a 50 minutos. |
| Ámbito de aplicación: | Especialistas conocedores del tema en el Distrito Fiscal del Santa. |
| Significación: | El instrumento da a conocer el Tratamiento de los casos de delitos informáticos contra el en el Distrito Fiscal del Santa, 2022; además, tiene enfoques conceptuales vinculados a las categorías de estudio, las cuales sustentan y enriquecen la temática a investigar. |

**4. Soporte técnico**

mediante el uso de las TIC (Tecnologías de la Información y Comunicaciones) logra apropiarse con conocimiento e intención de la información financiera de cualquier persona natural o jurídica, causando una afectación ilegal en su esfera patrimonial,

| Instrumento /Área | Subescalas (categorías) | Definición |
|---|---|---|
| **Delitos informáticos** | – Concepto | - Cometidos mediante el uso de las TIC con el fin de apropiarse de la información personal y financiera de cualquier persona natural o jurídica. |
| | – Ciberdelincuencia | - Convenio sobre la Ciberdelincuencia en Budapest |
| | – Ordenamiento Jurídico | - Ley N°30096 y su modificatoria Ley N°30171 |
| | – El bien jurídico penal | - Internet<br>- Funcionalidad informática |
| | - Órganos especializados | - Unidad Fiscal Especializada en Ciberdelincuencia<br>- División de Investigación de Delitos de Alta Tecnología (DIVINDAT) |
| **Delitos contra el patrimonio** | – Concepto | - Perpetrados con dolo mediante el uso de la fuerza o amenaza. |
| | – Base Legal | - Código Penal Peruano |

**5. Presentación de instrucciones para el juez**

A continuación, le presento el instrumento Guía de Entrevista relacionado al Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022, elaborado por Wendy Aracely De La Cruz Cherres y Juan Antonio Lulli Cáceres en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

| Categoría | Calificación | Indicador |
|---|---|---|
| **CLARIDAD** El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas. | 1. No cumple con el criterio | El ítem no es claro. |
| | 2. Bajo Nivel | El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de éstas. |
| | 3. Moderado nivel | Se requiere una modificación muy específica de algunos de los términos del ítem. |
| | 4. Alto nivel | El ítem es claro, tiene semántica y sintaxis adecuada. |
| **COHERENCIA** El ítem tiene relaciónlógica con la dimensión o indicador que está midiendo. | 1. Totalmente en Desacuerdo (nocumple con el criterio) | El ítem no tiene relación lógica con la dimensión. |
| | 2. Desacuerdo(bajonivel de acuerdo) | El ítem tiene una relación tangencial /lejana con ladimensión. |
| | 3. Acuerdo (moderado nivel) | El ítem tiene una relación moderada con la dimensión que se está midiendo. |
| | 4. Totalmente de acuerdo (alto nivel) | El ítem se encuentra está relacionado con la dimensión que está midiendo. |
| **RELEVANCIA** El ítem es esencial o importante, es decir debe ser incluido. | 1. No cumple con el criterio | El ítem puede ser eliminado sin que se vea. |
| | 2. Bajo Nivel | El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste. |
| | 3. Moderado nivel | El ítem es relativamente importante. |
| | 4. Alto nivel | El ítem es muy relevante y debe ser incluido. |

*Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente.*

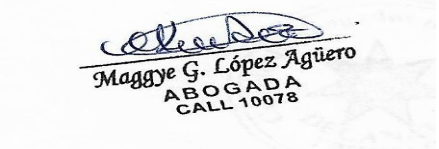
| | |
|---|---|
| CALIFICACIÓN | 1. No cumple con el criterio |
| | 2. Bajo Nivel |
| | 3. Moderado nivel |
| | 4. Alto nivel |

**Categorías del instrumento:**

- Primera categoría: Delitos informáticos
- Segunda categoría: Delitos contra el patrimonio
- Objetivos de las Categorías: Determinar el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, durante el periodo 2022.

| SUB CATE-GORÍAS | Ítem | Claridad | | | | Coherencia | | | | Relevancia | | | | Observa-ciones/ Recomen-daciones |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | |
| 1 | ¿Considera Ud. que, el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096 regula eficazmente el delito de fraude informático? SI - NO ¿Por qué? | | | | X | | | X | | | | X | | |
| 2 | ¿Considera Ud. que, en nuestro ordenamiento jurídico peruano se prevé mecanismos para poder detener, prevenir y sancionar los delitos informáticos contra el patrimonio? SI - NO ¿Por qué? | | | | X | | | X | | | | X | | |
| 3 | ¿Qué opinión le merece el aumento progresivo de las denuncias por la presunta comisión del delito de fraude informático, durante el periodo 2022? | | | X | | | | | X | | | X | | |
| 4 | ¿Considera Ud. que, los fiscales y funcionarios de las Fiscalías Corporativas Penales deben ser capacitados para abordar e investigar eficientemente los delitos informáticos contra el patrimonio? SI- NO ¿Por qué? | | | | X | | | | X | | | X | | |
| 5 | ¿Cuál cree Ud. que, es la principal razón por la cual se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet? | | | X | | | | X | | | | X | | |
| 6 | ¿Considera Ud. que, existen otras razones por las cuales se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet? | | | X | | | | X | | | | X | | |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | ¿Cuál considera Ud. que, sería el aporte de los miembros de la Unidad Fiscal especializada en Ciberdelincuencia del Ministerio Público en la persecución de los presuntos autores del ilícito penal de compras fraudulentas por internet? | | | | X | | | X | | | | | | X | |
| 8 | ¿Considera Ud. que, es necesaria la actuación de los agentes policiales de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) en las investigaciones aperturadas por la presunta comisión del delito de fraude en las operaciones o transferencias electrónicas? SI - NO ¿Por qué? | | | | X | | | X | | | | X | | | |
| 9 | ¿Considera Ud. que, las entidades financieras aplican eficientemente sus métodos de seguridad para proteger las cuentas de sus usuarios de fraudes realizados mediante operaciones y transferencias electrónicas? SI – NO ¿Por qué? | | | | X | | | X | | | | X | | | |
| 10 | ¿Qué deficiencias legislativas advierte Ud. en la tipificación del delito de fraude informático en la Ley de Delitos Informáticos – Ley N°30096? | | | X | | | | X | | | | | | X | |
| 11 | ¿Considera Ud. que, se debe modificar el artículo 8° de la Ley de Delitos Informáticos – Ley N°30096 que regula el delito de Fraude Informático en aras de una mejor aplicación? SI - NO ¿Por qué? | | | X | | | | X | | | | X | | | |
| 12 | Finalmente, ¿tiene Ud. alguna propuesta de solución o anotación que aportar con relación al delito de fraude informático? | | | X | | | | | X | | | | | X | |




Firma del
experto

# EVALUACIÓN POR JUICIO DE EXPERTOS

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento Guía de entrevista, a fin de conocer como se viene ejecutando el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022. La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente. Agradecemos su valiosa colaboración.

**1. Datos generales del juez:**

| | |
|---|---|
| **Nombre del juez:** | Melva Eudomilia Sánchez Medina. |
| **Grado profesional:** | Maestría ( **X** ) Doctor () |
| **Área de formación académica:** | Pregrado Universidad César Vallejo<br>Posgrado Universidad César Vallejo |
| **Áreas de experiencia profesional:** | Derecho Civil, Administrativo, Penal, Conciliación Extrajudicial. |
| **Institución donde labora:** | Universidad César Vallejo |
| **Tiempo de experiencia profesional en el área:** | 2 a 4 años ( ) Más de 5 años ( **X** ) |
| **Experiencia en Investigación /Temática** (si corresponde) | Título de estudio realizado. |

**2. Propósito de la evaluación:**

Validar el contenido del instrumento guía de entrevista por juicio de expertos, conocedores del tema.

**3.** Datos del instrumento

Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022.

| | |
|---|---|
| Nombre de la Prueba: | Guía de entrevista para analizar el tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022. |
| Autores: | De la Cruz Cherres, Wendy Aracely<br>Lulli Cáceres, Juan Antonio |
| Procedencia: | Chimbote. |
| Administración: | Abogados especialistas de manera presencial. |
| Tiempo de aplicación: | 30 a 50 minutos. |
| Ámbito de aplicación: | Especialistas conocedores del tema en el Distrito Fiscal del Santa. |
| Significación: | El instrumento da a conocer el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022; además, tiene enfoques conceptuales vinculados a las categorías de estudio, lascuales sustentan y enriquecen la temática a investigar. |

## 4. Soporte técnico

| Instrumento /Área | Subescalas (categorías) | Definición |
|---|---|---|
| **Delitos informáticos** | – Concepto | - Cometidos mediante el uso de las TIC con el fin de apropiarse de la información personal y financiera de cualquier persona natural o jurídica. |
| | – Ciberdelincuencia | - Convenio sobre la Ciberdelincuencia en Budapest |
| | – Ordenamiento Jurídico | - Ley N°30096 y su modificatoria Ley N°30171 |
| | – El bien jurídico penal | - Internet<br>- Funcionalidad informática |
| | - Órganos especializados | - Unidad Fiscal Especializada en Ciberdelincuencia<br>- División de Investigación de Delitos de Alta Tecnología (DIVINDAT) |
| **Delitos contra el patrimonio** | – Concepto | - Perpetrados con dolo mediante el uso de la fuerza o amenaza. |
| | – Base Legal | - Código Penal Peruano |

## 5. Presentación de instrucciones para el juez

A continuación, le presento el instrumento Guía de Entrevista relacionado al Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022, elaborado por Wendy Aracely De La Cruz Cherres y Juan Antonio Lulli Cáceres en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

| Categoría | Calificación | Indicador |
|---|---|---|
| **CLARIDAD** El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas. | 1. No cumple con el criterio | El ítem no es claro. |
| | 2. Bajo Nivel | El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de éstas. |
| | 3. Moderado nivel | Se requiere una modificación muy específica de algunos de los términos del ítem. |
| | 4. Alto nivel | El ítem es claro, tiene semántica y sintaxis adecuada. |
| **COHERENCIA** El ítem tiene relaciónlógica con la dimensión o indicador que está midiendo. | 1. Totalmente en Desacuerdo (nocumple con el criterio) | El ítem no tiene relación lógica con la dimensión. |
| | 2. Desacuerdo(bajonivel de acuerdo) | El ítem tiene una relación tangencial /lejana con ladimensión. |
| | 3. Acuerdo (moderado nivel) | El ítem tiene una relación moderada con la dimensión que se está midiendo. |
| | 4. Totalmente de acuerdo (alto nivel) | El ítem se encuentra está relacionado con la dimensión que está midiendo. |
| **RELEVANCIA** El ítem es esencial o importante, es decir debe ser incluido. | 1. No cumple con el criterio | El ítem puede ser eliminado sin que se vea. |
| | 2. Bajo Nivel | El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste. |
| | 3. Moderado nivel | El ítem es relativamente importante. |
| | 4. Alto nivel | El ítem es muy relevante y debe ser incluido. |

*Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente.*

| | |
|---|---|
| CALIFICACIÓN | 1. No cumple con el criterio |
| | 2. Bajo Nivel |
| | 3. Moderado nivel |
| | 4. Alto nivel |

**Categorías del instrumento:**

- Primera categoría: Delitos informáticos
- Segunda categoría: Delitos contra el patrimonio
- Objetivos de las Categorías: Determinar el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, durante el periodo 2022.

| SUB CATE-GORÍAS | Ítem | Claridad | | | | Coherencia | | | | Relevancia | | | | Observa-ciones/ Recomen-daciones |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | |
| 1 | ¿Considera Ud. que, el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096 regula eficazmente el delito de fraude informático? SI - NO ¿Por qué? | | | | X | | | | X | | | | X | |
| 2 | ¿Considera Ud. que, en nuestro ordenamiento jurídico peruano se prevé mecanismos para poder detener, prevenir y sancionar los delitos informáticos contra el patrimonio? SI - NO ¿Por qué? | | | | X | | | | X | | | X | | |
| 3 | ¿Qué opinión le merece el aumento progresivo de las denuncias por la presunta comisión del delito de fraude informático, durante el periodo 2022? | | | X | | | | | X | | | | X | |
| 4 | ¿Considera Ud. que, los fiscales y funcionarios de las Fiscalías Corporativas Penales deben ser capacitados para abordar e investigar eficientemente los delitos informáticos contra el patrimonio? SI- NO ¿Por qué? | | | X | | | | X | | | | X | | |
| 5 | ¿Cuál cree Ud. que, es la principal razón por la cual se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet? | | | X | | | | X | | | | X | | |
| 6 | ¿Considera Ud. que, existen otras razones por las cuales se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet? | | | X | | | | X | | | | | X | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | ¿Cuál considera Ud. que, sería el aporte de los miembros de la Unidad Fiscal especializada en Ciberdelincuencia del Ministerio Público en la persecución de los presuntos autores del ilícito penal de compras fraudulentas por internet? | | | | X | | | X | | | X | | |
| 8 | ¿Considera Ud. que, es necesaria la actuación de los agentes policiales de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) en las investigaciones aperturadas por la presunta comisión del delito de fraude en las operaciones o transferencias electrónicas? SI - NO ¿Por qué? | | | | X | | | X | | | | X | |
| 9 | ¿Considera Ud. que, las entidades financieras aplican eficientemente sus métodos de seguridad para proteger las cuentas de sus usuarios de fraudes realizados mediante operaciones y transferencias electrónicas? SI – NO ¿Por qué? | | | | X | | | X | | | | X | |
| 10 | ¿Qué deficiencias legislativas advierte Ud. en la tipificación del delito de fraude informático en la Ley de Delitos Informáticos – Ley N°30096? | | | X | | | | X | | | | X | |
| 11 | ¿Considera Ud. que, se debe modificar el artículo 8° de la Ley de Delitos Informáticos – Ley N°30096 que regula el delito de Fraude Informático en aras de una mejor aplicación? SI - NO ¿Por qué? | | | X | | | | X | | | | X | |
| 12 | Finalmente, ¿tiene Ud. alguna propuesta de solución o anotación que aportar con relación al delito de fraude informático? | | | | X | | | X | | | X | | |


Firma del
experto

# EVALUACIÓN POR JUICIO DE EXPERTOS

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento Guía de entrevista, a fin de conocer como se viene ejecutando el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022. La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente. Agradecemos su valiosa colaboración.

**1. Datos generales del juez:**

| | |
|---|---|
| **Nombre del juez:** | Gastón Jorge Quevedo Pereyra. |
| **Grado profesional:** | Maestría ( ) Doctor ( **X** ) |
| **Área de formación académica:** | Doctor en Derecho<br>Magister en Derecho Civil y Comercial. |
| **Áreas de experiencia profesional:** | Coordinador de Maestría en Gestión y Control Gubernamental de la Escuela de Postgrado de la Universidad Inca Garcilaso de la Vega. |
| **Institución donde labora:** | Universidad Inca Garcilaso de la Vega. |
| **Tiempo de experiencia profesional en el área:** | 2 a 4 años ( ) Más de 5 años **( X** ) |
| **Experiencia en Investigación /Temática** (si corresponde) | Derecho Público y Derecho Económico |

**2. Propósito de la evaluación:**

Validar el contenido del instrumento guía de entrevista por juicio de expertos, conocedores del tema.

**3. Datos del instrumento**

Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022.

| | |
|---|---|
| Nombre de la Prueba: | Guía de entrevista para analizar el tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022. |
| Autores: | De la Cruz Cherres, Wendy Aracely<br>Lulli Cáceres, Juan Antonio |
| Procedencia: | Chimbote. |
| Administración: | Abogados especialistas de manera presencial. |
| Tiempo de aplicación: | 30 a 50 minutos. |
| Ámbito de aplicación: | Especialistas conocedores del tema en el Distrito Fiscal del Santa. |
| Significación: | El instrumento da a conocer el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022; además, tiene enfoques conceptuales vinculados a las categorías de estudio, las cuales sustentan y enriquecen la temática a investigar. |

## 4. Soporte técnico

| Instrumento /Área | Subescalas (categorías) | Definición |
|---|---|---|
| **Delitos informáticos** | – Concepto | - Cometidos mediante el uso de las TIC con el fin de apropiarse de la información personal y financiera de cualquier persona natural o jurídica. |
| | – Ciberdelincuencia | - Convenio sobre la Ciberdelincuencia en Budapest |
| | – Ordenamiento Jurídico | - Ley N°30096 y su modificatoria Ley N°30171 |
| | – El bien jurídico penal | - Internet<br>- Funcionalidad informática |
| | - Órganos especializados | - Unidad Fiscal Especializada en Ciberdelincuencia<br>- División de Investigación de Delitos de Alta Tecnología (DIVINDAT) |
| **Delitos contra el patrimonio** | – Concepto | - Perpetrados con dolo mediante el uso de la fuerza o amenaza. |
| | – Base Legal | - Código Penal Peruano |

## 5. Presentación de instrucciones para el juez

A continuación, le presento el instrumento Guía de Entrevista relacionado al Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022, elaborado por Wendy Aracely De La Cruz Cherres y Juan Antonio Lulli Cáceres en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

| Categoría | Calificación | Indicador |
|---|---|---|
| **CLARIDAD** El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas. | 1. No cumple con el criterio | El ítem no es claro. |
| | 2. Bajo Nivel | El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de éstas. |
| | 3. Moderado nivel | Se requiere una modificación muy específica de algunos de los términos del ítem. |
| | 4. Alto nivel | El ítem es claro, tiene semántica y sintaxis adecuada. |
| **COHERENCIA** El ítem tiene relaciónlógica con la dimensión o indicador que está midiendo. | 1. Totalmente en Desacuerdo (nocumple con el criterio) | El ítem no tiene relación lógica con la dimensión. |
| | 2. Desacuerdo(bajonivel de acuerdo) | El ítem tiene una relación tangencial /lejana con ladimensión. |
| | 3. Acuerdo (moderado nivel) | El ítem tiene una relación moderada con la dimensión que se está midiendo. |
| | 4. Totalmente de acuerdo (alto nivel) | El ítem se encuentra está relacionado con la dimensión que está midiendo. |
| **RELEVANCIA** El ítem es esencial o importante, es decir debe ser incluido. | 1. No cumple con el criterio | El ítem puede ser eliminado sin que se vea. |
| | 2. Bajo Nivel | El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste. |
| | 3. Moderado nivel | El ítem es relativamente importante. |
| | 4. Alto nivel | El ítem es muy relevante y debe ser incluido. |

*Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente.*

| | |
|---|---|
| CALIFICACIÓN | 1. No cumple con el criterio |
| | 2. Bajo Nivel |
| | 3. Moderado nivel |
| | 4. Alto nivel |

**Categorías del instrumento:**

- Primera categoría: Delitos informáticos
- Segunda categoría: Delitos contra el patrimonio
- Objetivos de las Categorías: Determinar el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, durante el periodo 2022.

| SUB CATE-GORÍAS | Ítem | Claridad | | | | Coherencia | | | | Relevancia | | | | Observa-ciones/ Recomen-daciones |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | |
| 1 | ¿Considera Ud. que, el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096 regula eficazmente el delito de fraude informático? SI - NO ¿Por qué? | | | | X | | | | X | | | X | | |
| 2 | ¿Considera Ud. que, en nuestro ordenamiento jurídico peruano se prevé mecanismos para poder detener, prevenir y sancionar los delitos informáticos contra el patrimonio? SI - NO ¿Por qué? | | | | X | | | | X | | | X | | |
| 3 | ¿Qué opinión le merece el aumento progresivo de las denuncias por la presunta comisión del delito de fraude informático, durante el periodo 2022? | | | | X | | | | X | | | X | | |
| 4 | ¿Considera Ud. que, los fiscales y funcionarios de las Fiscalías Corporativas Penales deben ser capacitados para abordar e investigar eficientemente los delitos informáticos contra el patrimonio? SI- NO ¿Por qué? | | | X | | | | X | | | | X | | |
| 5 | ¿Cuál cree Ud. que, es la principal razón por la cual se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet? | | | X | | | | | X | | | | X | |
| 6 | ¿Considera Ud. que, existen otras razones por las cuales se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet? | | | X | | | | X | | | | X | | |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | ¿Cuál considera Ud. que, sería el aporte de los miembros de la Unidad Fiscal especializada en Ciberdelincuencia del Ministerio Público en la persecución de los presuntos autores del ilícito penal de compras fraudulentas por internet? | | | | X | | | | X | | | | X | | |
| 8 | ¿Considera Ud. que, es necesaria la actuación de los agentes policiales de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) en las investigaciones aperturadas por la presunta comisión del delito de fraude en las operaciones o transferencias electrónicas? SI - NO ¿Por qué? | | | | X | | | | X | | | | X | | |
| 9 | ¿Considera Ud. que, las entidades financieras aplican eficientemente sus métodos de seguridad para proteger las cuentas de sus usuarios de fraudes realizados mediante operaciones y transferencias electrónicas? SI – NO ¿Por qué? | | | | X | | | X | | | | | X | | |
| 10 | ¿Qué deficiencias legislativas advierte Ud. en la tipificación del delito de fraude informático en la Ley de Delitos Informáticos – Ley N°30096? | | | X | | | | X | | | | X | | | |
| 11 | ¿Considera Ud. que, se debe modificar el artículo 8° de la Ley de Delitos Informáticos – Ley N°30096 que regula el delito de Fraude Informático en aras de una mejor aplicación? SI - NO ¿Por qué? | | | X | | | | X | | | | X | | | |
| 12 | Finalmente, ¿tiene Ud. alguna propuesta de solución o anotación que aportar con relación al delito de fraude informático? | | | X | | | | | X | | | X | | | |

Firma del
experto

**ANEXO 10 – MATRIZ EVALUACIÓN POR JUICIO DE EXPERTOS**

UNIVERSIDAD CÉSAR VALLEJO

**TÍTULO: TRATAMIENTO DE LOS CASOS DE DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO EN EL DISTRITO FISCAL DEL SANTA, 2022.**

**INSTRUCCIONES:**

Señor encuestado se le solicita que conteste el siguiente cuestionario en forma anónima y con honestidad para así desarrollar la investigación señalada, se agradece de antemano por su colaboración.

**CONDICIÓN:**

Juez ☐ Fiscal ☐ Abogado ☐

Agente policial de la DIVINDAT ☐

**PREGUNTAS:**

1. ¿Considera Ud. que, en el Perú se regula eficazmente el delito de fraude informático?

   SI ☐ NO ☐ NO PRECISA ☐

2. ¿Considera Ud. que, en nuestro ordenamiento jurídico peruano existen mecanismos para detener, prevenir y/o sancionar los delitos informáticos?

   SI ☐ NO ☐ NO PRECISA ☐

3. ¿Considera Ud. que, el aumento progresivo de denuncias por fraude informático se debe a la insuficiente regulación de este delito?

SI ☐ NO ☐ NO PRECISA ☐

4. ¿Estima Ud. que, los fiscales y funcionarios de las Fiscalías Corporativas Penales están capacitados para investigar eficientemente los delitos informáticos?

SI ☐ NO ☐ NO PRECISA ☐

5. ¿Considera Ud. que, el motivo principal de archivamiento a nivel preliminar de las investigaciones por compras fraudulentas por internet es la deficiente regulación del delito de fraude informático?

SI ☐ NO ☐ NO PRECISA ☐

6. ¿Considera Ud. que, existen otros motivos por los cuales se archiva a nivel preliminar las investigaciones por compras fraudulentas por internet?

SI ☐ NO ☐ NO PRECISA ☐

7. ¿Considera Ud. determinante la participación de la Unidad Especializada en ciberdelincuencia del Ministerio Publico para la eficaz persecución del ilícito penal de compras fraudulentas por internet?

SI ☐ NO ☐ NO PRECISA ☐

8. ¿Considera Ud. que, es necesaria la actuación de los agentes policiales de la DIVINDAT en las investigaciones por fraude mediante operaciones o transferencias electrónicas?

SI ☐ NO ☐ NO PRECISA ☐

9. ¿Considera Ud. que, las entidades financieras brindan seguridad jurídica a sus usuarios ante posibles fraudes informáticos?

SI ☐ NO ☐ NO PRECISA ☐

10. ¿Considera Ud. que, existen vacíos legales en el artículo 8° de la Ley de Delitos Informáticos - Ley N°30096?

SI ☐ NO ☐ NO PRECISA ☐

11. ¿Considera Ud. que, se debe modificar el artículo 8° de la Ley N°30096 referente al delito de fraude informático?

SI ☐ NO ☐ NO PRECISA ☐

# EVALUACIÓN POR JUICIO DE EXPERTOS

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento Cuestionario, a fin de conocer como se viene ejecutando el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022. La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente. Agradecemos su valiosa colaboración.

**1. Datos generales del juez:**

| | |
|---|---|
| **Nombre del juez:** | Maggye Gabriela López Agüero. |
| **Grado profesional:** | Maestría ( **X** ) Doctor ( ) |
| **Área de formación académica:** | Posgrado Universidad César Vallejo |
| **Áreas de experiencia profesional:** | Derecho Civil, Administrativo, Penal, Conciliación Extrajudicial. |
| **Institución donde labora:** | Gerente de Asesoría Jurídica de la Municipalidad Distrital de Jesús - Cajamarca. |
| **Tiempo de experiencia profesional en el área:** | 2 a 4 años ( ) Más de 5 años **( X** ) |
| **Experiencia en Investigación /Temática** (si corresponde) | Título de estudio realizado. |

**2. Propósito de la evaluación:**

Validar el contenido del instrumento cuestionario por juicio de expertos, conocedores del tema.

**3. Datos del instrumento**

Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022.

| | |
|---|---|
| Nombre de la Prueba: | Cuestionario para analizar el tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, durante el período 2022. |
| Autores: | De la Cruz Cherres, Wendy Aracely<br>Lulli Cáceres, Juan Antonio |
| Procedencia: | Chimbote. |
| Administración: | Abogados especialistas de manera presencial. |
| Tiempo de aplicación: | 10 a 30 minutos. |
| Ámbito de aplicación: | Especialistas conocedores del tema en el Distrito Fiscal del Santa. |
| Significación: | El instrumento da a conocer el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022; además, tiene enfoques conceptuales vinculados a las categorías de estudio, las cuales sustentan y enriquecen la temática a investigar. |

## 4. Soporte técnico

| Instrumento /Área | Subescalas (categorías) | Definición |
|---|---|---|
| **Delitos informáticos** | – Concepto | - Cometidos mediante el uso de las TIC con el fin de apropiarse de la información personal y financiera de cualquier persona natural o jurídica. |
| | – Ciberdelincuencia | - Convenio sobre la Ciberdelincuencia en Budapest |
| | – Ordenamiento Jurídico | - Ley N°30096 y su modificatoria Ley N°30171 |
| | – El bien jurídico penal | - Internet<br>- Funcionalidad informática |
| | - Órganos especializados | - Unidad Fiscal Especializada en Ciberdelincuencia<br>- División de Investigación de Delitos de Alta Tecnología (DIVINDAT) |
| **Delitos contra el patrimonio** | – Concepto | - Perpetrados con dolo mediante el uso de la fuerza o amenaza. |
| | – Base Legal | - Código Penal Peruano |

## 5. Presentación de instrucciones para el juez

A continuación, le presento el instrumento Cuestionario relacionado al Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022, elaborado por Wendy Aracely De La Cruz Cherres y Juan Antonio Lulli Cáceres en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

| Categoría | Calificación | Indicador |
|---|---|---|
| **CLARIDAD** El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas. | 1. No cumple con el criterio | El ítem no es claro. |
| | 2. Bajo Nivel | El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de éstas. |
| | 3. Moderado nivel | Se requiere una modificación muy específica de algunos de los términos del ítem. |
| | 4. Alto nivel | El ítem es claro, tiene semántica y sintaxis adecuada. |
| **COHERENCIA** El ítem tiene relaciónlógica con la dimensión o indicador que está midiendo. | 1. Totalmente en Desacuerdo (nocumple con el criterio) | El ítem no tiene relación lógica con la dimensión. |
| | 2. Desacuerdo(bajonivel de acuerdo) | El ítem tiene una relación tangencial /lejana con ladimensión. |
| | 3. Acuerdo (moderado nivel) | El ítem tiene una relación moderada con la dimensión que se está midiendo. |
| | 4. Totalmente de acuerdo (alto nivel) | El ítem se encuentra está relacionado con la dimensión que está midiendo. |
| **RELEVANCIA** El ítem es esencial o importante, es decir debe ser incluido. | 1. No cumple con el criterio | El ítem puede ser eliminado sin que se vea. |
| | 2. Bajo Nivel | El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste. |
| | 3. Moderado nivel | El ítem es relativamente importante. |
| | 4. Alto nivel | El ítem es muy relevante y debe ser incluido. |

*Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente.*

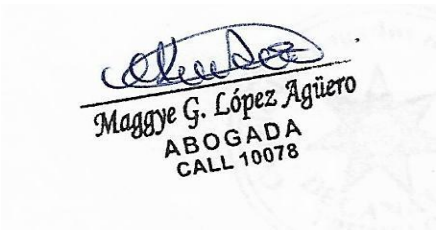
| | |
|---|---|
| CALIFICACIÓN | 1. No cumple con el criterio |
| | 2. Bajo Nivel |
| | 3. Moderado nivel |
| | 4. Alto nivel |

**Categorías del instrumento:**

- Primera categoría: Delitos informáticos
- Segunda categoría: Delitos contra el patrimonio
- Objetivos de las Categorías: Determinar el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, durante el periodo 2022.

| SUB CATE-GORÍAS | Ítem | Claridad | | | | Coherencia | | | | Relevancia | | | | Observa-ciones/ Recomen-daciones |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | |
| 1 | ¿Considera Ud. que, en el Perú se regula eficazmente el delito de fraude informático? | | | | X | | | | X | | | | X | |
| 2 | ¿Considera Ud. que, en nuestro ordenamiento jurídico peruano existen mecanismos para detener, prevenir y/o sancionar los delitos informáticos? | | | | X | | | | X | | | | X | |
| 3 | ¿Considera Ud. que el aumento progresivo de denuncias por fraude informático se debe a la insuficiente regulación de este delito? | | | | X | | | X | | | | X | | |
| 4 | ¿Estima Ud. que, los fiscales y funcionarios de las Fiscalías Corporativas Penales están capacitados para investigar eficientemente los delitos informáticos? | | | X | | | | X | | | | X | | |
| 5 | ¿Considera Ud. que, el motivo principal de archivamiento a nivel preliminar de las investigaciones por compras fraudulentas por internet es la deficiente regulación del delito de fraude informático? | | | X | | | | X | | | | X | | |
| 6 | ¿Considera Ud. que existen otros motivos por los cuales se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet? | | | | X | | | | X | | | | X | |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | ¿Considera Ud. determinante la participación de la Unidad Especializada en ciberdelincuencia del Ministerio Pública para la eficaz persecución del ilícito penal de compras fraudulentas por internet? | | | X | | | | | X | | | | X | | |
| 8 | ¿Considera Ud. que, es necesaria la actuación de los agentes policiales de la DIVINDAT en las investigaciones por fraude mediante operaciones o transferencias electrónicas? | | | X | | | | X | | | | | X | | |
| 9 | ¿Considera Ud. que, las entidades financieras brindan seguridad jurídica a sus usuarios ante posibles fraudes informáticos? | | | X | | | | | X | | | | X | | |
| 10 | ¿Considera Ud. que, existen vacíos legales en el artículo 8° de la Ley de Delitos Informáticos – Ley N°30096? | | | X | | | | | X | | | | X | | |
| 11 | ¿Considera Ud. que, se debe modificar el artículo 8° de la Ley N°30096 referente al delito de fraude informático? | | | X | | | | X | | | | X | | | |




Firma del
experto

# EVALUACIÓN POR JUICIO DE EXPERTOS

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento Cuestionario, a fin de conocer como se viene ejecutando el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022. La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente. Agradecemos su valiosa colaboración.

**1. Datos generales del juez:**

| | |
|---|---|
| **Nombre del juez:** | Melva Eudomilia Sánchez Medina. |
| **Grado profesional:** | Maestría ( X ) Doctor () |
| **Área de formación académica:** | Pregrado Universidad César Vallejo<br>Posgrado Universidad César Vallejo |
| **Áreas de experiencia profesional:** | Derecho Civil, Administrativo, Penal, Conciliación Extrajudicial. |
| **Institución donde labora:** | Universidad César Vallejo |
| **Tiempo de experiencia profesional en el área:** | 2 a 4 años ( ) Más de 5 años ( X ) |
| **Experiencia en Investigación /Temática** (si corresponde) | Título de estudio realizado. |

**2. Propósito de la evaluación:**

Validar el contenido del instrumento Cuestionario por juicio de expertos, conocedores del tema.

**3. Datos del instrumento**

Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022.

| | |
|---|---|
| Nombre de la Prueba: | Cuestionario para analizar el tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022. |
| Autores: | De la Cruz Cherres, Wendy Aracely<br>Lulli Cáceres, Juan Antonio |
| Procedencia: | Chimbote. |
| Administración: | Abogados especialistas de manera presencial. |
| Tiempo de aplicación: | 10 a 30 minutos. |
| Ámbito de aplicación: | Especialistas conocedores del tema en el Distrito Fiscal del Santa. |
| Significación: | El instrumento da a conocer el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022; además, tiene enfoques conceptuales vinculados a las categorías de estudio, lascuales sustentan y enriquecen la temática a investigar. |

## 4. Soporte técnico

| Instrumento /Área | Subescalas (categorías) | Definición |
|---|---|---|
| **Delitos informáticos** | – Concepto | - Cometidos mediante el uso de las TIC con el fin de apropiarse de la información personal y financiera de cualquier persona natural o jurídica. |
| | – Ciberdelincuencia | - Convenio sobre la Ciberdelincuencia en Budapest |
| | – Ordenamiento Jurídico | - Ley N°30096 y su modificatoria Ley N°30171 |
| | – El bien jurídico penal | - Internet<br>- Funcionalidad informática |
| | - Órganos especializados | - Unidad Fiscal Especializada en Ciberdelincuencia<br>- División de Investigación de Delitos de Alta Tecnología (DIVINDAT) |
| **Delitos contra el patrimonio** | – Concepto | - Perpetrados con dolo mediante el uso de la fuerza o amenaza. |
| | – Base Legal | - Código Penal Peruano |

## 5. Presentación de instrucciones para el juez

A continuación, le presento el instrumento Cuestionario relacionado al Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022, elaborado por Wendy Aracely De La Cruz Cherres y Juan Antonio Lulli Cáceres en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

| Categoría | Calificación | Indicador |
|---|---|---|
| **CLARIDAD** El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas. | 1. No cumple con el criterio | El ítem no es claro. |
| | 2. Bajo Nivel | El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de éstas. |
| | 3. Moderado nivel | Se requiere una modificación muy específica de algunos de los términos del ítem. |
| | 4. Alto nivel | El ítem es claro, tiene semántica y sintaxis adecuada. |
| **COHERENCIA** El ítem tiene relaciónlógica con la dimensión o indicador que está midiendo. | 1. Totalmente en Desacuerdo (nocumple con el criterio) | El ítem no tiene relación lógica con la dimensión. |
| | 2. Desacuerdo(bajonivel de acuerdo) | El ítem tiene una relación tangencial /lejana con ladimensión. |
| | 3. Acuerdo (moderado nivel) | El ítem tiene una relación moderada con la dimensión que se está midiendo. |
| | 4. Totalmente de acuerdo (alto nivel) | El ítem se encuentra está relacionado con la dimensión que está midiendo. |
| **RELEVANCIA** El ítem es esencial o importante, es decir debe ser incluido. | 1. No cumple con el criterio | El ítem puede ser eliminado sin que se vea. |
| | 2. Bajo Nivel | El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste. |
| | 3. Moderado nivel | El ítem es relativamente importante. |
| | 4. Alto nivel | El ítem es muy relevante y debe ser incluido. |

*Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente.*

| | |
|---|---|
| CALIFICACIÓN | 1. No cumple con el criterio |
| | 2. Bajo Nivel |
| | 3. Moderado nivel |
| | 4. Alto nivel |

**Categorías del instrumento:**

- Primera categoría: Delitos informáticos
- Segunda categoría: Delitos contra el patrimonio
- Objetivos de las Categorías: Determinar el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, durante el periodo 2022.

| SUB CATE-GORÍAS | Ítem | Claridad | | | | Coherencia | | | | Relevancia | | | | Observa-ciones/ Recomen-daciones |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | |
| 1 | ¿Considera Ud. que, en el Perú se regula eficazmente el delito de fraude informático? | | | | X | | | | X | | | | X | |
| 2 | ¿Considera Ud. que, en nuestro ordenamiento jurídico peruano existen mecanismos para detener, prevenir y/o sancionar los delitos informáticos? | | | X | | | | X | | | | X | | |
| 3 | ¿Considera Ud. que el aumento progresivo de denuncias por fraude informático se debe a la insuficiente regulación de este delito? | | | | X | | | X | | | | | X | |
| 4 | ¿Estima Ud. que, los fiscales y funcionarios de las Fiscalías Corporativas Penales están capacitados para investigar eficientemente los delitos informáticos? | | | | | X | | | X | | | X | | |
| 5 | ¿Considera Ud. que, el motivo principal de archivamiento a nivel preliminar de las investigaciones por compras fraudulentas por internet es la deficiente regulación del delito de fraude informático? | | | | X | | | | X | | | X | | |
| 6 | ¿Considera Ud. que existen otros motivos por los cuales se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet? | | | | | X | | | | | | | X | |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | ¿Considera Ud. determinante la participación de la Unidad Especializada en ciberdelincuencia del Ministerio Pública para la eficaz persecución del ilícito penal de compras fraudulentas por internet? | | | | X | | | | X | | | | X | | |
| 8 | ¿Considera Ud. que, es necesaria la actuación de los agentes policiales de la DIVINDAT en las investigaciones por fraude mediante operaciones o transferencias electrónicas? | | | | X | | | X | | | | | X | | |
| 9 | ¿Considera Ud. que, las entidades financieras brindan seguridad jurídica a sus usuarios ante posibles fraudes informáticos? | | | | X | | | X | | | | | X | | |
| 10 | ¿Considera Ud. que, existen vacíos legales en el artículo 8° de la Ley de Delitos Informáticos – Ley N°30096? | | | X | | | | X | | | | | X | | |
| 11 | ¿Considera Ud. que, se debe modificar el artículo 8° de la Ley N°30096 referente al delito de fraude informático? | | | | X | | | | X | | | X | | | |


Firma del
experto

# EVALUACIÓN POR JUICIO DE EXPERTOS

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento Cuestionario, a fin de conocer como se viene ejecutando el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022. La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente. Agradecemos su valiosa colaboración.

**1. Datos generales del juez:**

| | |
|---|---|
| **Nombre del juez:** | Gastón Jorge Quevedo Pereyra. |
| **Grado profesional:** | Maestría ( ) Doctor ( X ) |
| **Área de formación académica:** | Doctor en Derecho<br>Magister en Derecho Civil y Comercial. |
| **Áreas de experiencia profesional:** | Docente escuela de Postgrado Universidad Cesar Vallejo curso Metodología de la investigación. |
| **Institución donde labora:** | Universidad Cesar Vallejo entre otras universidades. |
| **Tiempo de experiencia profesional en el área:** | 2 a 4 años ( ) Más de 5 años ( X ) |
| **Experiencia en Investigación /Temática** (si corresponde) | Derecho Público y Derecho Económico |

**2. Propósito de la evaluación:**

Validar el contenido del instrumento cuestionario por juicio de expertos, conocedores del tema.

**3. Datos del instrumento**

Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022.

| | |
|---|---|
| Nombre de la Prueba: | Cuestionario para analizar el tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, durante el período 2022. |
| Autores: | De la Cruz Cherres, Wendy Aracely<br>Lulli Cáceres, Juan Antonio |
| Procedencia: | Chimbote. |
| Administración: | Abogados especialistas de manera presencial. |
| Tiempo de aplicación: | 10 a 30 minutos. |
| Ámbito de aplicación: | Especialistas conocedores del tema en el Distrito Fiscal del Santa. |
| Significación: | El instrumento da a conocer el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022; además, tiene enfoques conceptuales vinculados a las categorías de estudio, las cuales sustentan y enriquecen la temática a investigar. |

## 4. Soporte técnico

| Instrumento /Área | Subescalas (categorías) | Definición |
|---|---|---|
| **Delitos informáticos** | – Concepto | - Cometidos mediante el uso de las TIC con el fin de apropiarse de la información personal y financiera de cualquier persona natural o jurídica. |
| | – Ciberdelincuencia | - Convenio sobre la Ciberdelincuencia en Budapest |
| | – Ordenamiento Jurídico | - Ley N°30096 y su modificatoria Ley N°30171 |
| | – El bien jurídico penal | - Internet<br>- Funcionalidad informática |
| | - Órganos especializados | - Unidad Fiscal Especializada en Ciberdelincuencia<br>- División de Investigación de Delitos de Alta Tecnología (DIVINDAT) |
| **Delitos contra el patrimonio** | – Concepto | - Perpetrados con dolo mediante el uso de la fuerza o amenaza. |
| | – Base Legal | - Código Penal Peruano |

## 5. Presentación de instrucciones para el juez

A continuación, le presento el instrumento Cuestionario relacionado al Tratamiento de los casos de delitos informáticos contra el en el Distrito Fiscal del Santa, 2022, elaborado por Wendy Aracely De La Cruz Cherres y Juan Antonio Lulli Cáceres en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

| Categoría | Calificación | Indicador |
|---|---|---|
| **CLARIDAD** El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas. | 1. No cumple con el criterio | El ítem no es claro. |
| | 2. Bajo Nivel | El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de éstas. |
| | 3. Moderado nivel | Se requiere una modificación muy específica de algunos de los términos del ítem. |
| | 4. Alto nivel | El ítem es claro, tiene semántica y sintaxis adecuada. |
| **COHERENCIA** El ítem tiene relaciónlógica con la dimensión o indicador que está midiendo. | 1. Totalmente en Desacuerdo (nocumple con el criterio) | El ítem no tiene relación lógica con la dimensión. |
| | 2. Desacuerdo(bajonivel de acuerdo) | El ítem tiene una relación tangencial /lejana con ladimensión. |
| | 3. Acuerdo (moderado nivel) | El ítem tiene una relación moderada con la dimensión que se está midiendo. |
| | 4. Totalmente de acuerdo (alto nivel) | El ítem se encuentra está relacionado con la dimensión que está midiendo. |
| **RELEVANCIA** El ítem es esencial o importante, es decir debe ser incluido. | 1. No cumple con el criterio | El ítem puede ser eliminado sin que se vea. |
| | 2. Bajo Nivel | El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste. |
| | 3. Moderado nivel | El ítem es relativamente importante. |
| | 4. Alto nivel | El ítem es muy relevante y debe ser incluido. |

*Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente.*

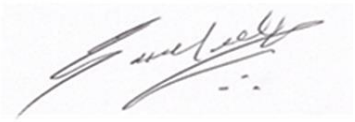
| | |
|---|---|
| CALIFICACIÓN | 1. No cumple con el criterio |
| | 2. Bajo Nivel |
| | 3. Moderado nivel |
| | 4. Alto nivel |

**Categorías del instrumento:**

- Primera categoría: Delitos informáticos
- Segunda categoría: Delitos contra el patrimonio
- Objetivos de las Categorías: Determinar el Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, durante el periodo 2022.

| SUB CATE-GORÍAS | Ítem | Claridad | | | | Coherencia | | | | Relevancia | | | | Observa-ciones/ Recomen-daciones |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | |
| 1 | ¿Considera Ud. que, en el Perú se regula eficazmente el delito de fraude informático? | | | X | | | | | X | | | X | | |
| 2 | ¿Considera Ud. que, en nuestro ordenamiento jurídico peruano existen mecanismos para detener, prevenir y/o sancionar los delitos informáticos? | | | | X | | | | X | | | | X | |
| 3 | ¿Considera Ud. que el aumento progresivo de denuncias por fraude informático se debe a la insuficiente regulación de este delito? | | | | X | | | | X | | | X | | |
| 4 | ¿Estima Ud. que, los fiscales y funcionarios de las Fiscalías Corporativas Penales están capacitados para investigar eficientemente los delitos informáticos? | | | X | | | | | X | | | | X | |
| 5 | ¿Considera Ud. que, el motivo principal de archivamiento a nivel preliminar de las investigaciones por compras fraudulentas por internet es la deficiente regulación del delito de fraude informático? | | | | X | | | | X | | | | X | |
| 6 | ¿Considera Ud. que existen otros motivos por los cuales se archivan a nivel preliminar las investigaciones por compras fraudulentas por internet? | | | | X | | | X | | | | X | | |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | ¿Considera Ud. determinante la participación de la Unidad Especializada en ciberdelincuencia del Ministerio Pública para la eficaz persecución del ilícito penal de compras fraudulentas por internet? | | | | X | | | | X | | | X | | | |
| 8 | ¿Considera Ud. que, es necesaria la actuación de los agentes policiales de la DIVINDAT en las investigaciones por fraude mediante operaciones o transferencias electrónicas? | | | | X | | | | X | | | | X | | |
| 9 | ¿Considera Ud. que, las entidades financieras brindan seguridad jurídica a sus usuarios ante posibles fraudes informáticos? | | | X | | | | | X | | | X | | | |
| 10 | ¿Considera Ud. que, existen vacíos legales en el artículo 8° de la Ley de Delitos Informáticos – Ley N°30096? | | | X | | | | X | | | | X | | | |
| 11 | ¿Considera Ud. que, se debe modificar el artículo 8° de la Ley N°30096 referente al delito de fraude informático? | | | | X | | | | X | | | | X | | |



Firma del
experto

## ANEXO 9 – PROYECTO DE PROYECTO DE LEY

**PROYECTO DE LEY N°00001/2023-CR PROYECTO DE LEY QUE MODIFICA EL Proyecto de Ley que modifica el Artículo 8 de la Ley N.º 30096 (Ley de Delitos Informáticos) e incorporar los Artículos A través de un Congresista, en uso de las atribuciones que le confiere el artículo 107° de la Constitución Política del Perú y conforme lo establecen los artículos 22, inc. c), 67, 74 y 75 del Reglamento del Congreso de la República, propone el siguiente proyecto de ley:**

**Proyecto de Ley N° 0001**

**Proyecto de Ley que** el Artículo 1 y el artículo 8 de la Ley N.º 30096 (Ley de Delitos Informáticos) y agregar los Artículos 1A y el 8A, 8B, 8C y 8D.

**Fórmula Legal**

**Artículo único**. **- Objeto de la presente ley**:

Ésta tiene por modificar el Artículo 1 y el artículo 8 de la Ley Nº 30096 (Ley de Delitos Informáticos) y agregar los Artículos 1A y el 8A, 8B, 8C y 8D, los cuales quedan redactados de la siguiente manera:

**Artículo 1.- Objeto de la Ley:**

La presente Ley tiene por objeto definir, prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

**Artículo 1A**: **Definiciones**:

Se incluye en la narrativa legal nuevas definiciones específicas de las conductas ejecutadas por los sujetos activos de este tipo de delitos informáticos, que serán sancionadas de acuerdo al bien jurídico tutelado que resulte o resulten afectados. Pudiendo ser conductas pluriofensivas.

a. **Clonación de tarjetas de crédito**: Consiste en obtener información del contenido de una tarjeta de crédito original y duplicarla en otra tarjeta portadora utilizando un equipo llamado "Skimmer"
b. **El Phishing**: Consiste en recolectar datos personales e información privilegiada con engaños a los propietarios de tal información por medios informáticos.
c. **Fraude en las operaciones y Transferencias electrónicas**: consiste en interceptar una transferencia luego de haber hackeado el acceso al correo electrónico de una persona para posteriormente apoderarse dicho dinero y así no llega a su destino original.
d. **"Compras fraudulentas por internet**" son las operaciones comerciales realizadas suplantando al usuario original, información obtenida a través del Phishing.
e. "**Homebanking**" consiste en la utilización indebida de páginas Url. falsas o simuladas del contratante original.
f. "**Vishing**" Consiste en la realización de llamadas de suma urgencia indicando la realización de compras falsas para luego solicitar información a modo de verificación de seguridad para poder proceder a bloquear la tarjeta afectada y así luego acceder a sus cuentas),
g. **"Sim Swapping"** consiste en la suplantación del chip del equipo del usuario legítimo, anulando dicho Sim Card para luego, activando el número en otro equipo, poder acceder así a la verificación en dos pasos consiguiendo de este modo acceso total a su información mientras el usuario se encuentra despojado de todo acceso a su línea móvil contratada.
h. **"E-skimming"** consiste en la adquisición de acceso a web auténticas para luego proceder a hackear dicho sistema y obtener el dinero de las operaciones que realizan los usuarios directamente a sus cuentas.

i. **“Ransomware”** consiste en un ciberataque que infecta un sistema y posteriormente bloquea acceso a la cierta información del usuario para luego enviar mensajes extorsivos exigiendo un monto de dinero para devolver la información a su propietario.
j. **“Smishing”**: consiste en la utilización de la mensajería de texto que trae programo el equipo móvil por defecto bombardeando masivamente y aleatoriamente a miles de usuarios con links fraudulentos que dan acceso a todo el teléfono a los autores.
k. **“Pharming”** se trata de colocar una URL similar al de la entidad financiera original utilizando un software malware el cual dirige o redirecciona a la víctima a una página web falsa creada con antelación por el ciberdelincuente.
l. **“Organización Criminal cibernética”** es la organización de dos o más personas destinada a cometer delitos informáticos.

**Artículo 8.- fraude informático**

El que deliberada e ilegítimamente procura para sí o para otro un beneficio ilícito en agravio de un tercero evadiendo los medios de seguridad de los sistemas informáticos públicos o privados a través de manipulación, sustitución, clonación o realización de algún tipo de interferencia o modificación destinado a obtener acceso no autorizado será reprimido con una pena privativa de libertad no menor de cinco ni mayor de ocho años y con sesenta a ciento veinte días-multa.

**Artículo 8A.- Compras fraudulentas por internet**

El que deliberada e ilegítimamente procura para sí o para otro un beneficio ilícito en agravio de un tercero evadiendo los medios de seguridad de los sistemas informáticos públicos o privados a través de manipulación, sustitución, clonación o realización de algún tipo de interferencia o modificación destinado realizar compras fraudulentas, con el uso de internet, en perjuicio ajeno será reprimido con una pena privativa de libertad no menor de cinco ni mayor de ocho años y con sesenta a ciento veinte días-multa.

**Artículo. – 8B.- fraude en las operaciones y transferencias electrónicas.**
El que deliberada e ilegítimamente procura para sí o para otro un beneficio ilícito en agravio de un tercero evadiendo los medios de seguridad de los sistemas informáticos públicos o privados a través de manipulación, sustitución, clonación o realización de algún tipo de interferencia o modificación destinado y así consiga realizar fraude en las operaciones y transferencias electrónicas, con el uso de internet, en perjuicio ajeno será reprimido con una pena privativa de libertad no menor de cinco ni mayor de ocho años y con sesenta a ciento veinte días-multa.

**Artículo. – 8C.- fraude informático en contra del Estado**
Los hechos tipificados en los Artículos 8A y 8B cuando se afecte el patrimonio del estado destinado a fines asistenciales o a programas de apoyo social serán sancionados con una pena privativa de libertad no menor de quince ni mayor de dieciocho años y con ciento cincuenta a doscientos cincuenta días-multa.

**Artículo. – 8D.- Fraude mediante Organización Criminal Cibernética.**
Los hechos tipificados en los Artículos 8A y 8B serán sancionados con una pena privativa de libertad no menor de quince ni mayor de dieciocho años y con ciento cincuenta a doscientos cincuenta días-multa cuando el agente haya obrado como parte de una organización criminal Cibernética.

Comuníquese al Señor Presidente de la República para su Promulgación.

para mi

Revista de Educación y Derecho
EDUCATION AND LAW REVIEW

UNIVERSITAT DE BARCELONA

Apreciado autor/a JUAN antonio LULLI CÁCERES,

Gracias por enviar el manuscrito "Tratamiento de los casos, delito Tratamiento de los casos de delitos informáticos contra el patrimonio en la Quinta Fiscalía Provincial Penal Corporativa del Santa, 2022 " a la Revista de Educación y Derecho. Con el sistema de gestión de publicaciones en línea que utilizamos podrá seguir el progreso y estado de su envío tras iniciar sesión con su cuenta personal en el sitio web de la revista:

URL del manuscrito: https://revistes.ub.edu/index.php/RED/authorDashboard/submission/43603
Nombre de usuario/a: jlullic

Si tiene alguna duda puede ponerse en contacto con nosotros. Gracias por elegir esta editorial para mostrar su trabajo.

Saludos cordiales,

Revista de Educación y Derecho

Síguenos en LinkedIn

Síguenos en Facebook

Síguenos en Twitter

---

Revista de Educación y Derecho
EDUCATION AND LAW REVIEW

UNIVERSITAT DE BARCELONA

Revista de Educación y Derecho (REYD)
http://revistes.ub.edu/index.php/RED