

UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
ESCUELA DE FORMACIÓN PROFESIONAL DE DERECHO



T E S I S

**Factores que determinan la no formalización de los delitos
informáticos en la tercera fiscalía provincial penal corporativa
de Carabayllo en el distrito fiscal de Lima Norte, 2022**

**Para optar el título profesional de:
Abogada**

Autor:

Bach. Karen Yaneth GUADALUPE ARIAS

Asesor:

Mg. Wilfredo Raúl TORRES ALFARO

Cerro de Pasco – Perú – 2025

UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
ESCUELA DE FORMACIÓN PROFESIONAL DE DERECHO



T E S I S

**Factores que determinan la no formalización de los delitos
informáticos en la tercera fiscalía provincial penal corporativa
de Carabaylo en el distrito fiscal de Lima Norte, 2022**

Sustentada y aprobada ante los miembros del jurado:

Dr. Miguel Ángel CCALLOHUANCA QUITO
PRESIDENTE

Dr. Oscar David PEREZ SAENZ
MIEMBRO

Mg. Nelson Wilder PALACIOS MATOS
MIEMBRO

La Unidad de Investigación de la Facultad de Derecho y Ciencias Políticas de la Universidad Nacional Daniel Alcides Carrión – UNDAC, ha realizado el análisis con el **SOFTWARE ANTIPLAGIO TURNITIN SIMILARITY**, que a continuación se detalla:

INFORME DE ORIGINALIDAD N° 008-2025

Presentado por:

Karen Yaneth GUADALUPE ARIAS

Escuela de Formación Profesional

DERECHO

Tipo de Trabajo:

TESIS

Título del Trabajo:

Factores que determinan la no Formalización de los Delitos Informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022.

Asesor:

Mg. Wilfredo Raúl TORRES ALFARO

Índice de Similitud: **22.00%**

Calificativo:

APROBADO

Se adjunta al presente el reporte de evaluación del software Antiplagio

Cerro de Pasco, 08 de enero de 2025.



Dr. Oscar David PEREZ SAENZ
DIRECTOR DE INVESTIGACION
SOFTWARE ANTIPLAGIO

DEDICATORIA

A mi abuela Nicolaza Callupe Cordova quien siempre me ha apoyado y desde el cielo cuida mis pasos. A mi madre Carmen Rosa Arias Callupe por ser el soporte a lo largo de esta formación profesional, por su amor incondicional y ser mi guía, la presente tesis es reflejo de su sacrificio y fortaleza. A mi hermano Ricardo Guadalupe Arias por ser mi mayor motivación, quien siempre ha cuidado de mí como un padre, quien con sus palabras siempre me ha brindado fuerzas para la culminación de la presente tesis.

AGRADECIMIENTO

Agradezco a Dios, quien guía mi camino y me ha da fortaleza en los momentos de aflicción y siempre guía mis pasos y cuida de mí.

Mi profundo agradecimiento a mi abuela Nicolaza Callupe Cordova, que desde el cielo sonrío por cada uno de mis logros, a mi madre Carmen Rosa Arias Callupe por cada sacrificio que ha realizado a fin de poder culminar mis estudios universitarios y a mi hermano Ricardo Guadalupe Arias, quien siempre me ha motivado.

Finalmente, quiero expresar mis más sinceros agradecimientos a mis docentes de la Facultad de Derecho y Ciencias Políticas de mi alma mater, por cada una de sus enseñanzas y haber forjado mi formación universitaria con cada una de sus enseñanzas en las aulas universitarias de donde me llevo los más gratos recuerdos y todos los conocimientos adquiridos.

RESUMEN

La investigación aborda el incremento y el impacto de los delitos informáticos en Lima, focalizándose en la Tercera fiscalía provincial Penal Corporativa de Carabayllo durante el 2022. El objetivo general es identificar los factores que influyen en la no formalización de los delitos informáticos en dicha Fiscalía, mientras que los objetivos específicos se enfocan en analizar cómo la carencia de pruebas y elementos de convicción afectan este proceso.

Se utilizará un método analítico y crítico, un diseño no experimental-descriptivo y análisis documental. La población de estudio son todas las carpetas fiscales vistas en la Tercera fiscalía provincial Penal Corporativa de Carabayllo, seleccionándose una muestra de 8 carpetas para el análisis. Para lo cual se utilizará como técnica de análisis una matriz de análisis documental para recopilar información relevante.

Conclusión: La investigación revela que la falta de medios probatorios sólidos es un factor primordial que influye en la no formalización de los delitos informáticos en esta Fiscalía. La complejidad inherente a la recolección de pruebas digitales y la ausencia de evidencia contundente pueden obstaculizar la continuación de los procesos penales.

Palabras Clave: Delitos informáticos, formalización, pruebas, convicción, procesos judiciales.

ABSTRACT

The investigation addresses the increase and impact of computer crimes in Lima, focusing on the Third Provincial Corporate Criminal Prosecutor's Office of Carabayllo during 2022. The general objective is to identify the factors that influence the non-formalization of computer crimes in said Prosecutor's Office, while the specific objectives focus on analyzing how the lack of evidence and elements of conviction affect this process.

An analytical and critical method, a non-experimental-descriptive design and documentary analysis will be used. The study population is all the tax folders seen in the Third Provincial Criminal Corporate Prosecutor's Office of Carabayllo, selecting a sample of 8 folders for the analysis. For which a documentary analysis matrix will be used as an analysis technique to collect relevant information.

Conclusion: The investigation reveals that the lack of solid evidence is a primary factor that influences the non-formalization of computer crimes in this Prosecutor's Office. The complexity inherent in the collection of digital evidence and the absence of compelling evidence can hinder the continuation of criminal proceedings.

Keywords: Cybercrimes, formalization, evidence, conviction, judicial processes.

INTRODUCCIÓN

En la actualidad, el avance tecnológico ha traído consigo beneficios significativos, pero también ha dado lugar a una nueva era de crimen: los delitos informáticos. Estos actos delictivos, perpetrados mediante el uso de la tecnología, han generado un impacto global, alterando la seguridad y la confianza en la esfera digital. En esta investigación, nos sumergimos en el contexto de Lima, específicamente en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo durante el año 2022, para examinar detenidamente la evolución y el alcance de los delitos informáticos en esta región.

La proliferación de incidentes a nivel internacional y nacional subraya la urgente necesidad de comprender los aspectos que rodean estos crímenes. Desde los inicios en los años 90, cuando delincuentes lograron acceder a sistemas financieros en Francia, hasta las estadísticas actuales que sitúan a México como uno de los países más afectados por la ciberdelincuencia en América Latina, evidencian un patrón preocupante. En este contexto, el Ministerio de Justicia y Derechos Humanos ha reportado un aumento exponencial de denuncias por delitos informáticos en el periodo 2018-2021, especialmente en Lima.

Esta investigación se enmarca en el ámbito del Derecho Penal y Procesal Penal, centrándose en un aspecto fundamental: ¿qué factores determinan la falta de formalización de los delitos informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo? Para abordar esta interrogante, se exploran problemas específicos como la carencia de pruebas y la insuficiencia de elementos de convicción, elementos cruciales en el proceso de formalización de casos. El objetivo general radica en identificar estos factores influyentes, mientras que los objetivos específicos se orientan a comprender cómo la falta de pruebas y elementos de convicción afectan este proceso.

Para alcanzar estos objetivos, se empleará una metodología que combine métodos analíticos y críticos, junto con un diseño no experimental-descriptivo. Se

analizarán minuciosamente las carpetas fiscales vistas en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo durante el 2022, seleccionando una muestra representativa para un análisis exhaustivo. La utilización de una matriz de análisis documental permitirá recopilar y analizar información pertinente para este estudio.

En última instancia, esta investigación pretende arrojar luz sobre los desafíos inherentes a la formalización de los delitos informáticos en una jurisdicción específica, enfatizando la necesidad de comprender y abordar las complejidades que rodean estos crímenes en la era digital.

ÍNDICE

DEDICATORIA	
AGRADECIMIENTO	
RESUMEN	
ABSTRACT	
INTRODUCCIÓN	
ÍNDICE	

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del problema	1
1.2. Delimitación de la investigación	2
1.3. Formulación del problema.....	3
1.3.1. Problema general	3
1.3.2. Problemas específicos	3
1.4. Formulación de objetivos	3
1.4.1. Objetivo general	3
1.4.2. Objetivos específicos.....	3
1.5. Justificación de la investigación	4
1.6. Limitaciones de la investigación.....	4

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes de estudio	5
2.2. Bases teóricas – científicas.....	7
2.3. Definición de términos conceptuales.....	24
2.4. Enfoque filosófico – epistémico.....	26

CAPÍTULO III

METODOLOGÍA Y TÉCNICAS DE INVESTIGACIÓN

3.1. Tipo de investigación	27
3.2. Nivel de investigación.....	27
3.3. Característica de la investigación	27

3.4. Método de investigación	28
3.5. Diseño de investigación	28
3.6. Procedimiento del muestreo	28
3.7. Técnicas e instrumentos de recolección de datos	29
3.8. Técnicas de procesamiento y análisis de datos	29
3.9. Orientación ética.....	29

CAPÍTULO IV

PRESENTACION DE RESULTADOS

4.1. Presentación, análisis e interpretación de resultados.....	30
4.2. Discusión de resultados.....	47

CONCLUSIONES

RECOMENDACIONES

REFERENCIAS BIBLIOGRÁFICAS

ANEXOS

INDICE DE TABLAS

Tabla 1	Técnicas e instrumentos de recolección de datos.	29
Tabla 2	Caso Fajardo - Vergara	30
Tabla 3	Caso Díaz - Fernandez	33
Tabla 4	Caso L.Q.R.R. (1).....	35
Tabla 5	Caso L.Q.R.R. (2).....	37
Tabla 6	Caso L.Q.R.R. (3).....	39
Tabla 7	Caso: VARGAS.....	41
Tabla 8	Caso: L.Q.R.R. (4).....	44
Tabla 9	Caso: ALVARADO - DIOSES	46

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del problema

Como sociedad somos conscientes del crecimiento tecnológico que se ha venido dando con el pasar de los años, lo que de muchas formas ha sido beneficioso para todos, el poder comunicarnos, el acceso a todo tipo de información al alcance de un click nos ha hecho de alguna manera la vida más fácil. Sin embargo, lastimosamente hay un lado negativo que gente inescrupulosa y con malicia ha logrado descifrar, ocasionando pérdidas no solo monetarias sino de información importante para muchos, el aprovechamiento malicioso de este grupo determinado de sujetos a quienes se les conoce como cyber delincuentes o delincuentes informáticos ha hecho que muchas personas se vean afectadas de distintas formas.

En el ámbito internacional, este tipo de delitos no son algo nuevo ya que en los 90's en Francia dos ladrones se habrían infiltrado en el sistema de telégrafos con el propósito de mediante un hackeo logaran tener acceso a los mercados financieros del país y robar los datos que en este se encontrarán. Así mismo, según los datos de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) a nivel de América Latina México encabeza la lista de países donde hay mayor incidencia de casos

de ciberdelincuencia, esto con una cifra de 463 casos de fraude cibernético en operaciones por comercio electrónico y banca móvil en cada hora (Universidad Internacional de la Rioja, 2023).

En el ámbito nacional, el Ministerio de Justicia y Derechos Humanos (MINJUSDH), a través de la presentación del documento “Ciberdelincuencia: Reporte de información estadística y recomendaciones para la prevención”, destacó el incremento de los casos entre los periodos del 2018 al 2021, donde se indica que de un total de 2,927 denuncias presentadas en el 2018 se incrementó a 14,671 en el año 2021 (MINJUSDH, 2021).

En el ámbito local, en el año 2019 hubo un incremento del 144% respecto de las cifras del año 2018, en el 2020 se vio un aumento de 25% respecto al año anterior; posteriormente en el 2021 creció un 65%. Destacando de dichas cifras que Lima es el departamento donde se registraron una cantidad mayor de denuncias por ciberdelitos en el país entre los años 2018 al 2021(MINJUSDH, 2021).

1.2. Delimitación de la investigación

Delimitación Espacial: El presente estudio ha considerado como espacio geográficamente delimitado la ciudad de Lima, en específico el Distrito Fiscal de Lima Norte, 2022.

Delimitación Temporal: Para la delimitación temporal en el presente estudio se ha considerado el año 2022.

Delimitación Académica: Respecto a la delimitación académica el presente estudio estuvo relacionado con el Derecho Penal y Derecho Procesal Penal.

1.3. Formulación del problema

1.3.1. Problema general

¿Cuáles son aquellos factores que determinarán la no formalización de los delitos informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022?

1.3.2. Problemas específicos

PE₁: ¿De qué manera la falta de presupuestos materiales determinará la no formalización de los procesos de delitos informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022?

PE₂: ¿En qué nivel la insuficiencia de elementos de convicción afecta en la formalización de los procesos de delitos informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022?

1.4. Formulación de objetivos

1.4.1. Objetivo general

Determinar qué factores son los que intervienen en la no formalización de los delitos informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022.

1.4.2. Objetivos específicos

OE₁: Analizar de qué manera la falta de presupuestos materiales determinarán la no formalización de los procesos de delitos informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022.

OE₂: Determinar el nivel en el que la insuficiencia de elementos de convicción afecta en la formalización de los procesos de delitos informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022.

1.5. Justificación de la investigación

La presente investigación es fundamental en el sentido de que, es importante poder conocer cuáles son las consideraciones que el Fiscal como representante del Ministerio Público toma en cuenta para decidir si formaliza o no la investigación respecto a los delitos informáticos.

Es necesario recalcar también que el tema planteado para este estudio resulta ser un tema que en la actualidad recién ha estado siendo considerado desde hace unos años como un problema relevante, por lo que doctrinal y jurisprudencialmente se analizó de forma minuciosa para no alterar la información a recopilarse.

Así mismo, este estudio resulta de mucha importancia para la comunidad jurídica; esto debido a que se realizó con la finalidad de poder servir de ayuda a abogados, operadores de justicia y a futuros estudios.

1.6. Limitaciones de la investigación

Respecto a los recursos materiales solo se tuvo como limitación que a nivel internacional no se pudo hallar tesis que contengan ambas variables planteadas en el presente estudio. Por otro lado, no se tuvieron más limitaciones ya que se cuenta con los recursos económicos, información académica relevante y tiempo suficiente para poder llevar a cabo la presente.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes de estudio

Rivera (2021). En su tesis titulada “Prevenir los delitos informáticos en el Sistema Financiero Ecuatoriano del 2020 al 2022”. Ecuador.

Se concluyó que, el principal problema es la falta de estrategias de prevención de los delitos informáticos, además de que, debido a la ignorancia por parte de los usuarios del sistema financiero sobre el peligro real que representa este ilícito. Así mismo, la falta de capacitación al personal policial y a los Fiscales que forman parte de la investigación para evitar así que no se altere los indicios probatorios que posteriormente servirán como herramientas necesarias para que el juez pueda administrar justicia como se debe y la sanción correspondiente.

Cabrera (2020). En su tesis titulada “Fundamentos jurídicos considerados por los fiscales penales del cercado de Cajamarca para archivar las investigaciones de delitos informáticos durante el periodo 2010-2018”.

Tuvo como objetivo identificar los fundamentos jurídicos considerados por los fiscales penales del cercado de Cajamarca para archivar las investigaciones de delitos informáticos. Para ello se empleó una metodología de tipo básico, con un enfoque cualitativo, de diseño no experimental transversal,

explicativo. Así mismo, su población estuvo conformada por 23 carpetas fiscales de las cuales se consideró para la muestra 10 de las mismas que se encuentran archivadas. La recopilación de información se hizo mediante el fichaje y la guía de análisis documental. Finalmente concluyendo que, del análisis de las disposiciones de investigaciones de delitos informáticos se obtuvo como resultado que los fundamentos jurídicos considerados por los fiscales para archivar tales investigaciones, son: la falta de individualización del sujeto; acción atípica, no es justiciable penalmente y adicionalmente delito de acción penal privada.

Ramos (2020). En su tesis titulada como “Factores procesales en el archivamiento de los delitos informáticos, vistos en la primera y segunda fiscalía provincial penal corporativa de Leoncio Prado, 2017 – 2018”.

Tuvo como objetivo principal demostrar los factores procesales que contribuyen en el archivamiento de los delitos informáticos en la Primera y Segunda Fiscalía Provincial Penal Corporativa de Leoncio Prado, 2017-2018. La metodología empleada fue de tipo aplicada, con un enfoque cuantitativo de nivel descriptivo – explicativo, de diseño correlacional. Para lo cual se trabajó con una población total de 9 carpetas fiscales y 10 encuestas aplicadas a los Fiscales Provinciales y Adjuntos de la primera y segunda Fiscalía Provincial Penal Corporativa de Leoncio Prado, de las cuales 6 carpetas y 10 encuestas fueron consideradas para formar parte de la muestra; mediante la aplicación de la ficha de registro de datos y el cuestionario personal se recopilaron los datos necesarios para el estudio. Concluyendo que, del cuadro N° 01 se han llegado a registrar 6 casos con disposición de archivo estos por factores que van desde problemas de tipificación, falta de peritos informáticos, insuficientes medios probatorios, falta de identificación de los presuntos autores y por lo que la tecnología no está al alcance de los operadores jurídicos; así mismo, del cuadro

N° 06 se advierte que el 90% (9) Fiscales Provinciales y Adjuntos consideran que, la falta de peritajes para la obtención de evidencia digital, la fragilidad de la prueba informática, falta de informática forense, carencia de fiscales especialistas en delitos informáticos si son los factores procesales que influyen en el archivamiento de los delitos informáticos.

Martínez (2023). En su tesis que lleva como título “Los delitos informáticos y su ineficacia en la aplicación de sanciones como consecuencia de sus vacíos jurídicos Huancayo, 2022”.

Tuvo como objetivo determinar de qué manera los delitos informáticos resultan ineficaces en la aplicación de sanciones como consecuencia de los vacíos jurídicos. Teniendo además como estructura metodológica el tipo básico, con un enfoque cuantitativo, de diseño no experimental correlacional. Su muestra estuvo conformada por 81 profesionales de los cuales el 47% son mujeres y el 53% de varones, el 25% trabaja en el Poder judicial, el 21% en el ministerio público, el 28% abogados colegiados y el 21% personal de la DIVINCRI PNP. Concluyendo que, teniendo de resultado que del coeficiente de correlación de Pearson en la hipótesis general en correlación fuerte en un 0.62, con respecto a la hipótesis específica sobre la ciberdelincuencia y la Ley N° 30096 su correlación es del 0.446 que su correlación moderada, por ultimo de hipótesis específica 2 su coeficiente correlación es de es del 0.426 entre el proceso judicial y la administración de justicia se evidencia que sí existe una relación significativa entre los delitos informáticos y la ineficacia de la aplicación de sanciones debido a los vacíos jurídicos, $p(0.00 < 0.05)$.

2.2. Bases teóricas – científicas

2.2.1. Delitos Informáticos

Para Acosta et al. (2020), los delitos informáticos; son actos ilegales realizados mediante el abuso de la tecnología, violación de la seguridad de la información de terceros, daño o extracción de cualquier dato almacenado en el

servidor o dispositivo; donde una persona tiene diferentes tipos de información es decir personal, financiera, empresarial entre otros que son de importancia para cada individuo, donde estas informaciones en muchas ocasiones son vulneradas por los delincuentes que se dedican al robo informático, lo cual esto lo realizan con la finalidad de sacar beneficios propios donde una vez obtenida la información de la persona esto lo extorcionan a través de chantajes, amenazas entre otros sucesos que se dan.

Por otra parte Loredó y Ramírez, (2013), menciona que el “Delito informático es el uso de cualquier sistema informático como medio o fin de un delito”, es así que las personas que se dedican a realizar estos tipos de actos delictivos, usan diferentes medios en poder acceder a la información personal, donde con las informaciones obtenidas realizan actos en poder realizar extorsiones a las personas.

El fenómeno informático es un hecho innegable, y aparentemente irreversible, que los ordenadores se han instalado entre nosotros. El principal problema es encontrar fórmulas de control efectivo en la relación donde la ley debe jugar un papel importante, con el papel de regular las relaciones sociales y el mecanismo de mantenimiento del orden público (Bramont-Arias, 1997).

Leyva (2021), considera que el paradigma clásico del poder a través del dominio de la información, ha tomado una nueva perspectiva, y es que el paradigma actual se torna en el dominio de la información tal, como lo hemos podido percibir en distintos casos de connotación internacional, ahí tenemos el caso de los WikiLeaks por ejemplo, constituyéndose al día de hoy en el arma que arroja de poder a diversos países y personas que han logrado alcanzar significativos avances en el campo tecnológico de las aplicaciones como el caso del Mark Zuckerberg que al día de hoy es dueño de las redes sociales más importantes del mundo como WhatsApp, Facebook e Instagram, lo que le brinda

un amplio margen de poder en las comunicaciones y la información que al día de hoy se difunde en gran porcentaje por las redes sociales mencionada.

Otros autores, consideran que el concepto de delito informático aún no ha encontrado consenso en la doctrina, y también lo denominan computer crime o computerkriminalität, ello en razón que la delincuencia informática comprende una serie de comportamientos que es difícil reducir o agrupar en una sola definición. De manera general, *“se puede definir el delito informático como aquél en el que para su comisión se emplea un sistema automático de procesamiento de datos o de transmisión de datos”* (Bramont-Arias 1997, p. 27).

Sujeto Activo en el Delito Informático

Peña Cabrera (2011), destaca que el sujeto activo es entendido como aquella persona que cuente con conocimientos mínimos acerca de la informática para efectivizar conductas prohibitivas. Resulta admisible apreciar una autoría mediata, cuando el hombre de atrás se aprovecha de la buena fe del hombre de adelante, del instrumento quien, sin dolo, desconociendo la naturaleza de los actos que está cometiendo, ingresa de forma indebida a una red o base de datos.

Cabe recalcar que no se puede considerar como sujeto activo a personas jurídicas solo naturales; pero que, sin embargo, si está implicado una persona jurídica esta puede ser pasible de consecuencias accesorias descritas en el Código Penal en el artículo 105°.

Sujeto Pasivo en el Delito Informático

Leyva (2021), considera que diversos autores consideran a la víctima como aquel o aquella persona afectada por el comportamiento del autor del delito. “Para la victimología, la víctima es el ser humano que padece daño en los bienes jurídicamente protegidos por la normativa penal: vida, salud, propiedad, honor, honestidad, etc.

Por otro lado, Leyva citando García, considera que hay duplicidad de víctimas y delinciente, puesto que existe una interacción entre ambos, asimismo la persona natural que experimenta subjetivamente con malestar o dolor una lesión objetiva de bienes jurídicos. Pero es una acepción restrictiva que dejaría fuera de toda consideración victimológica una rica y grave gama de comportamientos criminales dirigidos contra personas jurídicas o intereses supraindividuales. Una vez superado, además, el microscópico ámbito de la pareja criminal y los prejuicios psicologistas de los primeros estudios victimológicos, evidenció su insuficiencia, su estrechez. Pero si la víctima no ha tomado las precauciones del caso puede decaer el hecho en autorresponsabilidad y es atípico dicha conducta fraudulenta, sin embargo, las empresas, con el desarrollo continuo de la sociedad en una economía de mercado, siempre tienden a que su oferta llegue al público; el instrumento para conseguir esto son las computadoras, las cuales facilitan y aceleran este proceso. Es por esto que las víctimas más frecuentes de los delitos informáticos son personas jurídicas, con un cierto potencial económico. Esta característica corresponde con las notas propias de la delincuencia de cuello blanco o socioeconómico donde también se cuadra la delincuencia informática.

Bien jurídico protegido

Villavicencio (2014), considera que el bien jurídico protegido en los delitos informáticos se concibe en los planos de manera conjunta y concatenada; en el primero se encuentra la información de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo plano, los demás bienes afectados a través de este tipo de delitos como son la indemnidad sexual, intimidad, etcétera (pp. 288-289).

En este tipo de delitos no se puede establecer a la información como el único bien jurídico afectado, por ser el principal y el más importante; sino a un

conjunto de bienes que son afectados, debido a la característica de la conducta típica en esta modalidad delictiva que colisiona con diversos intereses colectivos. Es decir, se considera a este delito como un delito un delito pluriofensivo, sin perjuicio de que uno de tales bienes este independientemente tutelado por otro tipo penal. En efecto, los bienes jurídicos afectados son diversos por ser un delito de tipo pluriofensivo, lo que significa tener cuidado en la descripción de cada conducta ilícita señala en la normativa pertinente.

Entre las formas más comunes que utilizan los delincuentes cibernéticos son:

- **Phishing:** se hace por medio de mensajes fraudulentos para atraer a las víctimas hacia sitios web falsos, de modo que introduzcan en ellos información personal como contraseñas y datos bancarios.
- **Vishing:** el término deriva de "voice" y "phishing" y se refiere al tipo de ciberdelito que combina una llamada telefónica fraudulenta con información previamente obtenida desde internet. Generalmente, se usa después de haber realizado phishing con la intención de que la víctima brinde su token digital o clave SMS para que el ciberdelincuente haga una transacción financiera.
- **Smishing:** se da por mensajes de texto o de WhatsApp. Aquí la víctima recibe un mensaje, donde el ciberdelincuente se hace pasar por el banco y alerta sobre una supuesta compra sospechosa con su tarjeta de crédito. Luego, le alienta a cancelar dicha compra llamando a un número de banca telefónica falso, en el cual le pedirán sus datos confidenciales.
- **Carding:** es una forma de estafa que tiene como objetivo conseguir los datos de la tarjeta de crédito de la víctima para que los ciberdelincuentes hagan compras online con la misma.

- **Pharming:** utiliza malware o software malicioso para redirigir a los usuarios desprevenidos hacia versiones falsificadas de sitios web, con el fin de que introduzcan sus datos personales.
- **Keylogging:** este tipo de spyware o software malicioso oculto se introduce en el ordenador o smartphone de la víctima para registrar en secreto todo lo que escribe y así obtener información de sus cuentas y otros datos personales.
- **Sniffing:** sucede cuando la víctima se conecta a una red Wi-Fi pública no protegida y no cifrada. Bajo esta modalidad, los hackers pueden robar los datos rastreando su tráfico de internet con herramientas especiales.

Los Robos Cibernéticos

Es el conjunto de acciones empleadas por un grupo determinado de sujetos al momento de delinquir, engañar y obtener datos y/o información confidencial, como el acceso a cuentas bancarias por la banca móvil y otros medios en línea.

Ley N.º 30096

La presente Ley tiene por objeto 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 5. Propositiones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.

El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de cuatro ni

mayor de ocho años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal.

Tipos de Delitos Informáticos

Para abordar los tipos de delitos informáticos, se ha considerado oportuno tener en consideración aquellos reconocidos por la Organización de Naciones Unidas y aquellos contemplados en el Convenio de Ciberdelincuencia de Budapest:

a. Organización de Naciones Unidas - ONU

- Falsificaciones informáticas.
- Daño o modificaciones de programas o datos computarizados.
- Acceso no autorizado a servicios y sistemas informáticos.

b. Convenio de Ciberdelincuencia o Convenio de Budapest

Título I: Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Artículo 2 Acceso ilícito
- Artículo 3 Interceptación ilícita
- Artículo 4 Ataque a la integridad de datos
- Artículo 5 Ataques a la integridad del sistema
- Artículo 6 Abuso de los dispositivos

Título II: Delitos informáticos

- Artículo 7 Falsificación informática
- Artículo 8 Fraude Informático

Título III: Delitos relacionados con el contenido

- Artículo 9 Delitos relacionados con la pornografía infantil

Título IV: Delitos relacionados con infracción de la propiedad intelectual y de los derechos afines

- Artículo 10 Delitos relacionados con infracciones de la propiedad intelectual y de derechos afines.

Precisada la clasificación de delitos reconocidos por la ONU y aquellos contemplados en el Convenio de Ciberdelincuencia, nos corresponde referirnos a los mismos -delitos informáticos-, por ser materia de análisis de la presente investigación.

Tipos de delitos informáticos según la ONU

- Fraude cometido mediante manipulación de computadoras
- Falsificaciones informáticas
- Daño o modificaciones de programas o datos computarizados
- Acceso no autorizado a servicios y sistemas informáticos

Tipos de delitos informáticos según el Convenio de Budapest (Título 2 Delitos informáticos).

- Artículo 7 Falsificación informática
- Artículo 8 Fraude Informático

Regulación del Convenio de Budapest

Los temas que forman parte del Convenio son: Los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (Capítulo II). El Artículo 2, se refiere al acceso ilícito; el Artículo 3, se refiere a la Interceptación ilícita; el Artículo 4, referido al ataque a la integridad de datos; en el Artículo 5, se prevé los ataques a la integridad del sistema; el Artículo 6, está referido al Abuso de los dispositivos

También, se precisan los Delitos informáticos, en el artículo 7 la Falsificación informática, y en el artículo 8 el Fraude Informático. Por su parte, el Título 3 contempla los delitos relacionados con el contenido, entre los que se encuentran los delitos relacionados a pornografía infantil (Artículo 9); los delitos relacionados con infracciones de la propiedad intelectual y de los derechos

afines (Artículo 10); En el artículo 11 se prevé la tentativa y la complicidad, en el artículo 12 la responsabilidad de las personas jurídicas.

En los artículos 16 y 17 se prevé la conservación rápida de los datos informáticos almacenados por las autoridades competentes de cada Estado; los artículos 19 y 20 se refieren al registro y confiscación de datos informáticos almacenado y a la obtención en tiempo real de datos relativos al tráfico, respectivamente.

En el Capítulo III pudimos encontrar los principios en general relativos a la cooperación universal en el artículo 23; la extradición en el artículo 24; principios relativos a la ayuda recíproca en el artículo 25; en el artículo 27 se prevé lo relativo al método frente a demandas de ayuda recíproca en ausencia de consenso universal aplicable; en el artículo 35 se hace mención a la Red 24/7 con el objeto de: “(...), asegurar una ayuda instantánea para indagaciones que se relacionan con delitos vinculados a sistemas y datos informáticos, (...)”. Al 58 final, en el artículo 39 se hace mención a los efectos del pacto, como: Si 2 o más piezas han celebrado ya un convenio o tratado relativo a las preguntas contempladas en el presente acuerdo, o si lo realizan el en futuro, lo harán en consecuencia no sea incompatible con las metas e inicios del convenio. Nada de lo dispuesto en el Convenio afectará a otros derechos, restricciones, obligaciones y responsabilidades de cada parte.

Influencia del Convenio de Budapest en Perú

Huamán (2020), destaca en tanto que el Convenio de Budapest sobre la ciberdelincuencia trae consigo destacados beneficios para los demás Estados que ratificaron en acuerdo con dicho convenio. En ese aspecto podemos ver que los beneficios son específicos conforme a lo siguiente:

- El ejercicio de la política penal común de acuerdo a la creación de normas concretas que regulen actos de ciberdelincuencia o fraudulentos.

- En dicho Convenio se ha establecido herramientas con el fin de que los Estados parte tomen en cuenta para que estos sean utilizados en la prevención de dicho ilícito.
- Es necesaria la instauración de cooperación penal mediante organismos internos que prevengan, averigüen y sancionen los Estados parte para que se sancione todo hecho estipulado en el capítulo II de dicho Acuerdo.

Podemos ver que el Perú podrá gozar de dichos beneficios dispuestos en el acuerdo Budapest, siendo fundamental dicho desarrollo para cumplir con los fines preventivos que otras naciones ya han tomado en práctica, sin embargo, ante la regulación interna de dicho pacto internacional cabría la posibilidad de existir un choque o un desacuerdo entre ambas normativas o habrá una mejora extensiva en cuanto a delitos informáticos suscitados en el Perú.

De acuerdo a ello, Huamán (2020), tiene como objetivo identificar las metas que fueron instauradas en el acuerdo de Budapest; siendo la primera de ellas instaurar una política penal de aplicación común para que todas las sociedades puedan prevenir o defenderse de ataques cibernéticos; seguidamente identifica que el acuerdo de Budapest propone instaurar leyes específicas para la lucha contra la criminalidad informática, y por último identifica dicho autor la elaboración de medios de cooperación internacional ante la delincuencia cibernética.

En todos los casos en que se han desarrollado propuestas de responsabilidad penal en el Convenio de Budapest, las disposiciones han sido creadas o modificadas en el territorio con los mismos objetivos. En general, las normas peruanas tienen una redacción similar, incluyendo puntos claves como la necesidad de cometer el delito "intencional e ilícitamente" e incluso utilizan los mismos verbos controladores (infringir, fabricar, divulgar, alterar, suprimir, etc.). De hecho, lo que se ha observado es sólo una extensión de la terminología, ya

que algunos delitos van acompañados de actividades más allá de las recomendadas por la Convención (introducción, clonación, etc.).

Además, la Ley N° 30096, la categoría de delitos informáticos incluye otras actividades que no fueron consideradas en el texto final de Budapest, pero que luego fueron desarrolladas en sus protocolos. La situación es la siguiente: ataques sexuales a niños, niñas y jóvenes por medios técnicos (grooming), comercio ilegal de datos personales y modificaciones del artículo 162 (Interferencias telefónicas) y del artículo 323 (Discriminación e incitación a la discriminación) del Código Penal, incluye el uso de ordenadores. Los medios de comunicación o Internet lo catalogaron como agravante. Esto último no está exento de determinada disputa, sin embargo, en términos prácticos no perjudica en nada la futura utilización del Acuerdo, toda vez que entre los recientes adherentes se discuten protocolos para tipificar nuevos delitos como el discurso de odio y la xenofobia por medio de medios informáticos.

Huamán (2020), destaca que el establecimiento de un sistema uniforme de justicia penal sustantiva en el Perú es una tarea bastante avanzada, pero deben superarse varios obstáculos para lograr este objetivo. Al menos desde 2010, el interés por regular situaciones relacionadas con delitos informáticos ha dado lugar a diversas iniciativas legislativas, que han sido intensamente debatidas entre varios participantes del ecosistema. La definición del término "delito informático" en sí es problemática, ya que no hay acuerdo sobre si debería incluir únicamente delitos que legalmente poseen información o activos informáticos, o si también debería incluir delitos comunes cometidos utilizando computadoras. Por ejemplo, el texto no se procesaba en todos los casos y se penalizaban actividades comunes en Internet (como la creación de bases de datos) o actividades inofensivas, pero potencialmente rentables, como el hacking ético. Diversos expertos criticaron en su momento estas cuestiones y señalaron la distancia desfavorable entre esta norma y los estándares del

Convenio de Budapest. Recién cuando se aprobó la Ley N° 30171 en 2014, se mejoró la redacción y se modificaron o eliminaron las problemáticas.

Esto significa que tenemos una legislación que cumple con los estándares de Budapest, pero no está claro hasta qué punto creemos que los operadores del sistema de justicia la están utilizando de manera efectiva. Inicialmente, no había información pública sobre la ocurrencia de tales delitos, excepto actores privados que constantemente confirmaban la existencia de riesgos inminentes y trataban de ofrecer productos estables.

En ese aspecto, Huamán (2020), considera que no está claro cuántos de los casos iban más allá de investigaciones policiales, causas penales, juicios y veredictos. Sin figuras públicas ni otros medios para comprender la situación actual, los distintos actores trabajan a ciegas o descoordinados, a pesar de la existencia de una legislación adecuada para el uso general. Así lo demuestran las distintas medidas sectoriales impulsadas actualmente, que en la mayoría de los casos son contradictorias. Peor aún, otros han presentado denuncias por diversas violaciones de la ley para facilitar el trabajo de sus operadores sin seguir procedimientos acordados desde hace mucho tiempo.

Por ejemplo, si el Código Procesal Penal cuenta desde hace muchos años con un protocolo sobre injerencias legales en las comunicaciones, en 2015 se aprobó el Decreto Legislativo N° 1182, que crea un mecanismo al margen de esta ley que permitió a los policías obtener información geográfica sin su consentimiento, ni conocimiento, así como datos de ubicación. Esta última socava la legalidad de ciertas medidas de adquisición y reserva y amenaza la posición del Perú con respecto a la implementación de la Convención.

La Cooperación Internacional en el Convenio de Budapest

El Pacto de Budapest en el tercer capítulo establece un conjunto de deberes mínimos y posiciones habituales para permitir la cooperación entre los miembros. Estos compromisos todavía se refieren principalmente a la

adaptación de las leyes de extradición, la asistencia mutua y el establecimiento de unidades de respuesta a emergencias. En el primer caso, la iniciativa del Tratado de Budapest es que la extradición es posible siempre que se haya cometido un delito informático y el país correspondiente lo haya incorporado al código penal. Para ello, se propone añadir los delitos informáticos a los tratados de extradición anteriores y, en su defecto, utilizar la convención como base jurídica para su aplicación. En materia de asistencia mutua, se recomienda a los miembros compartir los resultados de las medidas recomendadas por la Sección de Derecho Penal en casos específicos con el fin de aumentar la eficiencia de los procesos penales.

Huamán (2020), considera que en el Perú no cuenta con una legislación en temas generales de cooperación que cumpla con los estándares de Budapest, que tienen como objetivo crear alianzas más estrechas entre sus estados miembros y fortalecer la cooperación entre países.

Por lo tanto, considera que el Perú tiene una buena oportunidad para mejorar su normativa interna, además de recibir apoyo y cooperación de otros países. Finalmente, se propone un modelo de colaboración basado en el establecimiento de puntos de contacto para dar respuesta a solicitudes urgentes que pueden o no estar relacionadas con el contenido de las solicitudes de asistencia mutua.

Huamán (2020), recalca que el Perú una vez que ha ratificado el tratado, el poder ejecutivo necesitará establecer un grupo de trabajo multiinstitucional para evaluar el proceso de utilización del tratado de Budapest. La composición mínima de este grupo de trabajo deberá ser: un representante de la Secretaría del Régimen Digital, un representante del Ministerio de Relaciones Exteriores, un representante del Ministerio de Justicia y Derechos Humanos, un representante del Ministerio de Transporte, un representante del Ministerio de

Relaciones Exteriores. El Ministerio del Interior, el Ministerio de Regulación y otros órganos que se consideren necesarios, incluso ajenos al sector público.

Asimismo, agrega que el propósito del grupo de trabajo es analizar la implementación del Convenio de Budapest y recomendar reformas a nivel nacional para lograr una adaptación exitosa.

Una vez que se establezcan los objetivos de la cooperación internacional, traerá enormes cambios y beneficios, proporcionando una mejor asistencia en la lucha contra el ciberdelito. En ese orden de ideas; se señala algunos aspectos positivos que pueden devenir de dicha activación funcional de Estado, como a continuación.

- Dentro de nuestro ecosistema digital es vulnerable a los ataques cibernéticos y puede incluso convertirse en un campo de pruebas para los terroristas digitales.
- Facilitar las investigaciones judiciales de delitos transfronterizos estableciendo canales oficiales de intercambio de información con los Estados miembros.
- Cuando en el país también se quiere impulsar el tema de la evidencia digital y emprender estrategias conjuntas contra el cibercrimen.

En ese sentido Huamán (2020), destaca que el uso del Acuerdo de Budapest estará relacionado con la manera en que se inicia el proceso de revisión y los tres objetivos declarados del Acuerdo de Budapest: desarrollar un marco unificado para el derecho penal sustantivo, estandarizar los procedimientos procesales y la experiencia en derecho informático, y promover el desarrollo global. Cooperación tras examinar la situación en este ámbito, cabe concluir que la utilización de este protocolo no requiere nuevos cambios significativos. Las mejores oportunidades para la formulación de políticas nacionales de seguridad cibernética pueden residir en la cooperación

internacional, lo que abriría la puerta a una mayor participación nacional en el espacio de discusión que la convención brinda a sus miembros.

En ese aspecto, Huamán (2020), considera que se observa la situación sobre el terreno, todo parece indicar que, en términos de cumplimiento, la aplicación del Tratado de Budapest requiere algunos cambios significativos.

Sin embargo, hay varias medidas que requieren una atención especial, sin las cuales no se pueden alcanzar los objetivos del acuerdo. El principal objetivo de estas actividades es hacer posible la implementación del Convenio y aprovecharlo, en particular las relacionadas con la armonización regulatoria y la cooperación internacional.

Sin embargo, la efectividad del uso del Convenio de Budapest (Convenio de Budapest sobre América Latina de 2018) varía y depende en gran medida de la relación entre la formulación de políticas nacionales, el grado de involucramiento de los actores y el papel que pueden desempeñar con mejoras y grado de respeto a los derechos humanos relevantes en cada periodo.

Por lo que Huamán (2020), en resumen, señala que se tiene que aceptar algunos escenarios que a veces son positivos y otras veces negativos para el ecosistema digital del Perú. La forma en que se desarrollen las cosas depende de la determinación de cada organización industrial individual. Por eso queremos que los debates sobre la implementación se lleven a cabo en un espacio abierto y transparente.

2.2.2. No formalización de la acción penal

Concepto de no formalización de la investigación

San Martín (2020), recalca que la no formalización de la investigación preparatoria, equivale al archivo de la investigación, el cual se encuentra estatuido en El artículo 334.1 del CPP define las bases sobre las cuales el fiscal puede disponer el archivo de la investigación al recibir una denuncia o al finalizar una subetapa procesal preliminar. Son: (i) el hecho no es un delito o es una

causa penal, (ii) que se presenten causas extintivas del derecho penal o no se nombra a la persona denunciada o investigada, como su nombre completo y apellido; y (iii) la faltante existencia de indicios y la participación de la persona que denuncia o investiga el delito.

Respecto al primer supuesto, se distingue entre la presunción de conducta atípica en la actividad delictiva y la ausencia de criminalidad. Un hecho puede ser atípico por falta de elementos objetivos o subjetivos, por razones válidas. Por otra parte, la conducta no es competencia penal porque el delito no tiene carácter penal o existen cláusulas que excluyen la pena.

De acuerdo a ello, San Martín (2020), precisa que las causales de extinción de la acción penal se encuentran establecidas en el artículo 78 del Código Procesal Penal establece las causas de terminación de una causa penal se origina: (i) por muerte del imputado, el plazo de prescripción, la amnistía y el derecho a la gracia, (ii) por ser cosa resuelta por el juez, (iii) en caso de ser por acción privada se extingue por desistir o por transacción. Finalmente, la causa de insuficiencia de pruebas surge cuando el fiscal encuentra pruebas insuficientes o no puede proceder con la investigación penal, lo que puede implicar no probar la existencia del delito y la responsabilidad penal del autor.

Naturaleza Jurídica de la No formalización de la Investigación

Ventocilla (2023), nos explica acerca de la naturaleza de los archivos fiscales en la teoría propuesta sustenta la siguiente posición:

1) Los archivos preliminares no tienen contenido jurisdiccional. El ordenamiento jurídico en el artículo 4, numeral 3 del Nuevo Código Procesal Penal literalmente señala que: *“La actividad investigativa realizada por el Ministerio de Estado (...) no tiene carácter jurisdiccional (...)”*, aunque esta disposición se refiere a una investigación, en lugar de referirse a la decisión tomada por el fiscal en relación con la emisión de la orden de sometimiento, pero según el Código, la solicitud tampoco tiene carácter jurisdiccional;

2) Otra rama de la doctrina que considera de carácter administrativo la fase investigativa propuesta por el fiscal, especialmente en los casos archivados, el profesor César San Martín Castro diría que la introducción del sistema de cuestiones de decisión es positiva, pero para nosotros está claro que los casos de decisión son un sistema de derecho administrativo, y hay que tener en cuenta que los casos de decisión obligan al Estado a agotar la vía administrativa y dan la oportunidad de impugnarlo ante las autoridades judiciales a través de procedimientos judiciales controvertidos. El contenido administrativo contenido en el artículo, que significa que la cuestión de decisión no resuelta puede ser modificada por decisión del poder judicial, esto no sucede en los casos fiscales, salvo la existencia de nuevos elementos, no puede ser refutado ante los tribunales, por lo que los procedimientos tributarios no califican como acto administrativo el acto, y mucho menos el objeto de la decisión (San Martín, 1999, p. 357).

Siguiendo a la doctrina Colombiana en comentarios del profesor Jaime Bernal Cuéllar y Eduardo Montealegre Lynett, sostienen si bien cuando se dicta resolución de archivo no existe proceso, esta circunstancia no impide ubicar la decisión como providencia de fondo, ya que resuelve aspectos fundamentales o sustanciales que tocan con el ejercicio de la acción penal y la existencia del delito y que a pesar de su trascendencia jurídica no hace tránsito a la cosa juzgada se refiere a decisiones que impiden nuevo debate por prueba sobreviniente el archivo es susceptible de ser revocado aunque se encuentre formalmente ejecutoriado y al no hacer tránsito a la cosa juzgada, la firmeza que adquiere con la ejecutoria es formal, en el sentido de precluir únicamente la posibilidad de interponer recursos contera la decisión mediante la cual el funcionario se abstiene de abrir investigación; y 3) Considero que el archivo fiscal tiene naturaleza jurisdiccional, teniendo en consideración que el fiscal como magistrado no es una simple autoridad administrativa, pues su actividad

se orienta a la legalidad y no a los intereses administrativos o de los administrados (Chávez, 2010).

El fiscal actúa como defensor de la legalidad y representante de la causa pública en el proceso penal. En efecto, el respeto de este principio implica que el Ministerio Público ejercite la acción penal por todo hecho que, revista los caracteres de un delito, sin perder de vista que su labor se ejecuta en función de la justicia y teniendo como parámetros a la Constitución caso contrario se puede promover la acción pertinente ante el órgano jurisdiccional. En la práctica en los distritos judiciales donde está operando el nuevo sistema procesal penal, se dictan disposiciones de archivo basadas casi con exclusividad en la denominada investigación preliminar, y que esto significa en buen romance, prescindir del juicio previo, es decir, dictar disposición de archivo aparentemente inconstitucional, pero que equivale a una absolución anticipada, que solo puede ser destruida por nueva prueba, caso contrario, es decir de no encontrarse nuevos elementos de convicción, ese archivo fiscal equivale a una cosa juzgada material que no permite reabrir el caso, por lo que es necesario se modifique la norma adjetiva para que se pueda impugnar el archivo fiscal sujetándose a las reglas del recurso de apelación y se dé seguridad jurídica, restableciendo la presunción de inocencia puesta en debate por la denuncia con éstas condiciones el archivo fiscal se rige como inimpugnable e inmutable, salvo que obedezca a razones de déficit o falta de elementos de prueba, por cuanto la existencia de nuevos elementos probatorios, no conocidos con anterioridad por el Ministerio Público, permitiría al titular de la acción penal reabrir la investigación preliminar, siempre que los mismos revelen la necesidad de una investigación del hecho punible y el delito no haya prescrito (Chávez, 2010).

2.3. Definición de términos conceptuales

- **Individualización del autor:** Hace referencia a la identificación y determinación de aquella persona responsable en la comisión de un delito,

para ello implica la recopilación de elementos materiales probatorios que permitan establecer la participación de un individuo en un hecho delictivo (Fiscalía General de la Nación, 2009).

- **Declaración indagatoria:** Es el acto procesal en el cual se recibe la declaración de una persona imputada en un proceso penal, con el objetivo de conocer su versión sobre los hechos investigatorios, siendo además considerado como el primer llamado efectuado de una persona para comparecer ante un proceso judicial sobre un delito investigado (Maio y Peralta, 2017).
- **Declaración testimonial:** Supone la declaración de un testigo sobre un hecho materia de investigación dentro de un proceso penal, considerado como una prueba importante, no porque supere a otras en valor, sino porque puede ser realizada en diferentes procedimientos (De Diego, 2001, p.133).
- **Fraude:** Definido como la acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete, ello implica la manipulación o engaño con ánimo de lucro (Acurio, 2007).
- **Fraude electrónico:** Resulta como una modalidad del delito de fraude, siendo efectuada mediante la manipulación informática o artificio similar que, con el propósito de lucrar, consigue una transferencia no consentida de cualquier activo patrimonial de un tercero (Acurio, 2007).
- **Presupuestos materiales:** Es entendida como las condiciones objetivas necesarias para que se considere una conducta como ilícita (Aldana y Bautista, 2014).
- **Prueba:** Conjunto de elementos materiales probatorios y evidencia física, que permite establecer la verdad sobre los hechos materia de investigación (Fiscalía General de la Nación, 2009).

- **Delito informático:** Denominación atribuida a aquella conducta ilícita cometida mediante medios informáticos, cuyo objetivo es dañar sistemas, satos o redes informáticas (Marca et al., 2021).

2.4. Enfoque filosófico – epistémico

La investigación presente se centra como puntos centrales en dos posturas; la primera, en la validez atribuida al derecho y la segunda es la importancia de la interpretación contextual de la normativa aplicada a un estado. Siendo de tal modo que ambos enfoques permiten analizar la norma vigente sobre los delitos informáticos y a la vez a la aplicación de estas en el ámbito fiscal, su propia interpretación y con ello el contexto empleado para su aplicación.

CAPÍTULO III

METODOLOGÍA Y TÉCNICAS DE INVESTIGACIÓN

3.1. Tipo de investigación

La presente investigación se realizó en base al tipo aplicado, debido a que la información recolectada fue de investigaciones básicas, de las cuales se formularon problemas e hipótesis con el propósito de responderlos sin manipularlos, ni alterarlos (Ñaupas et al., 2018, p. 136).

3.2. Nivel de investigación

Se tiene que, el nivel de investigación aplicado fue de tipo Descriptivo – Exploratorio, debido a que, este tipo de investigaciones comprenden la colección de datos para probar hipótesis o responder a interrogantes sobre el porqué de los objetos de forma más precisa.

3.3. Característica de la investigación

La investigación se caracterizó debido a la recolección de información de autores reconocidos, solo a nivel nacional sino también internacional, siendo como propósito principal poder ampliar todo aquello conocimiento sobre el procedimiento penal en casos de delitos informáticos y de aquellos factores que contribuyen a que estos casos se lleguen a formalizar en la sede fiscal.

3.4. Método de investigación

Para el presente estudio se aplicó el método analítico y crítico, el cual sirve para realizar análisis en el ámbito jurídico de los factores que determinan la no formalización de los procesos por delitos informáticos.

3.5. Diseño de investigación

El estudio contó con el diseño no experimental – descriptivo, por lo cual los datos que se van a recopilar serán plasmados de manera directa sin realizar modificaciones de por medio. El diseño descriptivo busca recopilar información sobre determinadas situaciones predeterminadas (Hernández et al., 2014).

El esquema es el siguiente:



Donde:

M= Muestra.

O= Observación

3.6. Procedimiento del muestreo

Población

La población será el conglomerado de todas las partes que posean una serie de características en común; en ese sentido, si esta se trata de seres humanos es adecuado denominarlos población, empero, si se tratase cualquier cosa que no sean individuos humanos se les denominará universo de estudio. (Sánchez et al., 2018).

La población estuvo conformada por todas las carpetas fiscales vistos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022.

Muestra

Una muestra es una colección de casos o individuos tomados de una población por el sistema de muestreo, probable o no. (Sánchez et al., 2018). En

cambio, la muestra se obtiene con el método de improbabilidad a discreción del investigador.

La muestra estuvo conformada por 8 carpetas fiscales sobre delitos informáticos vistos en la Tercera fiscalía provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022.

3.7. Técnicas e instrumentos de recolección de datos

Tabla 1 Técnicas e instrumentos de recolección de datos.

Técnica	Instrumento
Análisis documental	Matriz de análisis documental. Esta técnica es usada para la organización, clasificación y análisis de la información extraída de fuentes documentales.

Fuente: Criterio de la investigadora

3.8. Técnicas de procesamiento y análisis de datos

Se analizarán las carpetas fiscales mencionadas líneas arriba, a través de la matriz de análisis documental, en el cual se detallara primeramente aspectos generales de las carpetas fiscales, como el número de carpeta fiscal, el nombre de la Fiscalía correspondiente, los hechos materia de investigación; asimismo, la parte esencial de dicha matriz de análisis es el pronunciamiento a través de los indicadores fijados en la operación y análisis de variables, de los cuales se seleccionaron los que tenían mayor relevancia y aproximación al objetivo que pretende este estudio.

3.9. Orientación ética

Para llevar a cabo esta investigación se tuvo en consideración siempre prevalecer la verdad, respetando las etapas establecidas para la realización de toda investigación, denotando en ese sentido que declaro tener conocimiento de las sanciones que impone el sistema universitario en caso de incumplir con ello.

CAPÍTULO IV

PRESENTACION DE RESULTADOS

4.1. Presentación, análisis e interpretación de resultados

Tabla 2 Caso Fajardo - Vergara

“Factores que determinan la no Formalización de los Delitos Informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022”	
Nº DE CARPETA	180-2022
AGRAVIADO	Yenny Sara Huayhua Flores
IMPUTADO	Davi Johnny Fajardo Huilca y Harold Abelardo Vergara Zelada
MATERIA	La materia del caso se relaciona con presuntos delitos informáticos y financieros, incluyendo fraude informático y posiblemente asociado a la manipulación indebida de tarjetas bancarias y datos personales.
HECHOS	Los hechos sucedieron cuando Yenny Sara Huayhua Flores, al intentar realizar una llamada telefónica desde su hogar, se percató de problemas en su servicio telefónico y luego descubrió una transferencia no autorizada desde su cuenta bancaria hacia otra cuenta a nombre de Davi Johnny Fajardo Huilca. La investigación policial condujo a la detención de Davi Johnny Fajardo Huilca y luego a Harold Abelardo Vergara Zelada, quienes confesaron haber participado en la manipulación de tarjetas bancarias a cambio de dinero.
NO FORMALIZACIÓN DE LA ACCIÓN PENAL	Que el hecho constituya delito porque aún no se ha formalizado la acción penal, ya que se encuentran en la etapa de investigación. Los imputados han sido detenidos y se están recopilando pruebas para determinar la formalización de los cargos.

DELITOS INFORMÁTICOS	El presunto delito de fraude electrónico se evidencia a través de la transferencia no autorizada de fondos desde la cuenta bancaria de Yenny Sara Huayhua Flores hacia otra cuenta, a nombre de Davi Johnny Fajardo Huillca. Esta acción constituye un posible fraude informático al acceder y transferir fondos sin el consentimiento del titular de la cuenta bancaria afectada.
---------------------------------	--

Análisis

El 23 de febrero de 2022, Yenny Sara Huayhua Flores, de 43 años, presenta una denuncia en la DIVINDAT alegando ser víctima de un delito informático. Mientras estaba en su hogar, intenta realizar una llamada telefónica, pero descubre que su teléfono no puede hacer ni recibir llamadas. Al contactar a la operadora Movistar, le informan sobre una supuesta deuda pendiente de S/.17.00 soles y que su número estaba asociado al nombre de Héctor Porras Mayta o Héctor Viayta Porras.

Descubrimiento del Fraude

- Yenny Sara Huayhua Flores, alarmada por la situación, verifica su cuenta bancaria a través del sitio web del Banco de la Nación. Descubre que le falta una suma significativa de dinero: S/.6,910.00 soles. Investiga más a fondo y se da cuenta de que se realizó una transferencia no autorizada de S/.6,800.00 soles, más una comisión de S/.40.80 soles, hacia una cuenta del Banco de Crédito del Perú a nombre de Davi Johnny Fajardo Huillca.

Acciones Policiales

- La Policía Nacional del Perú, liderada por el CMDTE PNP José Montero Peche, emprende una investigación. Ubican y detienen a Davi Johnny Fajardo Huillca en Carabayllo, encontrándolo en posesión de un teléfono celular LG Modelo D331, junto con un IMEI específico (356062063374326) que se registra en el acta de registro e incautación.

- Davi Johnny Fajardo Huillca confiesa ser titular de la cuenta bancaria del Banco de Crédito del Perú involucrada en la transferencia. Afirma haber entregado su tarjeta y clave a su amigo "Harold", quien trabaja como delivery en la pollería Riveras Chicken. Este amigo le pagó 90 soles y no le devolvió la tarjeta.
- La policía, basada en esta información, detiene a Harold Abelardo Vergara Zelada, en posesión de un teléfono celular Samsung modelo A50 con un IMEI específico (358997070751313) y varias tarjetas bancarias que podrían estar relacionadas con el fraude.
- Harold confiesa haber recibido la tarjeta bancaria de Davi Johnny Fajardo Huillca y haberla entregado a un individuo llamado "José Carranza" a cambio de 500 soles. Da información limitada sobre José Carranza, solo proporcionando un número de teléfono asociado (986297948).

Consecuencias Legales

- Davi Johnny Fajardo Huillca y Harold Abelardo Vergara Zelada, junto con las tarjetas bancarias incautadas, son trasladados a la División de Investigación de Delitos de Alta Tecnología por presunta participación en delitos contra la tranquilidad pública y fraude informático contra Yenny Sara Huayhua Flores y el Estado Peruano.
- La Fiscalía Provincial Penal de Turno de Carabayllo es informada del arresto, siendo asumida la investigación por el Dr. Guillermo Domínguez Romero.

Este análisis detallado proporciona un panorama exhaustivo de los eventos, las acciones policiales, las confesiones de los detenidos y las implicaciones legales resultantes del presunto fraude informático contra Yenny Sara Huayhua Flores.

Comentario Final

El caso ilustra una situación de presunto fraude informático donde múltiples individuos están implicados en el desvío de fondos y el uso indebido de tarjetas bancarias. La rápida intervención policial condujo a la detención de los presuntos responsables, aunque la cadena de manipulación de tarjetas entre Davi Johnny Fajardo Huillca, Harold Abelardo Vergara Zelada y José Carranza sugiere una red más amplia involucrada en actividades fraudulentas. Este caso subraya la importancia de la vigilancia y seguridad en las transacciones financieras, así como la necesidad de una mayor conciencia sobre la protección de los datos personales y financieros en entornos digitales.

Tabla 3 Caso Díaz - Fernandez

“Factores que determinan la no Formalización de los Delitos Informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022”	
Nº DE CARPETA	2228-2021
AGRAVIADO	Banco de la Nación del Perú
IMPUTADO	Kevin Steve Díaz Montenegro y José Esteban Fernández Salinas
MATERIA	La materia del caso se relaciona principalmente con el presunto delito de fraude electrónico, dado que se describen acciones sospechosas, como retiros de efectivo sin el uso de tarjetas bancarias en un cajero automático, lo que indica una posible manipulación fraudulenta de cuentas bancarias.
HECHOS	En la ciudad de Lima, específicamente en un cajero automático ubicado en la Av. Isabel Chimpu Ocho N° 748, se observa una serie de transacciones inusuales durante la noche. El personal policial recibe información sobre actividades sospechosas en ese cajero automático. En respuesta a la alerta, se despliega un equipo policial dirigido por el instructor Capitán PNP José Tapia Combria, de la DIVIEOD - DIRINCRI, al lugar señalado. Observan un vehículo y a un individuo, identificado como José Esteban Fernández Salinas, realizando transacciones no autorizadas en el cajero automático. Se descubren cinco comprobantes de retiro de efectivo sin el uso de tarjeta, todos en minutos consecutivos y por sumas de dinero específicas, coincidiendo con las actividades observadas. Además, se

	<p>confisca una cantidad significativa de dinero en efectivo a José Esteban Fernández Salinas.</p> <p>Tras la intervención, se detiene a Kevin Steve Díaz Montenegro y a José Esteban Fernández Salinas, quienes se encontraban en el lugar y portaban elementos relacionados con las transacciones no autorizadas en el cajero automático.</p>
NO FORMALIZACIÓN DE LA ACCIÓN PENAL	<p>Individualización de los Autores: Los individuos implicados son identificados como Kevin Steve Díaz Montenegro, de 20 años, y José Esteban Fernández Salinas, de 23 años, quienes fueron detenidos en el lugar de los hechos</p>
DELITOS INFORMÁTICOS	<p>Fraude Electrónico: Queda implícito en las operaciones realizadas en el cajero automático sin el uso de tarjetas bancarias, lo que sugiere un posible fraude electrónico en la manipulación de cuentas y transacciones.</p> <p>Robo de Bancos: La acción de retirar dinero sin autorización en el cajero automático podría asociarse a un tipo de robo bancario.</p>

Análisis

El evento ocurrió en un cajero automático ubicado en la Av. Isabel Chimpu Ocho N° 748, en Lima, Perú. Se recibió información sobre actividades sospechosas en este lugar, específicamente retiros inusuales de efectivo durante altas horas de la noche. En respuesta a la alerta, el instructor Capitán PNP José Tapia Combria, junto con el personal de la DIVIEOD - DIRINCRI, se dirigió al cajero automático para investigar las actividades reportadas. Se observó la llegada de un vehículo con la placa D5A-359 y un individuo, José Esteban Fernández Salinas, quien se dirigió al cajero automático y realizó transacciones inusuales que incluyeron retiros de efectivo sin el uso de una tarjeta bancaria. Se descubrieron cinco comprobantes de retiros de efectivo sin el uso de tarjeta, todos realizados en minutos consecutivos y por montos específicos. Se confiscó una cantidad considerable de efectivo a José Esteban Fernández Salinas. Se procedió a la detención de Kevin Steve Díaz Montenegro y José Esteban Fernández Salinas, quienes fueron encontrados en el lugar con

elementos relacionados con las transacciones no autorizadas en el cajero automático.

Análisis del Incidente

Los hechos apuntan a un posible fraude electrónico, ya que se realizaron retiros de dinero en efectivo sin el uso de tarjetas bancarias. Esto sugiere un posible manejo fraudulento de cuentas bancarias en el cajero automático.

Comentario

El rápido accionar policial y la detención de los individuos involucrados sugieren una respuesta efectiva para evitar posibles delitos financieros. Este caso subraya la importancia de la vigilancia en los sistemas bancarios y la necesidad de medidas de seguridad más estrictas para proteger las transacciones financieras.

Este análisis destaca la detección y actuación rápida de la policía frente a un presunto caso de fraude electrónico en un cajero automático, resaltando la necesidad de mantener la seguridad en las operaciones bancarias para prevenir este tipo de delitos

Tabla 4 Caso L.Q.R.R. (1)

“Factores que determinan la no Formalización de los Delitos Informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022”	
Nº DE CARPETA	3059-2022
AGRAVIADO	La empresa ALI HOUSE S.A.C
IMPUTADO	L.Q.R.R.
MATERIA	Se trata de un presunto fraude informático, en el que se intentó acceder a la cuenta de la empresa utilizando métodos fraudulentos, manipulando la información de acceso mediante engaños para realizar transferencias no autorizadas.
HECHOS	La denunciante accedió a la página de Net Cash a través de la plataforma de búsqueda Google. Tras ingresar su contraseña, recibió una llamada de un supuesto representante del Banco BBVA que solicitó instalar un programa de acceso remoto en su computadora. Luego de seguir sus indicaciones, se produjeron manipulaciones en

	su computadora que resultaron en el bloqueo de acceso a su cuenta de Net Cash y transferencias no autorizadas desde la cuenta bancaria de la empresa.
NO FORMALIZACIÓN DE LA ACCIÓN PENAL	Que el hecho constituya delito porque aún no se ha formalizado la acción penal, ya que se encuentran en la etapa de investigación.
DELITOS INFORMÁTICOS	El presunto delito de fraude electrónico se evidencia a través de la transferencia no autorizada de fondos desde la cuenta bancaria

Análisis

El relato describe un presunto fraude informático perpetrado contra la empresa ALI HOUSE S.A.C. Los hechos comienzan cuando la denunciante accede a la página de Net Cash a través de la plataforma de búsqueda Google y recibe una llamada de una persona que se identifica como representante del Banco BBVA. Esta persona solicita a la denunciante que instale un programa de acceso remoto en su computadora para vincular la dirección IP con la identidad bancaria. A continuación, la denunciante sigue las indicaciones del supuesto representante del banco, proporciona información confidencial y permite la instalación de un programa remoto en su computadora. Posteriormente, se suceden una serie de eventos en los que la pantalla de su computadora se oscurece repetidamente y se bloquea. Durante estos incidentes, se realizaron transferencias no autorizadas desde la cuenta bancaria de la empresa por un total de 5,423.85 soles.

La empresa intenta bloquear el acceso a sus cuentas bancarias una vez que detecta la irregularidad, pero no obtiene más información del banco sobre las cuentas beneficiarias ni se le brinda más detalle sobre el fraude sufrido. La denuncia se califica como fraude informático según el artículo 8 de la Ley N.º 30096, el cual tipifica y sanciona el acceso ilegítimo a sistemas informáticos con el fin de obtener un beneficio ilícito en perjuicio de terceros. Además, se

evidencia la presunta comisión del delito en el relato de los hechos, donde se manipuló a la denunciante para obtener acceso a su información bancaria y realizar transferencias no autorizadas.

El Ministerio Público está llevando a cabo diligencias preliminares para recabar evidencia que permita fundamentar una posible formalización de la investigación. Se establece un plazo de 60 días para llevar a cabo estas diligencias preliminares, aunque el fiscal puede ampliar este plazo según las complejidades del caso.

Comentario

El relato expuesto es un claro ejemplo de fraude informático mediante técnicas de ingeniería social. Se destaca la astucia de los perpetradores al engañar a la víctima para instalar un programa que les permitió acceder ilegalmente a sus datos bancarios y realizar transferencias no autorizadas. Es importante que las entidades bancarias refuercen la seguridad y la educación sobre estas tácticas de fraude para prevenir situaciones similares en el futuro. Además, es crucial que se lleve a cabo una investigación exhaustiva para identificar y llevar a juicio a los responsables de estos actos ilícitos.

Tabla 5 Caso L.Q.R.R. (2)

“Factores que determinan la no Formalización de los Delitos Informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022”	
Nº DE CARPETA	388-2022
AGRAVIADO	José Antonio Morales Urrutia.
IMPUTADO	L.Q.R.R.
MATERIA	Delito contra el patrimonio, en la modalidad de Fraude Informático.
HECHOS	Se tiene como noticia criminal, la denuncia interpuesta por JOSE ANTONIO MORALES URUTIA, quien refiere haber sido víctima de hurto de dinero mediante compras por internet de su tarjeta de ahorros del Banco de Crédito del Perú — N° de tarjeta 455788043840083, por un monto de 477.24 Nuevos Soles, percatándose de los hechos el día 18 de abril de 2022 a las 16:00 horas, en circunstancias que recibió una llamada del BCP mediante

	el cual le informaron que su tarjeta habría sido bloqueada, porque habían realizarlo unas compras inusuales en Dólares, utilizando su tarjeta de ahorros, desconociendo a los autores del hecho, así mismo refiere que pueden notificarle al número 9132999 \ 49. adjuntando una hoja de los Últimos movimientos que habrían realizado con su tarjeta
NO FORMALIZACIÓN DE LA ACCIÓN PENAL	No hay declaración del imputado ni de testigos. Se desconocen algunos aspectos como la declaración del imputado y testigos, la falta de pruebas concretas y la individualización del autor.
DELITOS INFORMÁTICOS	Fraude electrónico. Se menciona un caso de fraude electrónico relacionado con compras inusuales realizadas sin autorización del titular de la tarjeta.

Análisis

El caso presentado relata una denuncia por hurto de dinero a través de compras por internet con la tarjeta de ahorros del Banco de Crédito del Perú. José Antonio Morales Urrutia denuncia que se percató de este hecho el día 18 de abril de 2022 a las 16:00 horas cuando recibió una llamada del banco informándole sobre compras inusuales en dólares realizadas con su tarjeta, desconociendo a los autores del hecho. Adjunta los últimos movimientos de su tarjeta bancaria que evidencian las compras fraudulentas.

El Ministerio Público ha calificado estos hechos como un presunto delito contra el patrimonio, en la modalidad de Fraude Informático, tipificado en el artículo 8 de la Ley N° 30096 de Delitos Informáticos. Este artículo penaliza la obtención ilícita de beneficios mediante tecnologías de la información o la alteración de datos informáticos en perjuicio de terceros.

En relación con el Ministerio Público, se destaca su función fundamental en el proceso penal como el órgano autónomo encargado de ejercer la acción penal, defender la legalidad y los intereses públicos, así como representar a la sociedad en los procesos judiciales.

Las diligencias preliminares que se llevan a cabo tienen como objetivo principal obtener los elementos de convicción necesarios para determinar si se debe formalizar una investigación preparatoria. Esto implica evaluar si existen indicios suficientes de la comisión del delito, si se ha individualizado al imputado y si se cumplen los requisitos de procedibilidad.

Comentario

Al respecto se destaca la importancia de la labor del Ministerio Público en la investigación y el esclarecimiento de los hechos, así como la necesidad de recopilar pruebas y evidencias para fundamentar la formalización de la investigación y perseguir a los presuntos responsables del fraude informático.

Tabla 6 Caso L.Q.R.R. (3)

“Factores que determinan la no Formalización de los Delitos Informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022”	
Nº DE CARPETA	690-2022
AGRAVIADO	Genry Luis Alonso Ronquillo
IMPUTADO	L.Q.R.R.
MATERIA	Delito contra el patrimonio - Estafa.
HECHOS	Fluye de la denuncia policial, que con fecha 18 de febrero de 2022, se apersono a la comisaria del Progreso la persona de Genry Luis Alonso Ronquillo, denunciando de manera extemporánea, presuntos hechos de estafa cometidos en su agravio sucedidos con fecha 09 de febrero de 2022, en circunstancias de haber recibido como a las diez de la mañana una llamada telefónica a su celular de parte del Banco BBVA Continental, indicándole que tenía que anular sus dos tarjetas de Crédito Visa de Cuenta N° 4147914971 que tenía un monto de S/. 20,000.00 soles y la tarjeta de Crédito Visa cuentan *5007 que también tenía un monto de S/. 20,000.00 soles, y que por la anulación de ambas tarjetas le darían una tarjeta Visa Signatura sin ningún cobro anual, pues si no anulaba ambas tarjetas de crédito le iban a cobrar una membresía anual de \$ 1,200.00 dólares, lo que acepta el agraviado la tarjeta Visa Signatura, a la cual harían la transferencia de ambas tarjetas por un monto total de S/. 40,000.00 soles, quienes también le piden la contraseña como un gesto de aceptación la cual accede dársela, pidiéndole también su dirección a fin de hacerle Llegar la carta

	de anulación de tarjeta, Indicándole además que el mismo día 09 de febrero al promediar las 03 o 04 de la tarde llegaría un joven para entregarle la carta de anulación de la tarjeta de crédito para que acordado, por lo que al promediar las tres de la tarde un joven de aproximadamente de 32 años, vestido con camisa con el logo del banco Continental, su credencial y un folder manila que contenía la carta de anulación de la tarjeta, quien le pide las tarjetas de crédito las que corta en su presencia y se las lleva, indicándole que dentro de las 24 horas le llegaría su nueva tarjeta a su domicilio, y al 16 de febrero de revisar su estado de cuenta darse con la sorpresa que habían retirado de su tarjeta visa un monto de S/. 4,115.00soles, y de la tarjeta MasterCard un monto de S/. 3,300.00 soles, por un total de S/. 7,115.00 soles.
NO FORMALIZACIÓN DE LA ACCIÓN PENAL	No hay declaración del imputado ni de testigos. Se desconocen algunos aspectos como la declaración del imputado y testigos, la falta de pruebas concretas y la individualización del autor.
DELITOS INFORMÁTICOS	Fraude electrónico, Engaño mediante llamada telefónica, obtención de información sensible y retiros no autorizados.

Análisis

La denuncia interpuesta por Genry Luis Alonso Ronquillo por un presunto caso de estafa sufrida el 9 de febrero de 2022. Según su testimonio, recibió una llamada del Banco BBVA Continental donde le informaron sobre la anulación de dos tarjetas de crédito Visa, sugiriendo la obtención de una nueva tarjeta sin costo anual. Bajo esta premisa y como parte del proceso, le solicitaron su contraseña y dirección, supuestamente para enviarle la carta de anulación de la tarjeta.

Posteriormente, un individuo se presentó en su domicilio para recoger las tarjetas que fueron cortadas en su presencia, con la promesa de que en 24 horas recibiría la nueva tarjeta. Sin embargo, al revisar su estado de cuenta, notó retiros no autorizados por un monto total de S/. 7,115.00 soles.

La calificación jurídica apunta al delito de estafa, tipificado en el artículo 196 del Código Penal, relacionado con la obtención de un beneficio ilícito a costa

de terceros mediante engaño. El Ministerio Público debe llevar a cabo la investigación preliminar para determinar si existen pruebas que sustenten la comisión del delito, asegurando los elementos materiales y la identificación de los implicados.

Se destaca la importancia de la etapa de investigación preliminar, donde se deben realizar diligencias urgentes para determinar la existencia y naturaleza del delito, así como la identificación de los involucrados y la recolección de elementos probatorios.

Comentario

El caso presenta un presunto fraude informático relacionado con la obtención de información privada de tarjetas bancarias a través de engaño telefónico. El Ministerio Público deberá llevar a cabo una investigación preliminar para determinar la existencia del delito, identificar a los responsables y recolectar pruebas que sustenten el caso.

Tabla 7 Caso: VARGAS

“Factores que determinan la no Formalización de los Delitos Informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022”	
Nº DE CARPETA	1050-2022
AGRAVIADO	Margarita Nancy Salas Zuluaga
IMPUTADO	Carlos Vargas Trujillo
MATERIA	Delito contra el Patrimonio - Estafa
HECHOS	La agraviada se comunicó por redes sociales con Carlos Vargas Trujillo para comprar una trimóvil. La supuesta vendedora solicitó un pago por adelantado, primero el 50% y luego S/. 400.00 soles, y finalmente aceptó S/. 300.00 soles por parte de la víctima. Posteriormente, debido a limitaciones en el Banco, la denunciada proporcionó otra cuenta perteneciente a Edwin Alexander Herrera Cisneros, donde Margarita depositó los S/. 100.00 soles restantes. Después de la transacción, el perfil de la presunta estafadora desapareció de las redes sociales.

NO FORMALIZACIÓN DE LA ACCIÓN PENAL	No hay declaración del imputado ni de testigos. Se desconocen algunos aspectos como la declaración del imputado y testigos, la falta de pruebas concretas y la individualización del autor.
DELITOS INFORMÁTICOS	Fraude electrónico, Engaño mediante llamada telefónica, obtención de información sensible y retiros no autorizados.

Análisis

Este fragmento describe una denuncia de estafa realizada por Margarita Nancy Salas Zuluaga, quien reportó haber sido víctima de un fraude el 10 de agosto de 2022. Según su declaración, contactó a través de Facebook a una persona identificada como Carlos Vargas Trujillo para comprar una trimóvil valorada en S/. 3,000. La presunta estafadora le pidió el 50% del monto por adelantado para concretar la compra. Al inicio, la denunciante no accedió, pero luego la vendedora le ofreció pagar S/. 400.00 soles por adelantado y el resto a la entrega.

La denunciante realizó un giro de S/. 300.00 soles y envió la captura a través de WhatsApp. Posteriormente, ante la imposibilidad de realizar más giros en el Banco de Crédito del Perú (BCP), la estafadora le proporcionó otra cuenta bancaria del Banco Interbank perteneciente a Edwin Alexander Herrera Cisneros, donde Margarita depositó los S/. 100.00 soles restantes. Sin embargo, al verificar las redes sociales después de la transacción, descubrió que el perfil de Facebook y el número de WhatsApp de la vendedora habían desaparecido.

La calificación jurídica se enfoca en el delito de estafa, definido en el artículo 196 del Código Penal, que castiga a quien obtiene un beneficio ilícito en perjuicio de terceros a través de engaño.

Se ordena iniciar una investigación preliminar para esclarecer los hechos denunciados, identificar a los posibles responsables y recabar más información sobre la transacción fraudulenta. Se programan diligencias, incluyendo la declaración de la agraviada Margarita Nancy Salas Zuluaga y la declaración

testimonial de Edwin Alexander Herrera Cisneros para el día 31 de agosto de 2022 en las oficinas de la fiscalía provincial Penal Corporativa de Carabayllo.

El Ministerio Público está procediendo a realizar las diligencias preliminares para determinar la veracidad de la denuncia y reunir elementos que permitan iniciar una investigación formal si se confirman indicios del delito.

Comentario

En el análisis de esta situación, se destaca la complejidad que implica la identificación y persecución de delitos cometidos a través de medios digitales y de comunicación. La estafa perpetrada mediante la manipulación en redes sociales y comunicación telefónica refleja cómo los criminales se valen de estos canales para engañar y defraudar a las víctimas. La dificultad radica en la falta de pruebas sólidas y la identificación completa de los presuntos responsables, lo que dificulta la formalización de la acción penal. Aunque se presume la comisión de un delito de estafa, la ausencia de testigos y evidencia contundente presenta un desafío para llevar a cabo un proceso legal efectivo. Es crucial seguir investigando y recopilar pruebas que permitan identificar con precisión a los autores de estos actos fraudulentos. Además, se hace evidente la necesidad de concienciar a la población sobre la seguridad en las transacciones en línea y la verificación de la identidad de los vendedores antes de realizar cualquier pago anticipado para evitar situaciones de este tipo.

Tabla 8 Caso: L.Q.R.R. (4)

“Factores que determinan la no Formalización de los Delitos Informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022”	
Nº DE CARPETA	398-2023
AGRAVIADO	Cristhian Edwin BERNAL SARAVIA
IMPUTADO	LQRR
MATERIA	Relacionarse con presuntos delitos informáticos, específicamente aquellos vinculados con la denuncia de una transacción no reconocida realizada en una plataforma online, como la Apple Web Store, utilizando una tarjeta de crédito sin el consentimiento del titular.
HECHOS	En esta sección, se espera que se detalle la secuencia de eventos o acciones que llevaron al incidente reportado. En un caso de fraude informático, esto podría incluir cómo se realizó la transacción, quién la llevó a cabo (si se puede identificar), la fecha y hora, la plataforma o servicio utilizados y cualquier otro detalle relevante que explique cómo ocurrió el presunto delito.
NO FORMALIZACIÓN DE LA ACCIÓN PENAL	No hay declaración del imputado ni de testigos. Se desconocen algunos aspectos como la declaración del imputado y testigos, la falta de pruebas concretas y la individualización del autor.
DELITOS INFORMÁTICOS	Fraude electrónico, Engaño mediante llamada telefónica, obtención de información sensible y retiros no autorizados.

Análisis

El texto resalta el papel determinante del Ministerio Público en el proceso penal, indicando que este órgano constitucional autónomo tiene la titularidad del ejercicio de la acción penal, la defensa de la legalidad y de los intereses públicos según lo estipulado en la Constitución. Se menciona que representa a la sociedad en estos procesos. Esta sección destaca la autoridad y responsabilidad del Ministerio Público en la aplicación de la ley y la administración de justicia. Subraya la importancia de su papel en la defensa de los intereses colectivos y en la búsqueda de la verdad durante los procesos penales.

Se subraya la obligación del Ministerio Público y sus fiscales de actuar con objetividad en sus decisiones durante las investigaciones preliminares o preparatorias. Se establece que la objetividad va más allá de lo que afirma una denuncia, incidiendo en lo que se evidencia de su contenido y de las diligencias iniciales de investigación. Se enfatiza la necesidad de que el fiscal investigador actúe de manera imparcial para determinar la responsabilidad o inocencia del imputado. Esta parte enfatiza la imparcialidad como un principio fundamental para los fiscales al llevar a cabo sus funciones. Destaca que las decisiones deben basarse en hechos objetivos y pruebas, no solo en la acusación inicial, para garantizar una investigación justa y equitativa.

Se presenta un caso específico de denuncia por parte de Cristhian Edwin Bernal Saravia, quien reporta una compra no reconocida en la Apple Web Store con su tarjeta Interbank. Esta sección proporciona un ejemplo concreto que ilustra la aplicación práctica de los principios discutidos anteriormente. Sirve como caso de estudio para comprender cómo se aplican los conceptos teóricos de la intervención del Ministerio Público y la objetividad en una situación real.

Comentario

Este análisis detallado revela cómo se enfoca en los pilares fundamentales del sistema judicial, promoviendo la transparencia, la justicia y la imparcialidad en el proceso penal a través del rol del Ministerio Público y los principios que rigen su actuación.

Tabla 9 Caso: ALVARADO - DIOSES

“Factores que determinan la no Formalización de los Delitos Informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022”	
Nº DE CARPETA	992-2023
AGRAVIADO	Leonardo Castillo Acevedo
IMPUTADO	Marcos David Alvarado Falla y Dennys Antonio Dioses Ramírez.
MATERIA	Fraude informático, específicamente descrito como delitos contra los datos informáticos, según lo establecido en el artículo 8 de la Ley 30171. Este delito implica el uso indebido de tecnologías de la información o la comunicación para obtener un beneficio ilegítimo perjudicando a otra persona
HECHOS	Los hechos se suscitaron cuando Leonardo Castillo Acevedo recibió llamadas telefónicas y mensajes de una persona que se identificó como Gabriel Cavero Sánchez, supuesto asesor del Banco Pichincha. Esta persona ofreció créditos y solicitó información personal al agraviado, quien accedió. Posteriormente, se realizaron transacciones fraudulentas en las cuentas bancarias del agraviado, las cuales él no autorizó.
NO FORMALIZACIÓN DE LA ACCIÓN PENAL	Falta de pruebas que evidencien el hecho. se constata una falta de acciones legales por parte de las autoridades competentes para perseguir y enjuiciar a los presuntos responsables del fraude informático a pesar de la existencia de evidencia o indicios claros.
DELITOS INFORMÁTICOS	Fraude electrónico, relacionados con los delitos informáticos podrían evidenciarse en el acceso ilegítimo y el uso no autorizado de los datos informáticos del agraviado para realizar transacciones fraudulentas.

Análisis

Se relatan los eventos ocurridos el 24 de junio de 2023, donde se detalla la interacción entre el denunciante y un presunto estafador haciéndose pasar por asesor bancario. Se mencionan las transacciones fraudulentas realizadas en las tarjetas bancarias del denunciante al día siguiente.

Se hace referencia a las atribuciones constitucionales y legales del Ministerio Público, destacando su responsabilidad en el ejercicio de la acción penal, la defensa de la legalidad y la representación de la sociedad. Se subraya

la obligación de los fiscales de actuar con objetividad e indagar los hechos para determinar la responsabilidad o inocencia del imputado. Se detallan las finalidades de la investigación preliminar, enfatizando la necesidad de determinar la veracidad de los hechos denunciados, asegurar pruebas materiales y individualizar a las personas involucradas.

Se explica que estas diligencias son fundamentales para iniciar una investigación preparatoria. Se realiza una clasificación legal de los eventos denunciados como fraude informático, especificando la tipificación de este delito según el artículo 8 de la Ley 30171. Se detallan las acciones que constituyen el fraude informático y las penas asociadas. Se establece el plazo razonable para la investigación preliminar, señalando que, en este caso, se fija un lapso de 60 días naturales para llevar a cabo las diligencias necesarias.

Comentario:

El documento presenta una narrativa detallada de los eventos alegados por el denunciante y contextualiza los pasos legales y procesales que el Ministerio Público debe seguir en este caso de presunto fraude informático. Destaca la importancia de la objetividad en la investigación y la búsqueda de pruebas para determinar la existencia de un delito.

La calificación jurídica precisa de los actos denunciados como fraude informático muestra una clara intención de categorizar legalmente los hechos y establecer las posibles consecuencias legales para los presuntos autores. El planteamiento del plazo para la investigación preliminar muestra una consideración sobre la complejidad y la necesidad de realizar diligencias exhaustivas para esclarecer los hechos denunciados.

4.2. Discusión de resultados

Las hipótesis planteadas se centran en los factores que podrían influir en la no formalización de los delitos informáticos en la Tercera Fiscalía Provincial

Penal Corporativa de Carabayllo, Lima Norte, en el año 2022. Analicemos los resultados de estas hipótesis:

Hipótesis General

"Los factores que intervienen en la no formalización de los delitos informáticos en la Tercera Fiscalía Provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022 son la falta de medios probatorios recabados en las diligencias de investigación."

Esta hipótesis general sugiere que la carencia de medios probatorios es un factor primordial que influye en la no formalización de los delitos informáticos. Es esencial considerar que, en casos de delitos informáticos, la recolección de pruebas suele ser más compleja debido a la naturaleza digital de los crímenes. La falta de evidencia sólida puede dificultar la atribución de responsabilidad a los presuntos autores.

Hipótesis Específicas

HE1: La falta de presupuestos materiales determinará la no formalización de los procesos de delitos informáticos en los casos donde no se haya logrado individualizar al imputado, así como también en los casos donde el hecho denunciado no logre ser encuadrado en el tipo penal como delito. Esta hipótesis específica apunta a dos situaciones principales: la incapacidad para identificar al presunto autor del delito y la falta de enmarcado del hecho en un tipo penal específico. La falta de individualización del imputado puede dificultar la continuación del proceso penal, ya que se necesita un imputado identificado para proceder legalmente. Además, si el hecho denunciado no cumple con los requisitos para ser considerado un delito, podría resultar en la no formalización del caso.

HE2: Se determinó que la insuficiencia de elementos de convicción afecta en un nivel considerablemente alto en la formalización de los procesos de delitos informáticos en la Tercera Fiscalía Provincial Penal Corporativa de

Carabaylo en el Distrito Fiscal de Lima Norte, 2022. Esta hipótesis específica sugiere que la falta de elementos de convicción tiene un impacto significativo en la formalización de los casos de delitos informáticos. La insuficiencia de pruebas sólidas y contundentes puede obstaculizar la presentación de cargos y la continuación del proceso legal.

CONCLUSIONES

PRIMERA

La investigación revela que la falta de medios probatorios sólidos es un factor primordial que influye en la no formalización de los delitos informáticos en esta Fiscalía. La complejidad inherente a la recolección de pruebas digitales y la ausencia de evidencia contundente pueden obstaculizar la continuación de los procesos penales.

SEGUNDA

Se concluye que la falta de presupuestos materiales, como la incapacidad para individualizar al imputado o la ausencia de enmarcado del hecho denunciado como un delito, influyen directamente en la no formalización de los procesos de delitos informáticos. Es esencial contar con la identificación del presunto autor y que el acto denunciado cumpla con los requisitos legales para ser considerado un delito.

TERCERA

Se ha determinado que la insuficiencia de elementos de convicción tiene un impacto considerable en la formalización de los casos de delitos informáticos. La falta de pruebas sólidas y contundentes puede dificultar la presentación de cargos y la continuación del proceso legal.

RECOMENDACIONES

PRIMERA

El Ministerio Público debería ofrecer capacitaciones especializadas a los fiscales y personal investigador sobre métodos de recolección de pruebas digitales. Además, es necesario proporcionar recursos tecnológicos avanzados para facilitar la obtención y análisis de evidencia digital.

SEGUNDA

Establecer alianzas con entidades especializadas en delitos informáticos para fortalecer la investigación y la adquisición de conocimientos especializados en el campo digital, lo que puede ayudar en la recolección de pruebas más sólidas.

TERCERA

Implementar protocolos y procedimientos claros para la recolección, preservación y presentación de evidencia digital. Esto ayudará a garantizar la consistencia y la solidez de las pruebas presentadas en casos de delitos informáticos.

REFERENCIAS BIBLIOGRÁFICAS

- Acosta, M., Benavides, M. y García, N. (2020). *Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios*. *Revista Venezolana de gerencia*. Obtenido de <https://www.redalyc.org/journal/290/29062641023/29062641023.pdf>
- Acurio, S. (2016). Delitos Informáticos: Generalidades. Portal Web Jurídico. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
- Aldana, M. G. y Bautista, J. E. (2014). *Reglas de prueba en el proceso penal salvadoreño*. Unidad técnica Ejecutiva del Sector de Justicia. https://escuela.fgr.gob.sv/wp-content/uploads/leyes-nuevas/Libro-de-Reglas-de-Prueba.pdf?utm_source=chatgpt.com
- Bramont-Arias, L. (1997). *El delito informático en el Código penal peruano*. Editorial de la Pontificia Universidad Católica del Perú. <https://repositorio.pucp.edu.pe/index/handle/123456789/181585>
- Cabrera, M. (2020). *Fundamentos jurídicos considerados por los fiscales penales del cercado de Cajamarca para archivar las investigaciones de delitos informáticos durante el periodo 2010-2018*. [Tesis para optar el título profesional de abogada, Universidad Privada del Norte]. <https://hdl.handle.net/11537/24533>
- Chávez, W. (2010). *El Archivo Fiscal y su Aplicación en el Nuevo Código Procesal Penal* (Tomo 3). Editorial Gaceta Jurídica.
- De Diego, L. (2001). Medios de prueba en Proceso Penal. LITOCOM, S. [file:///C:/Users/Usuario/Downloads/194_%20Medios%20de%20prueba%20en%20el%20proceso%20penal%20\(1\).pdf](file:///C:/Users/Usuario/Downloads/194_%20Medios%20de%20prueba%20en%20el%20proceso%20penal%20(1).pdf)
- Fiscalía General de la Nación (2009). *Manual de Procedimientos de Fiscalía en el Sistema Penal Acusatorio Colombiano*. https://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/03/spoa.pdf?utm_source=chatgpt.com
- Huamán, M. (2020). *Los delitos informáticos en Perú y la suscripción del convenio de Budapest* [Tesis de pregrado, Universidad Andina de Cusco]. Repositorio

UANDINA.

https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/4116/Marleny_Tesis_bachiller_2020.pdf?sequence=1&isAllowed=y

Leyva, C. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. *Revista Lucerna Iuris Et Investigatio*, 1, 29-47.

<https://revistasinvestigacion.unmsm.edu.pe/index.php/Lucerna/article/view/18373>

Loredo, J. y Ramírez, A. (2013). *Delitos informáticos su clasificación y un visión general de las medidas de acción para convatirlos*. México. Obtenido de http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Maio, J. y Peralta, R. (2017). DERECHO PROCESAL PENAL. Guía de estudio 05. https://www.mseg.gba.gov.ar/areas/Vucetich/GUIAS%20DE%20MATERIAS%202021/5%20Procesal%20Penal.pdf?utm_source=chatgpt.com

Marca, J., García, M., Jiménez, A. y Ruz, P. (2021). *La prueba penal y las nuevas tecnologías*, 7ma ed. Cooperación Española, conocimiento interconecta. https://interconecta.aecid.es/Gestin%20del%20conocimiento/LA%20PRUEBA%20PENAL%20Y%20LAS%20NUEVAS%20TECNOLOG%20C3%8DAS.pdf?utm_source=chatgpt.com

Martínez, C. (2023). *Los delitos informáticos y su ineficacia en la aplicación de sanciones como consecuencia de sus vacíos jurídicos Huancayo, 2022*. [Tesis para optar el título profesional de abogado, Universidad Peruana de las Américas]. <http://repositorio.ulasamericas.edu.pe/123456789/3651>

Ministerio de Justicia y Derechos Humanos (2021). *MINJUSDH presenta estudio sobre ciberdelitos en el país y propone recomendaciones a la ciudadanía*. <https://www.gob.pe/institucion/minjus/informes-publicaciones/3396016-reporte-de-ciberdelincuencia>

Peña, A. (2011). *Derecho Penal - Parte Especial*. Editorial Idemsa.

- Ramos, K. (2020). *Factores procesales en el archivamiento de los delitos informáticos, vistos en la primera y segunda fiscalía provincial penal corporativa de Leoncio Prado, 2017 – 2018*. [Tesis para optar el título profesional de abogada, Universidad de Huánuco]. <http://repositorio.udh.edu.pe/123456789/2524>
- Rivera, F. (2021). *Prevenir los delitos informáticos en el Sistema Financiero Ecuatoriano del 2020 al 2022*. [Tesis para optar el título de abogado, Universidad de Guayaquil]. Ecuador. <http://repositorio.ug.edu.ec/handle/reduq/58070>
- San Martín, C. (2020). *Lecciones de Derecho Procesal Penal*. Editorial INPECCP y CENALES.
- Trujillo, E. (2021, marzo 01). *Acción penal*. Portal Web Economipedia. <https://economipedia.com/definiciones/accion-penal.html>
- Universidad Internacional de la Rioja (2023). *Ciberdelincuencia: ¿Qué es y cuáles son los ciberdelitos más comunes?*. <https://mexico.unir.net/ingenieria/noticias/que-es-ciberdelincuencia/>
- Villavicencio, F. (2014). *Delitos Informáticos*. Editorial IUS ET VERITAS
- Ventocilla, G. (2023). *Vulneración del derecho de motivación en las disposiciones de no formalización ni continuación de la investigación preparatoria, Sexta Fiscalía Penal Corporativa de Huánuco, 2019 – 2020* [Tesis de pregrado, Universidad de Huánuco]. Repositorio Institucional UDH. <https://repositorio.udh.edu.pe/handle/20.500.14257/4099>

ANEXOS

ANEXO 1

INSTRUMENTOS DE RECOLECCIÓN DE DATOS

CARPETAS



0060605450320220003880000

Ministerio Público
03°FPPC-CARABAYLLO(NCPP)
SGF

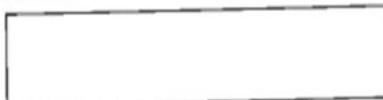
CARGO DE INGRESO DE CARPETA FISCAL

3°FPC-CARABAYLLO 1°DESPACHO - 1°DESPACHO: DESPACHO 1, 3 FPC CARABAYLLO

CASO : 606054503-2022-388-0 **DEPENDENCIA** : 03°FPPC-CARABAYLLO(NCPP)
ESPECIALIDAD : PENAL **DISTRITO FISCAL** : LIMA NORTE
F. INGRESO : 20/04/2022 17:53
MOTIVO INGRESO : INFORME POLICIAL **NRO. FOLIOS** : 3
INFORME POLICIAL :
NUMERO DE OFICIO : 1796-2022-REG.POL-LIMA/DIVPOL NORTE1-CEP-SEINPOL
OBSERVACIONES : COMISARIA PROGRESO

DELITO(S) :
FRAUDE INFORMATICO

INVESTIGADO : L.Q.R.R.
DENUNCIANTE : MORALES URRUTIA JOSE ANTONIO



Recibido



MINISTERIO PÚBLICO



12/12/2022

3.17 PM

N° CASO : 506014504-2022-3059-0

DISTRITO FISCAL : DISTRITO FISCAL DE LIMA
FISCALÍA : 5to Despacho-CUARTA FISCALÍA CORPORATIVA PENAL DE CERCADO DE LIMA-BREÑA-RÍMAC-JESÚS MARÍA
FECHA INGRESO : 12/12/2022 15:19:00
CUADERNO : PRINCIPAL

REMITENTE : HECTOR TITO QUISPE ARIAS
TIPO : PNP - DIVINDAT/DIRINCRI
DELITO (S) : Delitos Informáticos
DENUNCIANTE (S) : ALICIA DOLORES CABEZUDO HIDALGO
AGRAVIADO (S) : ALI HOUSE SAC
DENUNCIADO (S) : LQRR
N° DE INFORME POLICIAL : OFICIO NRO. 10935-2022-DIRINCRI PNP/DIVINDAT-DEPIDI2-E1
ANEXO : 1
N° FOLIOS : 7
OBSERVACIONES :



apertura
Julio

Ministerio Público
03°FPPC-CARABAYLLO(NCPP)
SGF

CARGO DE INGRESO DE CARPETA FISCAL

3°FPC-CARABAYLLO 1°DESPACHO - 1°DESPACHO: DESPACHO 1, 3 FPC CARABAYLLO

CASO : 606054503-2023-1057-0 **DEPENDENCIA** : 03°FPPC-CARABAYLLO(NCPP)
ESPECIALIDAD : PENAL **DISTRITO FISCAL** : LIMA NORTE
F. INGRESO : 12/07/2023 10:33
MOTIVO INGRESO : INFORME **NRO. FOLIOS** : 8
INFORME POLICIAL : .
NUMERO DE OFICIO : 3383-2023 REG POL LIMA DIVPOL NORTE 1 DEPINCRI CARABAYLLO
OBSERVACIONES : DEPINCRI CARABAYLLO. N° DE ORDEN 26856453. DENUNCIA DIRECTA N° 347. FORMATO DIGITAL.

DELITO(S) :

ESTAFA

DENUNCIADO : LANDAETA ACOSTA DAMARIS
DENUNCIADO : SUDARIO ESPINOZA MARIANA DE LOS ANGELES
AGRAVIADO : MEZA MAYS CARMEN MILAGROS

CASOS RELACIONADOS CON LAS PARTES

CASO	FE. HECHO	APELLIDOS Y NOMBRES	TIPO DE PARTE	DOC. IDENT.	OBSERVACION
MEZA MAYS, CARMEN MILAGROS					
606010102-2012-516-0	16/08/12	MEZA MAYS, CARMEN MILAGROS	AGRAVIADO	S.D.	
606014509-2018-1470-0	07/07/17	MEZA MAYS, CARMEN MILAGROS	AGRAVIADO	DNI 44322866	
606054501-2021-440-0	18/09/21	MEZA MAYS, CARMEN MILAGROS	AGRAVIADO	DNI 44322866	
606054501-2021-443-0	16/09/21	MEZA MAYS, CARMEN MILAGROS	AGRAVIADO		

SUDARIO ESPINOZA MARIANA DE LOS ANGELES



Ministerio Público
03°FPPC-CARABAYLLO(NCPP)
SGF

CARGO DE INGRESO DE CARPETA FISCAL

3°FPPC-CARABAYLLO 2° DESPACHO - 2° DESPACHO: HUACACHI ZANZI, ERIKA BEATRIZ

CASO : 606054503-2021-2228-0 **DEPENDENCIA** : 03°FPPC-CARABAYLLO(NCPP)
ESPECIALIDAD : PENAL **DISTRITO FISCAL** : LIMA NORTE
F. INGRESO : 28/11/2021 13:03
MOTIVO INGRESO : INFORME POLICIAL **NRO. FOLIOS** :
INFORME POLICIAL : .
NUMERO DE OFICIO : .
OBSERVACIONES : TURNO SEMANA DEL 22 AL 29 DE NOVIEMBRE

DELITO(S):

BANDA CRIMINAL

IMPUTADO : DIAZ MONTENEGRO KEVIN SLEE **CONDICION:3**
IMPUTADO : FERNANDEZ SALINAS JOSIAS ESTEBAN **CONDICION:3**
AGRAVIADO : LA SOCIEDAD



G



006060545032022000690000

Ministerio Público
03°FPPC-CARABAYLLO(NCPP)
SGF

CARGO DE INGRESO DE CARPETA FISCAL

3°FPC-CARABAYLLO 1°DESPACHO - 1°DESPACHO: DESPACHO 1, 3 FPC CARABAYLLO

CASO : 606054503-2022-690-0 DEPENDENCIA : 03°FPPC-CARABAYLLO(NCPP)
ESPECIALIDAD : PENAL DISTRITO FISCAL : LIMA NORTE
F. INGRESO : 23/06/2022 09:35
MOTIVO INGRESO : INFORME NRO. FOLIOS : 2
INFORME POLICIAL :
NUMERO DE OFICIO : 767-2022 REG POL LIMA DIVPOL NORTE 1 CEP SEINPOL
OBSERVACIONES : COMISARIA EL PROGRESO



DELITO(S) :
ESTAFA
INVESTIGADO : L.Q.R.R.
AGRAVIADO : ALONSO RONQUILLO GENRY LUIS



Recibido





0060605450320220010500000

Ministerio Público
03°FPPC-CARABAYLLO(NCPP)
SGF

CARGO DE INGRESO DE CARPETA FISCAL

3°FPC-CARABAYLLO 1°DESPACHO - 1°DESPACHO: DESPACHO 1, 3 FPC CARABAYLLO

CASO : 606054503-2022-1050-0 DEPENDENCIA : 03°FPPC-CARABAYLLO(NCPP)

ESPECIALIDAD : PENAL DISTRITO FISCAL : LIMA NORTE

F. INGRESO : 17/08/2022 09:48

MOTIVO INGRESO : INFORME NRO. FOLIOS : 22

INFORME POLICIAL :

NUMERO DE OFICIO : 4098-2022-REG-POL-LIMA/DIVPOL-N-1/CEP-SEINCRI

OBSERVACIONES : DENUNCIA 1609
OCURRENCIA 23957487

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN
1° DESPACHO 3ra Fiscalía Provincial
Penal Corporativa de Carabaylo
Distrito Fiscal de Lima Norte

17 AGO 2022

RECIBIDO

Hora: 10:45 Firma: [Firma]

Folios: 22

DELITO(S) :

ESTAFA

INVESTIGADO : L.Q.R.R.

AGRAVIADO : SALAS ZULUAGA MARGARITA NANCY

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN

Recibido por Mesa de Partes Virtual.



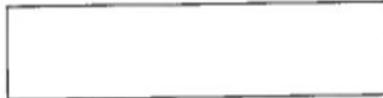
03°FPPC-CARABAYLLO(NCPP)
SGF

CARGO DE INGRESO DE CARPETA FISCAL

3°FPC-CARABAYLLO 1°DESPACHO - 1°DESPACHO: DESPACHO 1, 3 FPC CARABAYLLO

CASO	: 606054503-2023-398-0	DEPENDENCIA	: 03°FPPC-CARABAYLLO(NCPP)
ESPECIALIDAD	: PENAL	DISTRITO FISCAL	: LIMA NORTE
F. INGRESO	: 16/03/2023 12:08		
MOTIVO INGRESO	: INFORME	NRO. FOLIOS	: 7
INFORME POLICIAL	: -		
NUMERO DE OFICIO	: 1078-2023-REG-POL-LIMA/DIVPOL-N-1-CSI-SEINCRI		
OBSERVACIONES	: DENUNCIA VIRTUAL		

DELITO(S) :	FRAUDE INFORMATICO
INVESTIGADO :	L.Q.R.R.
AGRAVIADO :	BERNAL SARAVIA CRISTHIAN EDWIN



Recibido



CARGO DE INGRESO DE CARPETA FISCAL

3°FPC-CARABAYLLO 1°DESPACHO - 1°DESPACHO: DESPACHO 1, 3 FPC CARABAYLLO

CASO : 606054503-2023-992-0 DEPENDENCIA : 03°FPPC-CARABAYLLO(NCPP)

ESPECIALIDAD : PENAL DISTRITO FISCAL : LIMA NORTE

F. INGRESO : 03/07/2023 16:08

MOTIVO INGRESO : INFORME NRO. FOLIOS : 7

INFORME POLICIAL : .

NUMERO DE OFICIO : 4683-2023-REG POL-LIMA/DIVPOL-N-1/CEP-SEINCRI

OBSERVACIONES : RECIBIDO VIRTUALMENTE

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN

1° DESPACHO 3ra Fiscalía Provincial
Penal Corporativa de Carabaylo
Distrito Fiscal De Lima Norte

03 JUL 2023

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN

Recibido por Mesa de Partes Virtual.
mp.1d.3fppc.carabaylo@mpln.gob.pe

RECIBIDO

Hora: 16:17 Firma:
Folios: 07

DELITO(S) :

FRAUDE INFORMATICO

INVESTIGADO : L.Q.R.R.

AGRAVIADO : CASTILLO ACEVEDO LEONARDO

ANEXO 02

UNIVERSIDAD NACIONAL “DANIEL ALCIDES CARRIÓN”, FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS, ESCUELA DE FORMACIÓN PROFESIONAL DE DERECHO
TESIS: FACTORES QUE DETERMINAN LA NO FORMALIZACIÓN DE LOS DELITOS INFORMÁTICOS EN LA TERCERA FISCALÍA PROVINCIAL PENAL CORPORATIVA DE CARABAYLLO EN EL DISTRITO FISCAL DE LIMA NORTE, 2022.

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	METODOLOGÍA
<p>Problema General ¿Cuáles son aquellos factores que determinarán la no formalización de los delitos informáticos en la Tercera fiscalía provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022?</p> <p>Problemas Específicos PE1: ¿De qué manera la falta de presupuestos materiales determinará la no formalización de los procesos de delitos informáticos en la Tercera fiscalía provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022? PE2: ¿En qué nivel la insuficiencia de elementos de convicción afecta en la formalización de los procesos de delitos informáticos en la Tercera fiscalía provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022?</p>	<p>Objetivo General Determinar qué factores son los que intervienen en la no formalización de los delitos informáticos en la Tercera fiscalía provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022.</p> <p>Objetivos Específicos OE1: Analizar de qué manera la falta de presupuestos materiales determinarán la no formalización de los procesos de delitos informáticos en la Tercera fiscalía provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022. OE2: Determinar el nivel en el que la insuficiencia de elementos de convicción afecta en la formalización de los procesos de delitos informáticos en la Tercera fiscalía provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022.</p>	<p>Hipótesis General Provincial Penal Corporativa de Carabayllo en el Distrito Los factores que intervienen en la no formalización de los delitos informáticos en la Tercera Fiscalía Fiscal de Lima Norte, 2022 son la falta de medios probatorios recabados en las diligencias de investigación.</p> <p>Hipótesis Específicas HE₁: La falta de presupuestos materiales determinará la no formalización de los procesos de delitos informáticos en los casos donde no se haya logrado individualizar al imputado, así como también en los casos donde el hecho denunciado no logre ser encuadrado en el tipo penal como delito. HE₂: Se determinó que la insuficiencia de elementos de convicción afecta en un nivel considerablemente alto en la formalización de los procesos de delitos informáticos en la Tercera fiscalía provincial Penal Corporativa de Carabayllo en el Distrito Fiscal de Lima Norte, 2022.</p>	<p>Identificación de variables Variable 1: No formalización de la Acción Penal. Variable 2: Delitos informáticos. Definición conceptual de la no formalización de la acción penal Es el instrumento en derecho que debe ejercitarse para iniciar un proceso judicial en la jurisdicción penal (Trujillo, 2021). Definición conceptual de los delitos informáticos Se define a delito informático como aquel que se da con la ayuda de la informática o de técnicas anexas (Acurio, 2016, p.10).</p>	<p>Variable 1: ✓ Presupuestos materiales. ✓ Insuficientes elementos de convicción. Variable 2: ✓ Daño a la información (borrar, dañar o alterar). ✓ Violación del derecho a la intimidad y privacidad.</p>	<p>Presupuestos materiales: • Que el hecho constituya delito. • Individualización del autor. Insuficientes elementos de convicción • Falta de pruebas que evidencien el hecho. • No hay declaración del imputado ni de testigos. Daño a la información (borrar, dañar o alterar) • Fraude electrónico. • Robo de bancos. Violación del derecho a la intimidad y privacidad • Violación a los derechos de autor. • Pornografía infantil.</p>	<p>Tipo de investigación: Tipo aplicado. Nivel de investigación: Descriptivo - exploratorio. Enfoque: Cualitativo. Diseño: No experimental – descriptivo. Corte: Transversal. Método: Analítico y crítico. Análisis: Análisis documental.</p>