

**UNIVERSIDAD SAN PEDRO**

**FACULTAD DE DERECHO Y CIENCIA POLITICA**

**PROGRAMA DE ESTUDIO DE DERECHO**



**Actos de investigación y tratamiento normativo en los delitos de fraude informático, Distrito Fiscal de Lima Sur, 2021**

Tesis para optar el Título Profesional de abogada

**Autor:**

**Tacuche Rodriguez, Shirley Carolina**

**Asesor – 0000-0003-3965-5904**

**Urcia Quispe, Manuel Ulises**

**HUACHO - PERÚ**

**2022**

**PALABRAS CLAVE:**

<b>Tema</b>	Fraude
<b>Especialidad</b>	Derecho

**KEYWORDS:**

<b>Theme</b>	Fraud
<b>SPECIALITY</b>	Laws

**LÍNEA DE INVESTIGACIÓN – OCDE:**

<b>Línea de Investigación</b>	Instituciones fundamentales del derecho penal
<b>Área</b>	Ciencias Sociales
<b>Subarea</b>	Derecho
<b>Disciplina</b>	Derecho

ACTOS DE INVESTIGACIÓN Y TRATAMIENTO NORMATIVO EN LOS  
DELITOS DE FRAUDE INFORMÁTICO, DISTRITO FISCAL DE LIMA SUR, 2021

## RESUMEN

El objetivo de la investigación que se realizó fue determinar si son suficientes los actos de investigación dispuestos para esclarecer las denuncias realizadas por el delito de fraude informático en el Distrito Fiscal de Lima Sur, año 2021. Objetivo que se logró alcanzar mediante el análisis de los aspectos normativos de su regulación a nivel internacional y nacional sobre el delito de fraude informático y sus actos de investigación llevados a cabo, se analizó la legislación comparada en la materia y los datos estadísticos de casos o carpetas referente a las denuncias formuladas por el delito de fraude informático en el Distrito objeto de estudio.

La metodología adoptada en esta investigación fue de tipo descriptivo y diseño no experimental. El instrumento empleado fue el análisis documental y el cuestionario realizado a los especialistas en la materia. De los resultados se logró determinar que las investigaciones efectuadas durante las diligencias iniciales no son suficientes para el esclarecimiento e identificación de las personas responsables por las denuncias de los delitos de fraude informático en el Distrito Fiscal objeto de estudio, siendo necesaria una serie de medidas a fin de reducir la impunidad, como la capacitación especializada de los principales actores intervinientes y persecutores, la implementación a nivel nacional de fiscalías especializadas descentralizadas, una regulación más clara, precisa sobre la materia y unificar medidas de cooperación entre Estados.

## **ABSTRACT**

The objective of the investigation that was carried out was to determine if the acts of investigation arranged to clarify the complaints made for the crime of computer fraud in the Fiscal District of Lima Sur, year 2021, are sufficient. Objective that was achieved through the analysis of the normative aspects of its regulation at the international and national level on the crime of computer fraud and its investigative acts carried out, the comparative legislation on the matter and the statistical data of cases or folders referring to the complaints made for the crime of computer fraud in the District under study.

The methodology adopted in this research was descriptive and non-experimental design. The instrument used was the documentary analysis and the questionnaire made to the specialists in the matter. From the results it was possible to determine that the investigations carried out during the initial proceedings are not sufficient for the clarification and identification of the persons responsible for the denunciations of the crimes of computer fraud in the Fiscal District under study, being necessary a series of measures to in order to reduce impunity, such as the specialized training of the main intervening actors and persecutors, the implementation at the national level of decentralized specialized prosecutors, a clearer, more precise regulation on the matter and unifying cooperation measures between States.

## INDICE

Palabras Clave.....	i
Título .....	ii
Resumen .....	iii
Abstract .....	iv
Índice .....	v
1. INTRODUCCIÓN	
1.1 Antecedentes y Fundamentación .....	1
1.2 Justificación de la investigación .....	9
1.3 Problema .....	10
1.4 Conceptualización y Operacionalización de las variables .....	11
A. Actos de Investigación .....	12
Concepto .....	12
Objeto de investigación.....	15
Rol de la PNP en los actos de investigación .....	16
Rol del Ministerio Público en los actos de investigación .....	18
La prueba y las nuevas tecnologías .....	20
B. Delito de Fraude Informático.....	23
Características.....	26
Tratamiento normativo.....	28
1.5 Hipótesis .....	30
1.6 Objetivos.....	30
2. METODOLOGIA	
2.1 Tipo de investigación .....	31
2.2 Población y muestra.....	32
2.3 Técnicas e instrumentos de investigación .....	32

3. RESULTADOS	
3.1 Descripción de los Resultados de la Técnica: Análisis Documental.....	33
3.2 Descripción de Resultados de la Técnica: Encuesta .....	45
4. ANÁLISIS Y DISCUSIÓN.....	60
5. CONCLUSIONES Y RECOMENDACIONES .....	71
6. AGRADECIMIENTOS.....	75
7. REFERENCIAS BIBLIOGRAFICAS .....	76
8. ANEXOS Y APÉNDICES .....	80

# **I. INTRODUCCIÓN**

## **1.1 Antecedentes y fundamentación del problema**

### **Antecedentes Internacionales:**

A nivel internacional, se encontraron los estudios desarrollados por:

Hidalgo (2018) en su trabajo para su titulación los delitos informáticos y su afectación sobre los bienes jurídicos presentado en la Universidad Católica de Santiago de Guayaquil-Ecuador, su objetivo de investigación fue comprobar la afectación de los delitos informáticos sobre los bienes jurídicos analizando el estado actual de las legislaciones penales no solo ecuatoriana sino también extranjera a fin de determinar si existe entre otros armonización entre las mismas legislaciones, estudio descriptivo no experimental y transversal, el autor concluyó que si bien el surgimiento de la tecnología y su evolución en nuestras vidas nos ha beneficiado en distintos aspectos haciendo ella más simple, practica y además dinámica, sin embargo resulta preocupante su regulación desde el punto de vista penal, no solo en Ecuador, sino a nivel global, resultando necesaria que la regulación sea armonizada en materia a fin de frenar los efectos negativos. Por otro lado, sostuvo también que es importante modificar los enfoques penales a fin de evitar que se deje en el abandono el problema social que generan dichos delitos, considerándolos como verdaderos peligros y vulneración de bienes jurídicos, favoreciendo su tipificación en el ordenamiento jurídico interno, el poder ingresar a un sistema sin contar con autorización implicaría la pérdida de confianza en los sistemas de seguridad de las entidades.

Iggstrom (2018) en su trabajo realizado para obtener el diplomado académico en Auditoria Forense, cuyo título es propuesta de reglamento a la obtención de pruebas periciales por peritos informáticos dentro la auditoría forense en Bolivia presentado en la Universidad Mayor de San Andrés de Bolivia, tuvo como propósito el determinar la importancia de la implementación de un reglamento durante el procedimiento a la obtención de la prueba informática mediante el trabajo del perito

auditor al interior de los procesos penales bolivianos, para ello el autor utilizó fuentes primarias, secundarias y terciarias, siendo estas consultas directas a profesionales del área, trabajos doctrinales de auditoría forense y de revistas de Derecho electrónico en internet; estudio de tipo explorativo y diseño no experimental, llegando a las siguientes conclusiones, en el ordenamiento jurídico Boliviano los delitos informáticos entraron en vigor mediante la Ley N° 1768 que tipifica la manipulación, ingreso y modificación o uso inapropiado de información almacenada en el sistema informático, resultando indispensable el trabajo que realizan los peritos en la materia a fin de que puedan coadyuvar a la correcta aplicación y emisión de una sentencia al interior de un proceso. Para ello, el auditor forense informático al momento de la emisión de un dictamen requiere de elementos de prueba que sean suficientes, relevantes y también oportunos, incluyendo toda aquella prueba que se haya podido obtener dentro del ámbito informático, para ello se necesita de la implementación de un Reglamento que oriente sobre el recaudo de elementos de prueba vitales para la demostración de los hechos, de la misma forma resulta indispensable contar con personal capacitado y calificado en la materia.

#### **Antecedentes Nacionales:**

Carrera (2021) en su tesis denominada deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021 presentado en la Escuela de Postgrado de la Universidad C. Vallejo, investigación que se realizó en el Distrito Fiscal de Lima, cuyo objetivo fue el evidenciar las deficiencias encontradas en el marco de las investigaciones por el delito de fraude informático en el distrito mencionado, el método fue no experimental, enfoque cualitativo-básico, para ello se entrevistó al fiscal adjunto provincial, a los asistentes en función fiscal y a conocedores del derecho, llegando a las siguientes conclusiones, falta de capacitación adecuada y especializada de los principales intervinientes, la Policía Nacional, Ministerio Público y DIVINDAT, por otro lado menciona la falta de actualización de la normativa en materia, no habiéndose al día de hoy incorporado nuevas modalidades

delictivas acordes con la realidad, no teniéndose en cuenta tampoco los grandes avances tecnológicos, lo que genera que se lleven a cabo investigaciones muy deficientes en la persecución de estos delitos. Además, considera el tesista que la Ley 30096 sobre los delitos informáticos debe contemplar más artículos que involucren una mejor ciberseguridad, de manera que se puedan identificar plenamente a los autores de estos ilícitos; indica también que una de las causas a la deficiente investigación es debido a la falta de coordinación adecuada entre PNP Y MP.

Custodio (2021) en su tesis las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático presentado a la Escuela Profesional de Derecho de la Universidad C. Vallejo, cuya finalidad fue determinar si corresponde incluir las nuevas modalidades delictivas de cibercrímenes en la ley especial N° 30096; la investigación es de diseño cuantitativo y de tipo descriptivo, para ello se realizó un cuestionario a una población conformada por cinco magistrados especialistas en materia penal, cinco representantes del Ministerio Público y sesenta conocedores del derecho, especialistas en materia penal llegando a las siguientes conclusiones, la tecnología nos ha servido para reducir distancias, así como ha resultado de gran utilidad para la realización de actividades académicas y laborales, sin embargo dichos beneficios han sido también aprovechados por los ciberdelincuentes, quienes han hecho surgir nuevos ilícitos penales, cuyo actuar busca captar a víctimas a través del uso de la tecnología perjudicándolas económicamente, sobresaliendo entre los principales ilícitos penales, el fraude informático, siendo el que tiene mayor incidencia en los últimos años; se debería incluir las nuevas modalidades delictivas en la Ley Especial, a fin de que no se genere confusión en los procesos penales y no queden impune estas denuncias, la normatividad debe ir de la mano con el avance tecnológico y las nuevas formas de delinquir de los ciberdelincuentes, como lo viene haciendo ya el vecino país Colombia. En el código penal de Argentina se han tipificado los delitos informáticos se encuentran en el apartado de los delitos comunes, dotando de esta forma de mayor protección y brindando seguridad jurídica en materia.

Montalvo (2020) en su tesis la investigación del delito de Estafa y su archivamiento en el Ministerio Público sede Lima, 2018 presentado ante la Universidad C. Vallejo para optar el título de abogado, cuya finalidad fue el determinar de qué forma las investigaciones realizadas por el delito de Estafa han conllevado a un archivamiento de las mismas en la sede del Ministerio Público de Lima, en el año 2018, la metodología adoptada fue la de recolección de información recabada de las entrevistas que se realizaron a personal administrativo y fiscal de la Fiscalía, en ese mismo sentido se obtuvo información de la guía de análisis documental recabada durante el proceso de elaboración del presente trabajo, el autor determinó concluyendo que el actuar por parte de la fiscalía en términos de estrategias de investigación que lleva a cabo a fin de investigar los delitos de estafa, son limitados, siendo en ciertos casos necesario la identificación y ubicación de las personas que hacen uso de las tecnologías para la comunicación, a través de los requerimientos a los órganos jurisdiccionales correspondientes, encargados de las medidas limitativas de derechos sobre el levantamiento del secreto de las comunicaciones que permitan identificar las personas involucradas, no siendo la Ley N° 30096 favorable para el delito de Estafa mediante dichos actos de investigación; así también se arriba a la conclusión de que respecto a los delitos de estafa son archivados de manera liminar; y se ha demostrado también que las denuncias han sido archivadas al no haberse podido requerir o bien obtener una resolución favorable respecto a las solicitudes del Levantamiento del Secreto de las Comunicaciones.

Ccori (2020) en su tesis de maestría implicancias Jurídicas del Fraude Informático y la Protección Penal del Delito Contra el Patrimonio Distrito Fiscal de Lima Norte 2020 sustentada ante la Universidad C. Vallejo, cuya finalidad fue determinar la protección que se brindó frente a los del delito en el D.F. de Lima Norte en el año 2020 y su connotación jurídica; respecto a la metodología la investigación es de tipo cualitativa, de nivel descriptivo y de tipo no experimental, se recolecto información mediante de las entrevistas realizadas a integrantes de la Fiscalía, Magistrados especializados en materia penal y otros operadores judiciales, así también se obtuvo información de fuente documentada, artículos científicos nacional e internacional, el

autor arribó a las siguientes conclusiones, se concluye inicialmente que las sanciones previstas para la comisión de estos delitos no logran ser efectivas, debido a que hay cierta complejidad en el modus operandi empleado por los autores, situación que genera dificultades de persecución, amparados en normas penales confusas. Así también sostiene que el efecto negativo de la comisión del delito de fraude informático repercute no solo en los agraviados directo del ilícito sino también en perjuicio del Estado. El accionar del ciberdelincuente genera grandes pérdidas económicas.

Pardo (2018) en su tesis de maestría tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018 presentado en la Universidad Cesar Vallejo, cuyo objetivo fue el de analizar el aspecto normativo de los delitos informáticos en el D.F. de Lima en el año 2018, la metodología empleada fue la de recolección de datos mediante las entrevistas realizadas y cuyo instrumento fue la guía de entrevista, mediante el que se recogió información valiosa de los conocedores del tema tanto a nivel local como a nivel internacional. El autor concluye que es deficiente el tratamiento normativo en los delitos de fraude informático, ello debido a que al interior del delito de fraude informático se incluyen otras modalidades de delitos, situación que genera incertidumbre jurídica y como consecuencia impunidad en la comisión de estos delitos, de la misma forma el delito informático en su modalidad de hurto también es deficiente, en esta modalidad nuestra legislación no contempla de manera expresa esta modalidad por lo que dicha laguna legal acarrea múltiples dificultades durante su investigación. Lo mismo sucede con el delito informático en su modalidad de estafa, no existe de forma expresa este ilícito penal.

### **Fundamentación del Problema:**

Los medios tecnológicos constituyen una herramienta significativa, de gran interés y cada vez de mayor uso en nuestra sociedad y a nivel mundial, cuyo beneficio es dar mayor facilidad y rapidez en distintas actividades cotidianas, simplificándonos la vida.

En los últimos años, de la mano con el progreso de la tecnología, las nuevas formas de criminalidad han aprovechado haciendo uso de estas herramientas informáticas para delinquir.

Los Cibercrimenes son aquellas conductas que tienen como finalidad cometer delitos a través del uso de herramientas informáticas, vulnerando la información y contenido de un sistema informático.

Frente a estas nuevas formas de criminalidad, distintas a los delitos ordinarios o comunes los Estados dieron respuesta mediante el Convenio sobre la Ciberdelincuencia suscrito en la ciudad de Budapest el día 23 de noviembre de 2001, destinado inicialmente para los países europeos, posteriormente se fueron adhiriendo los demás Estados no pertenecientes a Europa, Convenio que entro en vigencia el 1 de julio del año 2004; en el Perú también fue aprobado, ratificado y entró finalmente en vigencia el del 01 de diciembre de 2019.

El interés en cuanto a su regulación interna se manifestó mediante la Ley N° 30096 “Ley de Delitos Informáticos” y la Ley N° 30171, denominados así en tanto son cometidos por medios informáticos, siendo el bien jurídico afectado la información, en lo específico la presente investigación se va a centrar en el delito de Fraude informático, ubicado en el art. 8 de la Ley mencionada.

No obstante, los esfuerzos de la legislación actual nacional, no resultaron suficiente para hacer frente a estos delitos que perjudican siempre a una cantidad mayor del eslabón más vulnerable de la cadena de seguridad, los usuarios.

Entre las principales causas que debilitaron la eficacia de la presente la Ley tenemos fueron el no contar con un reglamento que pueda materializar las disposiciones de la Ley especial, tampoco se tiene una orientación o definición

respecto a las terminologías que se emplean en estos delitos particulares, resultando necesario por su particularidad y distinción respecto a los delitos comunes. El tratamiento jurídico penal del delito de fraude informático es insuficiente, comprendiéndose en el mismo tipo penal distintas modalidades delictivas, lo que genera confusión al momento de interpretar la norma, no permitiendo una sanción efectiva, en la Ley Especial tampoco se hace mención a técnicas especiales de investigación, siendo ello necesario al tratarse de delitos que revisten cierta complejidad.

Las causas a una deficiente persecución de estos delitos son múltiples, entre las más resaltantes que se generaron durante las investigaciones a nivel de fiscalía son: la ausencia de fiscalías en cibercrimenes en todo el Perú, inexistencia de instrumentos adecuados, ausencia de actos de investigación o formas de investigación obsoletas, falta de capacitación a los fiscales, la policía especializada no se abastece, la investigación resulta ser más complicada al cometerse estos delitos en el extranjero, la existencia de paraísos para la delincuencia informática, países como Nicaragua, Guatemala, Bolivia, quienes no tienen una regulación en materia de delitos informáticos favorecen el incremento e impunidad, además por la naturaleza de estos delitos es compleja la obtención de las pruebas, en estos casos trataríamos con pruebas digitales pudiendo ser fuente de pruebas, una laptop, un celular, un USB.

Según las estadísticas elaboradas por la Oficina de Racionalización y Estadística, que obtuvo información de los sistemas de apoyo al trabajo Fiscal (SIATF y SGF) sostuvo que durante el año 2018, de enero a noviembre se presentaron 3,851 delitos informáticos, representando el 0.47% del total de delitos cometidos a nivel nacional, de la misma forma del análisis del periodo entre enero y noviembre de 2019 los delitos informáticos representaron un total de 6,906, siendo el 0.71% del total de los delitos cometidos en dicho periodo, siendo superior en un 79.33% respecto al registro que se realizó en el mismo periodo el año anterior. Además, en el mes de noviembre de 2019 el delito informático con mayor incidencia fueron los delitos

contra el patrimonio, con un total de 2,641 casos, constituyendo el 38.24% del total de los delitos informáticos. Por lo que se puede fácilmente advertir que estos delitos en los últimos años se encuentran notablemente en aumento.

De la misma forma fue oportuno el análisis respecto a la cifra negra muy elevada de estos delitos, que comprende la ausencia de denuncia de los afectados; deben considerarse también aquellos casos en que si bien las mismas entidades a quienes se le ha vulnerado su sistema de seguridad toman conocimiento de los hechos, sin embargo estas no revelan las cifras exactas de sus clientes afectados, alegándose un tema de imagen y protección, en tanto que podría generarse un pánico en sus clientes el saber que sus medidas de protección son vulneradas, en ciertos casos con facilidad y frecuencia.

Por tales motivos, resultó indispensable dar pronta solución a la deficiente regulación en la materia e identificar los actos de investigación indispensables en las investigaciones de los delitos de fraude informático durante las diligencias preliminares, teniendo en cuenta además que los problemas generados a nivel de investigación truncan las siguientes etapas del proceso penal, en efecto, el artículo 336 del NCPP establece los requisitos para formalizar y continuar con la investigación preparatoria. Primero que el hecho investigado tenga connotación penal, segundo que el hecho investigado no haya prescrito y tercero que se haya identificado al autor del ilícito, esta última condición es la que resulta muy dificultosa de cumplir en la mayor parte de casos, por la misma complejidad y naturaleza de los delitos informáticos, que trae hoy como consecuencia que los casos, en su mayoría, en el Distrito Fiscal de Lima sur concluyan en un archivo, realidad que en los próximos años continuara incrementando de manera exponencial, generando impunidad y perjudicando cada vez más a las personas, familias e inclusive al propio Estado, siendo que hoy en día todos hacen uso de la herramienta tecnológica con el fin de simplificar sus actividades cotidianas.

## **1.2 Justificación de la investigación**

Los delitos de fraude informático están al orden del día y han incrementado cada año de manera exponencial, habiéndose cada vez más familias peruanas perjudicadas por un sistema de seguridad bancario vulnerable, por una deficiente investigación y por una normatividad especial incompleta. En ese sentido no se puede ser ajeno a uno de los tantos problemas que enfrenta hoy en día nuestra sociedad, me refiero a las cuantiosas pérdidas económicas de las familias peruanas por un sistema de seguridad de las entidades bancarias vulnerables y por un órgano estatal con serias dificultades para la averiguación, persecución y erradicación de los delitos de fraude informático.

Fue fundamental que se realice un análisis de lo que es palpable y se observa hoy, en cuanto a las estadísticas proporcionadas por la ORACE denotó claramente el aumento de denuncias, así también resultó ser una realidad de las fiscalías del distrito fiscal de Lima Sur, donde las denuncias por falta de una debida investigación acorde a la realidad de estos delitos incrementaron el número de los archivos, generando gran impunidad para los usuarios que decidieron creer en los sistemas financieros de las entidades bancarias y que al no haber contratado seguro alguno se le responsabilizó por aquellas pérdidas, generadas claramente por los así llamados “crackers”.

Estos delitos de particular complejidad debieron ser investigados de manera distinta a los delitos comunes y la ley especial vigente reglamentada llenando aquellos vacíos que se han encontrado en la misma, de manera que se puedan llevar a cabo verdaderas y propias investigaciones acordes a la complejidad y en búsqueda de la prueba digital para que todas aquellas denuncias no queden impunes y disminuya considerablemente la cantidad de denuncias que son archivadas.

La investigación se llevó a cabo con el fin de verificar cuales eran los actos de investigación que se disponían realizarse durante las diligencias preliminares y si estas eran lo suficientemente exhaustivas para hacer frente a estos delitos, así también se

buscó analizar la confiabilidad de la normas emitidas respecto al delito de fraude informático, la norma actual, la Ley N° 30096 y la N° 30171, esta última modifica la Ley primigenia, sin embargo adolece de un Reglamento, así también existe el tipo penal de Fraude Informático, donde incorporan más tipos penales, por lo que amerita la positivización de una norma acorde a la realidad y complejidad de estos delitos adoptando métodos más adecuados y técnicas especializadas durante la investigación, en ese sentido el aporte al derecho es evidente porque se busca de raíz la solución al problema jurídico y procedimental en la persecución delictiva.

### **1.3 Problema**

En consecuencia, el problema es el que a continuación se formula:

¿Los actos de investigación llevados a cabo durante las diligencias preliminares son suficientes para el esclarecimiento de los delitos de fraude informático en el Distrito Fiscal de Lima Sur, durante el año 2021?

#### 1.4 Conceptualización y operacionalización de las variables:

Variables	Definición Conceptual	Dimensiones	Indicadores	Instrumento	Tipo de Escala de Medición
<b>ACTOS DE INVESTIGACIÓN</b>	Las diligencias preliminares son la etapa inicial de toda investigación donde Policía Nacional y Ministerio Público, trabajan de manera coordinada para llevar a cabo los actos de naturaleza urgente e indispensables, a fin de asegurar el material probatorio necesarios y oportuno e identificar a los presuntos responsables como a los hechos materia de investigación.	Definición conceptual	Concepto de actos de investigación	Análisis documental.	Nominal
			Concepto de diligencias preliminares		
		Disposición Fiscal	Actos urgentes e inaplazables	Encuesta	
			Diligencias a realizarse		
Elementos de convicción	Diligencias preliminares	- Declaraciones - Prueba Digital			
<b>DELITO DE FRAUDE INFORMATICO</b>	Delito que tiene mayor incidencia respecto a los demás delitos informáticos, la conducta reprochable se traduce en la obtención ilícita de datos, información, mediante el uso de la herramienta informática para el aprovechamiento propio o de terceros.	Tratamiento Normativo	Ley N° 30096, y la Ley N° 30171, Ley que modifica la Ley de delitos informáticos, ubicado en el art. 8 de la Ley.	Análisis documental Encuesta	Nominal
		Modalidades	Introducción, alteración de datos informáticos	Análisis documental	Nominal
			Borrado o Supresión de datos informáticos.	Encuesta	
		Clonación de datos informáticos.			

## **1.5 Conceptuación y operacionalización de las variables**

### **A.- Actos de investigación**

#### **Concepto**

Son considerados aquellos actos primigenios realizados por disposición fiscal con apoyo de la policía con la finalidad de recabar el material probatorio necesario para esclarecer los hechos objeto de investigación de un ilícito penal, así como individualizar a los presuntos responsables. Se puede decir entonces que por actos de investigación se entienden aquellos actos comunes y especiales que se realizan al principio de toda investigación y son llevados a cabo por la policía (Chavez, 2020).

El autor Chavez sostuvo que los actos iniciales de investigación aquellos actos especiales realizados teniendo en cuenta la complejidad y naturaleza de algunos delitos y considero correcto, en tanto no se le puede dar el mismo tratamiento de investigación a todos los delitos, en ese sentido considero que el tipo penal de fraude informático tienen cierta particularidad que motiva su investigación basado principalmente en la búsqueda de una prueba de índole digital.

Por otro lado, otros autores hacen referencia a la labor conjunta que debieran de realizar el binomio Policía – Ministerio Público durante las investigaciones. Rivera (2019) refiere que es considerado el trabajo conjunto que se realiza entre ambas instituciones con la finalidad de esclarecer los hechos acontecidos.

En efecto, el Ministerio Público realiza sus labores de investigación auxiliado por la Policía Nacional, ambos llevan a cabo un trabajo coordinado persiguiendo fines comunes.

Tal y como sostuvo Monja (2016), los actos de investigación deben analizarse en su conjunto a fin de no afectar la labor de investigación que desarrolla fiscalía (Como se citó en Mendoza, 2021, p. 19).

Respecto a las labores que realizan el fiscal y la policía, estos deben trabajar en equipo persiguiendo los mismos fines de la investigación, manteniendo cada uno su rol, es así que mediante la Constitución y el Código Procesal Penal al fiscal se le asignan funciones de dirección y conducción de la investigación del delito, es quien debe decide la estrategia a adoptarse en una investigación coordinando su labor con la policía y escuchando las recomendaciones que pudiera plantearle, por otro lado la policía es el órgano que se encarga de prevenir, investigar y combatir la delincuencia, entre otras funciones asignadas específicamente mediante la Constitución.

Arpasi (2018) concluyó que a quien compete dirigir la investigación es al fiscal, estos actos de investigación puede llevarlos a cabo a título personal o bien delegar algunas diligencias a la policía, sin embargo, la investigación será conducida por los representantes del Ministerio Público (Como se citó en Torres, 2021, p 12).

Independientemente de las diligencias que se dispongan durante las diligencias preliminares, a fin de evitar excesos, estas deben respetar el plazo razonable previsto para ellas, en ese sentido conforme a lo manifestado por la Corte Suprema, dependiendo del delito para los casos simples será de 120 días naturales, para los casos complejos será un máximo de 8 meses, y para los casos de criminalidad organizada el plazo máximo se extiende hasta 36 meses.

Cuando se toma conocimiento de un hecho delictivo las diligencias que se realizan tiene como fin realizar los actos de naturaleza urgente e inaplazables

a fin de establecer si los hechos denunciados han ocurrido, así como recabar los elementos probatorios e identificar a los presuntos responsables; en consecuencia durante las diligencias preliminares se realizaran los actos de investigación donde el fiscal buscara obtener los elementos de convicción que demuestren que las personas sindicadas son responsables de los hechos denunciados (Torres, 2021).

Concluidas las diligencias preliminares el fiscal tiene seis caminos distintos, o bien archiva la denuncia, emitiendo una disposición de archivo, esto sucede cuando, en base a lo que establece el art. 334 del NCPP, el hecho denunciado no constituye delito, o bien por existir supuestos que van a extinguir la acción penal.

Procede el archivo también cuando el hecho hubiera prescrito o faltara la identificación del responsable de la comisión del hecho delictivo.

Un segundo camino es el principio de oportunidad, salida mediante la cual el fiscal se abstiene de ejercer la acción penal en contra del responsable de los hechos, tal y como lo establece el art. 2 del NCPP.

El tercer camino que tiene el fiscal es formalizar la denuncia, en este caso el fiscal emite una disposición de formalización y continuación de la investigación preparatoria.

Un cuarto camino es el acuerdo reparatorio, en este caso el fiscal está en la obligación de recurrir a este mecanismo y de abstenerse de ejercer la acción penal, así se afirma en el art. 2, numeral 6 del NCPP.

Un quinto camino es el proceso inmediato, situación que implica que se omita la etapa de investigación preparatoria e intermedia y se pase directamente a juicio.

Un sexto camino es el de emitir una acusación directa, y esto sucede cuando culminadas las diligencias preliminares se pasa directamente a la etapa intermedia.

Torres (2021) sostiene que resulta entonces indispensable que durante la primera etapa de investigación se recabe información sólida que puedan ser sostenidas en la etapa de juicio oral y que sirvan de sustento a las decisiones adoptadas por el juez.

### Objetivo de la investigación

Con respecto al objetivo de todo acto de investigación, Gracia (2019) indicó que el objetivo primordial del Ministerio Público es reunir todos los elementos necesarios para esclarecer los hechos que se denuncian. Es deber del Ministerio Público una vez que toma conocimiento de un hecho criminal iniciar las investigaciones. Dicha denuncia puede no necesariamente terminar en una acusación sino en una abstención de investigar, en un archivo temporal o en la aplicación de un criterio de oportunidad.

Sin embargo, más adelante mencionó que es necesario precisar que es fundamental la rapidez de los actos de investigación para tener un caso exitoso, debiendo necesariamente tener presente de no vulnerar los derechos humanos y fundamentales de las personas investigadas, y en caso de necesidad de restricción de los derechos acudir al órgano judicial para obtener la autorización correspondiente. (p.46)

Tal y como comúnmente se dice “tiempo que pasa verdad que huye”, lo que las esencias de los actos primigenios de investigación buscan es recabar todos los vestigios o indicios dejados en el lugar donde ocurre un hecho ilícito, así como recabar las declaraciones de las personas que presenciaron los hechos

o el registro de cámaras que hubieran podido grabar algún hecho ilícito con la finalidad de dar con los responsables de los hechos, siempre respetando los derechos de todo ciudadano involucrado en los hechos.

Rol de la PNP en los actos iniciales de investigación:

Finalidad de la Policía Nacional del Perú

Es importante hacer mención a las funciones con rango constitucional que se le otorgó a la PNP.

Según lo señalado en el art. 166 de nuestra Constitución, la Policía debe garantizar o restablecer el orden interno, además de brindar protección y ayuda a los miembros de la sociedad y hacer cumplir las normas, en el ámbito de investigación previene realiza investigaciones y lucha contra la delincuencia.

Existen algunas funciones que están expresamente asignadas a la Policía, sobretodo en cuanto al desarrollo de las investigaciones, en lo específico en las técnicas especiales de investigación. Delgado, Espinoza y Espinoza (2007) aseguran que la PNP y el Ministerio Público deben realizar un trabajo coordinado y conjunto con el fin de recabar y asegurar la prueba.

## Funciones y atribuciones de la Policía

De la misma forma el NCPP del año 2004 en su art. 67, respecto a las atribuciones asignadas a la Policía Nacional en materia de investigación, son las siguientes:

1. Cuando toma conocimiento de la comisión de delitos dar cuenta de inmediato al fiscal.
2. Llevar a cabo aquellas diligencias que son consideradas urgentes e indispensables para impedir se produzcan consecuencias ulteriores.
3. Identifica a los autores del hecho denunciado (autor y partícipes de ser el caso).
4. Reunir todo el material probatorio indispensable para esclarecer los hechos e imputar responsabilidades.
5. Apoyar en las labores de investigación al Ministerio Público durante toda la etapa investigación preparatoria.

Así también el NCPP en su art. 68 las atribuciones propias de la Policía, dichas atribuciones se llevan a cabo bajo la conducción del Fiscal, tal es el caso de recibir denuncias o sentar actas, tomar declaraciones, vigilar y proteger el lugar donde ocurre un hecho de índole delictuosa, realizar el registro de las personas, reunir y mantener los elementos o bienes que tengan conexión con el delito, llevarse a cabo las actuaciones que tengan como fin identificar a los responsables del hecho, realizar planos y tomas fotográficas, realizar grabaciones, como la captura de los presuntos responsables, el allanamiento de locales de uso público, entre otras.

De todas aquellas diligencias que realiza la Policía sentara en actas de manera detallada y precisa los acontecimientos materia de investigación.

Reyna (2015) afirmó que cuando Fiscalía toma conocimiento de un hecho delictivo dispone que la Policía realice las diligencias que tengan naturaleza de urgente e indispensables, diligencias que tienen como objetivo primero determinar si los sucesos ocurrieron, segundo garantizar los indicios y evidencias, y tercero individualizar a los responsables.

No cabe duda el rol importante que tiene aún la Policía Nacional durante la investigación de los hechos, sin embargo, se debe tener en cuenta que este poder no es absoluto, debiéndose realizar sus funciones en respeto de los derechos básicos y elementales garantizados constitucionalmente que asisten a todo detenido o investigado, los mismos que encontramos en el art. 71 del NCPP.

Del mismo modo al día de hoy subsisten limitaciones de tipo operativo que impiden que la Policía pueda realizar sus funciones de manera eficiente, en efecto muchas comisarias del país aún carecen de medios de comunicación idóneos para poner en conocimiento los hechos delictivos, limitaciones en los medios de transporte, la insuficiencia de personal, falta de capacitación, entre otros, son los principales problemas al ejercicio eficiente de sus funciones y a la lucha contra las distintas formas de criminalidad.

#### Rol del Ministerio Público en los actos iniciales de investigación

Según lo señalado en el art. 158 de nuestra Constitución, el órgano defensor de la legalidad es un órgano independiente presidido por el Fiscal de la Nación, quien viene elegido por la Junta de Fiscales Supremos durante un lapso de tiempo de tres años. Es importante hacer mención a la autonomía y funciones con rango constitucional que se le otorga al Ministerio Público.

## Funciones y atribuciones del Ministerio Público

Entre las funciones de investigación del Ministerio Público plasmados en el art. 159 del NCPP se encuentran las siguientes:

1. Es el encargado de promover de oficio o bien a solicitud de parte la acción judicial en beneficio y en defensa de la Ley y de los intereses del Estado.
2. Vigila que se respete y cumpla con la autonomía e independencia de los órganos jurisdiccionales, así como por la recta administración de la justicia.
3. Representa a la sociedad en todos los procesos de naturaleza judicial.
4. Es el encargado de dirigir las investigaciones desde el principio con total autonomía, para tal fin puede solicitar apoyo a la Policía Nacional para la efectuar ciertas diligencias.
5. Previo a la emisión de las resoluciones judiciales, cuando fuera el caso, emitir los correspondientes dictámenes fiscales.
6. Tiene iniciativa legislativa.

Será entonces Fiscalía el órgano director encargado de dirigir las actuaciones necesarias para el esclarecimiento de los hechos con apoyo de la Policía, garantizando los Derechos Constitucionalmente que asiste a toda persona involucrada en una investigación.

El Ministerio Público debe conducirse con total imparcialidad, para ello controla jurídicamente los actos de investigación que realiza la Policía. Quispe (2020) indica que el personal fiscal es una persona con formación jurídica, por tal motivo tiene un conocimiento en materia jurídica, apto para encabezar las investigaciones desde el principio, así como para recabar el material probatorio relevante para sostener una acusación, sin embargo, para alcanzar dicho fin requieren del apoyo de personal idóneo en materia de investigación, en pocas palabras se requiere del apoyo del personal policial especializado en la disciplina.

## La prueba y las nuevas tecnologías

### Concepto

La prueba, tal y como lo ha reconocido nuestro Tribunal Constitucional es un derecho constitucionalmente implícito que encontramos en el derecho al debido proceso, art. 139 inciso 3. Dellepiane (1994) sostuvo que el recurso mediante el que se logra certeza de los hechos que son objeto de denuncia es la prueba.

La prueba como tal busca efectivizar la responsabilidad jurídico penal de los implicados al interior de un juicio, la estructura del derecho a probar está compuesta por cinco momentos distintos: en primer lugar se tiene el derecho a ofrecer los medios probatorios que se consideran básicos, en segundo lugar el derecho a que estos medios sean admitidos, en tercer lugar el derecho a que sean actuados, el derecho a que se produzcan y conserven las pruebas habiendo sido actuadas de manera anticipada, y por último a que los medios probatorios sean valorados por el juzgador.

La prueba constituye una necesidad básica de sustentar o corroborar hechos o afirmaciones sostenidas, es considerada también una necesidad intelectual de los seres humanos que tienen capacidad para conocer. (Rodríguez, 2019).

Rodríguez (2019) afirmó que la distinción entre actos de investigación y prueba se basa en que los primeros son indispensables para obtener la prueba. Se investiga para probar.

La actividad probatoria de las partes está orientada a persuadir, generar certeza en los magistrados sobre la teoría planteada y llevada a juicio, en lo

especifico la finalidad que buscan lograr es la convicción sobre sus afirmaciones realizadas durante el proceso.

El proceso penal peruano se orienta hacia un sistema denominado de sana-critica, los magistrados al momento de fallar basan sus decisiones en las reglas de la lógica, de la ciencia y de las máximas de las experiencias.

El art. 156 del NCPP indica que es objeto de prueba todo lo que esté relacionado a la imputación planteada, la punibilidad y la determinación de la sanción.

Sobre los medios de prueba el mismo Código Procesal Penal nos refiere que estos pueden ser:

- a) La Confesión sincera
- b) El testimonio
- c) La pericia
- d) El careo
- e) La prueba documental
- f) Los otros medios de prueba.

En los últimos años debido los pasos gigantes en la tecnología de la información, las laptops y teléfonos inteligentes han revolucionado nuestras vidas. Sin embargo, el derecho no puede quedarse indiferente frente a ello, más aún si con más frecuencia se ofrecen como medios probatorios documentos recogidos de soportes electrónicos, me estoy refiriendo a la prueba tecnológica o también llamada electrónica.

Quiles (s.f.) indicó que por “prueba electrónica” o “tecnológica” se consideran las grabaciones, los sonidos y las imágenes que se soportan en

instrumentos electrónicos en los que se guardan información y que son indispensables para acreditar los hechos en juicio.

La prueba tecnológica o electrónica se denomina como tal en tanto los hechos objeto de investigación o la información relevante se encuentran al interior de modernos instrumentos tecnológicos.

Estudios como el de Sanchez (2016) estableció que lo que se registra en internet y en las modernas redes sociales constituyen un almacenamiento de evidencias electrónicas, representando un verdadero y propio medio de prueba digital reproducible en juicio (Como se citó en Zarzosa, 2018, p.19).

Las evidencias a las que se hace referencia se ubican al interior de las aplicaciones que hoy en día están al alcance de todos y que por su difusión e importancia en nuestras vidas cotidianas son de uso ordinario, recogiendo una cantidad exorbitante de información, aplicativos que también son usados como medio para la comisión de delitos.

De la misma forma en que se obtienen o recaban los medios probatorios ordinarios, las pruebas electrónicas deben obtenerse en respeto de los derechos fundamentales, asimismo deben ser recabados integralmente y de manera autentica, bajo sanción de pedir su nulidad en las etapas correspondientes.

En el Perú la prueba digital como tal no está expresamente incorporada en nuestro Código Procesal Penal, sin embargo, de manera indirecta puede ser considerado como una prueba documental.

Tal y como refirió Bueno de mata (2013) No existe una regulación particular para la prueba electrónica. Lo que implica que la prueba digital sea trasladada a juicio e incorporada mediante la prueba documental. La prueba

digital podría considerarse como una prueba independiente y autónoma inclusive como un número apertus. (Como se citó en Zarzosa, 2018, p.20)

Zarzosa (2018) refiere que la definición que se acerca más al concepto de prueba digital es la que sostiene que es todo tipo de información que se obtiene mediante algún medio o dispositivo electrónico y que tiene como fin demostrar y convencer al juez de un hecho ocurrido y siempre que para su obtención se haya garantizado los derechos básicos para la obtención de la prueba, de manera que constituya prueba lícita, idónea, pertinente y útil.

La importancia de un análisis forense e informático a la prueba electrónica es demostrar la autenticidad del material probatorio aportado, de manera que no se pueda dudar de la veracidad e integridad de la información sustraída de los soportes electrónico.

Aldama (2017) respecto a las pericias informáticas indica que son aquellas que se realizan a los instrumentos que contienen información o datos almacenados en soportes informáticos, tales como tablets, laptops, celulares, Usb, entre otros. Los procedimientos que se adopten deben garantizar la sustracción íntegra de la información sin manipulación alguna, para ello se debe mantener la cadena de custodia durante toda la pericia. Siendo el fin de la pericia la de identificar al autor, analizar las actividades realizadas con el dispositivo electrónico objeto de análisis, así como recuperar la información eliminada de los correos o de las demás redes sociales, así como de cualquier otra información que sea pública en Internet.

## B.- Delito de Fraude informático

### Concepto

El delito de fraude informático se encuentra incluido en el catálogo de los delitos informáticos, incorporado primigeniamente mediante la Ley N<sup>a</sup> 30096, y posteriormente modificada mediante la Ley N<sup>a</sup> 30171, Ley que modifica la Ley de delitos informáticos, ubicado en el art. 8 de la Ley.

Cabe destacar que con el avance y desarrollo de las nuevas herramientas informáticas se han generado usos indebidos de las mismas para la comisión de lo que hoy constituyen ilícitos penales, siendo la informática una herramienta poderosa para aprovecharse de datos y de información valiosa vulnerada sin autorización alguna, constituyendo una verdadera preocupación para todos los Estados.

El delito de Fraude informático en los últimos años ha generado un interés cada vez más creciente, siendo el protagonista de los delitos informáticos, sin embargo, dicho delito debe entenderse de manera muy amplia, en efecto, en este tipo penal se encuadran varios comportamientos o otros delitos que debieron, según mi consideración, ser tipificados de manera individual.

Puedo definirlo entonces como aquel delito que procura un perjuicio ilícito, normalmente de índole patrimonial a un tercero, llevado a cabo mediante el diseño, introducción, alteración, borrado, supresión o clonación de sistemas informáticos. Sin embargo, no siempre se habla de perjuicio patrimonial directo en este delito, en tanto es posible que se incluyan en el tipo penal conductas centradas también a la obtención de información o datos indispensables para generar posteriormente dichos perjuicios.

Gutiérrez (1991) sostuvo que el delito de fraude informático lesiona más de un bien jurídico. En un primer momento lesiona el interés económico,

el interés del Estado, el sistema económico y financiero, así como el funcionamiento de los sistemas informáticos.

En efecto, estos delitos provocan no solo un perjuicio personal, para el sujeto pasivo sino también para el sistema crediticio, sistema financiero y Estado en general, al haberse vulnerado los accesos y sistemas de seguridad de las entidades encargadas de proteger las inversiones o ahorros familiares (Como se citó en Acurio del Pino, s.f., p.22).

García (2008) sostiene que el delito de fraude informático o también llamado de estafa mediante el uso de medios informáticos, descienden de los cibercrimes, delitos en los que mediante el uso del sistema informático se realizan transferencias económicas electrónicas a favor de la persona autora.

Tal y como se mencionó durante el presente trabajo, el delito de fraude informático interpretado de manera amplia incluye varios comportamientos, pudiendo fácilmente encuadrar en varios tipos penales, que debieran ser distintos tipos penales.

Según Posada (2017) indicó que los cibercrimes y delitos informáticos surgieron en los años setenta del siglo XX, donde inicialmente se pusieron de manifiesto una serie de transferencias realizadas sin consentimiento alguno generando daños informáticos, situación que conllevó a un cambio en los Estados respecto a las nuevas nociones y formas de delinquir, lo que permitió de cierta forma hacer frente a estos nuevos ilícitos penales que ponían en evidencia la fragilidad de los sistemas de seguridad y generaban desconfianza entre los usuarios a las nuevos sistemas informáticos por peligrar la exposición de datos e información considerada privada.

Los delitos informáticos, son más complejos que los delitos comunes por ser cometidos normalmente por personas altamente capacitadas, quienes se encuentran a la vanguardia de los avances tecnológicos, sea porque el lugar de comisión de los hechos no es fácilmente identificable, sumado a ello se tiene que los países no han logrado, pese a los esfuerzos fortalecer cooperaciones internacionales para combatir estos ilícitos penales.

La fuente de cooperación más sólida que se tiene al día de hoy es el Convenio de Budapest del año 2001, el mismo que estableció los siguientes tipos delictivos:

- 1) Los delitos contra la Confidencialidad, Disponibilidad e Integridad de los datos y sistemas informáticos,
- 2) Los delitos informáticos propiamente dichos,
- 3) Los delitos con contenidos ilícitos,
- 4) Infracciones a la ley de propiedad intelectual

#### Características de los delitos informáticos

Existen algunos caracteres comunes a los delitos informáticos, según el maestro Fernández (2014) indicó que son:

- La ausencia de uniformidad en las legislaciones de los distintos Estados respecto a los delitos informáticos;
- La globalidad de los efectos en la comisión de estos delitos, los cuales muchas veces se producen en un lugar distinto a donde se originan;
- La ausencia de una sanción a estas conductas delictivas, las que en algunos países encuentran sus paraísos, no siendo aun tipificadas en algunos países:
- La lentitud de la implementación de las normas sancionadoras respecto a los

avances de la tecnología.

Características comunes, que también se ubican en el delito de fraude informático y que rinde dificultosa su persecución y represión.

Otro autor Tellez (2003) indicó las siguientes características:

1. Denominados delitos de cuello blanco, por la particularidad en los conocimientos que requieren los autores de dichos ilícitos.
2. Son consideradas ocupacionales en tanto se realizan o despliegan mientras los autores realizan sus propios trabajos.
3. Son acciones de oportunidad, en las que se aprovecha de las ocasiones creadas o altamente intensificada en el mundo del sistema tecnológico y económico.
4. Generan significativas pérdidas, produciendo por lo contrario grandes beneficios para los autores.
5. Aprovechan al máximo la condición tiempo-espacio ya que no se requiere de su presencia física para beneficiarse de cuantiosas cantidades de cuentas de usuarios de otros países.
6. Son en constante aumento sin embargo aún son pocas las denuncias que se realizan, y ello debido a una ausencia de regulación en la materia.
7. Son muy sofisticados.
8. Las investigaciones que se realizan no son lo suficientemente técnicas como para corroborar estos delitos, que de por sí son complejos.

9. Aumentan de manera exponencial por lo que resulta necesario una regulación puntual sobre estos delitos. (p. 8)

#### Tratamiento normativo

En el Perú fue aprobado y ratificado en el año 2019 el Convenio sobre la Ciberdelincuencia del Consejo de Europa.

Inicialmente los delitos informáticos se encontraban al interior del art.186 inciso 3, segundo párrafo de nuestro Código Penal del año 1991, no siendo tipificado como un delito en sí, sino se consideró como un agravante del tipo penal de hurto, posteriormente en el Capítulo X del C.P. se integraron los delitos denominados “delitos informáticos” en los artículos 207-A, 207-B, 207-C, y 207-D. Sin embargo, en el año 2013 entro en vigencia la Ley N° 30096, Ley especial de Delitos Informáticos, conformada por siete capítulos.

La última modificación a esta Ley Especial se dio con la Ley N° 30171 la misma que modifica la Ley Especial de Delitos Informáticos, su objetivo fue el de adecuar la normativa al Convenio de Budapest. Dicha ley prevé en su art. 8 el delito de Fraude Informático, manifestando que:

“El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el **diseño, introducción, alteración, borrado, supresión, clonación** de datos informáticos o cualquier **interferencia** o **manipulación** en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.”

a) Verbo rector

El artículo 8 de la Ley Especial establece en el primer párrafo enuncia los verbos típicos con los que intenta configurar el delito de fraude informático, es así que tenemos las acciones de diseñar, introduce, altera, borra, suprime o clona, interfiere o manipula datos informáticos o el funcionamiento de un sistema informático. Como bien se puede entender el verbo rector diseñar implicaría proyectar, planificar, respecto al verbo rector introducir, quiere decir ingresar en este caso a los sistemas informáticos, borrar, vale decir quitar algún tipo de información, suprimir, esto es desaparecer, alterar lo que implica dañar, quitar la estructura primigenia.

Al mencionar el mismo artículo que para que se configure el tipo penal es necesario que el autor procure para sí mismo o en favor de un tercero un provecho ilícito, se trata de un delito de resultado no siendo suficiente que se cumpla el verbo rector para la comisión del delito.

- b) Sujeto activo: el tipo penal no solicita particularidad alguna respecto al sujeto activo, pudiendo ser autor de este delito cualquier persona.
- c) Sujeto pasivo: puede ser cualquier ser humano que es perjudicado económicamente mediante el uso de la herramienta tecnológica.
- d) Bien jurídico protegido: la doctrina lo considera como un delito pluriofensivo, al atentar el mismo contra el orden económico, la intimidad de la persona y la libertad, empero, considero que el bien jurídico que se salvaguarda es el patrimonio económico, el mismo que debe ser entendido como los bienes que pueda tener una persona y que puede ser cuantificado económicamente.

Respecto al bien jurídico, Villavicencio (2014) nos menciona que primero que para la configuración de este delito se requiere del empleo de sistemas automatizados de información, segundo lo que se afecta con estos delitos es la indemnidad, la intimidad, y dichos bienes tienen cierta importancia económica por la información que se sustrae. (Como se citó en Custodio , 2021, p, 20)

- e) Comportamiento delictivo: el tipo penal prevé que realizada algunas de las conductas mencionadas el sujeto pasivo será sancionado con una pena que va de 3 a 8 años y con 65 a 120 días-multa. Sin embargo, si las conductas afectaran el patrimonio Estatal, cuyos recursos estén destinados a programas de índole asistencial o de apoyo social la pena se incrementará y será no menor de 5 ni mayor de 10 años y de 80 a 140 días-multa.

## **1.5 Hipótesis**

### **Hipótesis general**

Los actos de investigación llevados a cabo durante las diligencias preliminares no son suficientes para el esclarecimiento de los delitos de fraude informático en el Distrito Fiscal de Lima Sur, durante el año 2021.

## **1.6 Objetivos**

### **Objetivo General**

Determinar si los actos de investigación llevados a cabo durante las diligencias preliminares son suficientes para el esclarecimiento de los delitos de fraude informático en el Distrito Fiscal de Lima Sur, durante el año 2021.

### **Objetivos Específicos**

**OE1.** Determinar si las diligencias realizadas y dispuestas a nivel fiscal resultan determinante para el esclarecimiento del delito de fraude informático, en el Distrito Fiscal de Lima Sur, durante el año 2021.

**OE2.** Determinar si resulta necesario un tratamiento normativo más completo para una lucha adecuada del delito de fraude informático, en el Distrito Fiscal de Lima Sur, durante el año 2021.

**OE3.** Establecer la importancia de la prueba digital en la investigación de los delitos fraude informático en el Distrito Fiscal de Lima Sur, durante el año 2021.

## **II. Metodología**

### **2.1 Tipo de investigación**

La investigación realizada fue de tipo empírica, diseño no experimental, de nivel descriptivo y de corte transversal.

Para Murillo (2008), la investigación aplicada denominada también investigación práctica o empírica busca aplicar o utilizar los conocimientos que se adquieren y al mismo tiempo adquirir nuevos conocimientos. Los resultados que se obtienen de la investigación son el fruto de una rigurosa, organizada y sistemática forma de conocer la realidad.

Los diseños de investigación transversal tienen como fin el realizar una descripción de las variables y analizar su relación entre ellas en un cierto tiempo. (HERNANDEZ S. 2006, p. 154). Además, es una investigación no experimental, denominación dada visto que no se van a manipular las variables.

Es un estudio descriptivo porque pretende identificar las propiedades, características y perfiles de personas, grupos, comunidades, procesos que están bajo análisis y estudio. (HERNANDEZ S. 2006, p. 92)

## **2.2 Población y muestra**

### **Población**

La población a quienes se destinaron la aplicación de la encuesta estuvo constituida por 30 personas entre Fiscales y Asistentes del Distrito Fiscal de Lima Sur especializados en el tema.

### **Muestra**

No se trabajará con muestra, toda vez que la encuesta se aplicará a la totalidad de la población señalada en el párrafo precedente.

## **2.3 Técnicas e instrumentos de investigación**

Para desarrollar esta investigación se optó por técnicas de recolección de información que a continuación se exponen:

### **Análisis Documental**

Mediante la técnica del análisis documental, se recabó toda la información necesaria para responder a nuestra investigación, cuya fuente principal fueron registros, folletos, libros, estadísticas proporcionadas por el mismo Distrito Fiscal de Lima Sur sobre las denuncias sobre el delito de fraude informático

durante el año 2021. Se empleó como instrumento la ficha de análisis del contenido.

### **Encuesta**

Durante la investigación se efectuó una encuesta anónima a través del cuestionario con preguntas cerradas y con alternativas obtenido mediante la operacionalización de las variables, indicadores, problemas e hipótesis, permitiéndose aplicar la encuesta anónima para obtener información provenientes de la muestra de la población objeto de análisis y estudio, los mismos que serán tabulados y porcentuados mediante tablas, gráficos para su posterior interpretación y discusión, situación que permitió redactar las conclusiones y recomendaciones.

Se empleó el instrumento cuestionario estructurada en base a nuestra propuesta de investigación.

## **3. Resultados**

### **3.1 Resultados de la técnica de análisis documental**

#### **CUADRO N° 01: DEFINICIÓN DE DELITO DE FRAUDE INFORMATICO**

<b>Convenio sobre la Ciberdelincuencia regula en su art. 8 el delito de fraude informático.</b>	Las partes mediante su legislación interna adoptaran las medidas a fin de tipificar como delito aquellas conductas que generan perjuicios patrimoniales a terceros:  A. Mediante la introducción, alteración, borrado o
---	---

	<p>supresión de datos informáticos.</p> <p>B. Otras interferencias en los sistemas informáticos, con la finalidad de recabar de forma ilegítima un provecho económico para sí o en beneficio de terceros.</p>
<p><b>Laura Mayer Lux y Guillermo Oliver Calderón.</b></p> <p><i>El delito de fraude informático: concepto y delimitación. Vol. 9 Numero 1 (2020): Primer semestre 2020.</i></p>	<p>El autor indica que la noción de fraude informático desde un punto de vista estricto está relacionado menoscabo de naturaleza económica que se lleva a cabo mediante la manipulación, alteración o bien a través del uso de programas informáticos.</p> <p>Desde una visión general en el fraude informático se incluyen conductas que no necesariamente son causas directas de un perjuicio patrimonial, sino también que implica comportamientos que tienen como fin obtener información necesaria para generar ese perjuicio económico, pudiendo generar de esta forma confusión respecto a otros tipos penales de la parte especial.</p>
<p><b>Santiago Acurio Del Pino, profesor de Derecho Informático de la PUCE.</b></p>	<p>Sostiene que la doctrina ha denominado a los delitos generados por el uso disvalioso de la informático</p>

<p><i>Delitos Informáticos: Generalidades</i> <i>2016 Ecuador.</i></p>	<p>como delitos informáticos, criminalidad mediante computadoras, delincuencia informática, criminalidad informática.</p>
<p><b>Miguel Ángel Davara.</b></p>	<p>Las características de los delitos objeto de estudio son la intangibilidad de los datos en las redes, como valor supremo en esta sociedad, el anonimato que favorece y brinda protección a los delincuentes, la difícil tarea de recabar pruebas, las dificultades no solo físicas sino también lógicas y normativas para poder investigar, procesar y enjuiciar estos hechos delictivos, son las que más resaltan y favorecen el incremento de estos delitos que deben ser tratados y solucionados a nivel nacional.</p>
<p><b>Davara Rodríguez</b></p>	<p>El delito informático es aquella acción que se manifiesta mediante el empleo de un elemento informático o bien telemático, o afectando los derechos de la persona titular de la fuente informática.</p>
<p><b>Pérez López</b></p>	<p>El autor mediante el uso de las herramientas informáticas genera para sí o para terceros un beneficio impropio mediante las siguientes</p>

	acciones: diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o manipulación en el funcionamiento de un sistema informático.
--	--

**CUADRO N° 02: DEFINICIÓN DE ACTOS DE INVESTIGACIÓN**

<p><b>Mario Nicolas Cadavid Botero.</b>  <i>Fiscal Delegado ante el Tribunal Catedrático - Facilitador</i></p>	<p>Afirma que es necesario realizar la distinción entre actos de investigación y actos de prueba, la finalidad de los primeros es reunir las evidencias o demás elementos materiales probatorio que serán empleados en el juicio oral para verificar las teorías de las partes y de Fiscalía, las que servirán de sustento en los fallos judiciales.</p> <p>Los actos de investigación por su complejidad tienen distintos niveles de limitación de los derechos y garantías constitucionales, en ese sentido es necesario que previo a su afectación el Fiscal debe evaluar la necesidad, trascendencia, y un control de los requisitos constitucionales y legales.</p>
--	--

	<p>Los actos de investigación encuentran su justificación en la necesidad de encontrar evidencia, indicios y otros elementos materiales probatorios.</p>
<p>La prueba en el proceso penal colombiano, Fiscalía General de la Nación, Colombia 2008, p. 39</p>	<p>La finalidad de todo acto de investigación es la de observar, identificar, recaudar, analizar y obtener las evidencias o elementos materiales probatorios que serán posteriormente llevados al juzgamiento para corroborar las posiciones asumidas por las partes, así como para justificar las decisiones que correspondan al Juez.</p>
<p><b>Pedro Pablo Carmona Sánchez</b> - <i>Actos de investigación que requieren autorización previa del Juez de Control - CNPP</i></p>	<p>Son los actos que se realizan durante la etapa de investigación cuyo director será Fiscalía en representación de la Sociedad, quien en colaboración y participación de los peritos y policía recaban todos los elementos necesarios para sostener su tesis planteada. Para tal fin en ciertos casos será necesario la previa intervención del Juez de Control, esto cuando el acto de investigación a llevarse a cabo implique la vulneración directa o indirecta de los derechos constitucionales de toda persona.</p>

<p><b>Ramiro Salinas Siccha.</b> <i>Conducción de la Investigación y Relación del Fiscal con la Policía en el Nuevo Código Procesal Penal.</i></p>	<p>El Fiscal con el fin de reunir los elementos necesarios para esclarecer los hechos y las responsabilidades lleva a cabo actos de investigación. Disponiendo la participación del implicado, agraviado y demás sujetos que puedan aportar información útil para el esclarecimiento de la denuncia. La naturaleza preparatoria de los actos de investigación y su diferencia con los actos de prueba radica en que los primeros no tienen carácter jurisdiccional y solo son útiles a fin de emitir resoluciones propias de la etapa en la que se encuentran. Siendo el Ministerio Público el representante de la Sociedad, planteará la investigación competente conducir y controlar los actos de investigación que realiza la policía.</p>
<p><b>Burgos Mariños Víctor.</b> <i>El proceso penal peruano: una investigación sobre su constitucionalidad.</i></p>	<p>La investigación del delito es un requisito indispensable de todo juicio penal, mediante el que a través de los actos de investigación se reúnen los elementos probatorios que puedan fundar y sostener la acusación fiscal. Los actos de investigación tienen la finalidad de acreditar el hecho punible y su autoría, son aquellos</p>

	actos que tienden a asegurar el material probatorio mediante el auxilio de la Policía.
--	--

**CUADRO N° 03: EL DELITO DE FRAUDE INFORMATICO EN LA LEGISLACIÓN COMPARADA**

<b>ESPAÑA</b>	<p>El fraude informático es una tipología de cibercrimen en el que se emplean medios informáticos como medio para realizar transferencias de patrimonios de terceros a favor del autor.</p> <p>Se encuentra regulado en el art. 248 numeral 2 del código penal español de 1995 y es considerado como una modalidad de estafa. Aunado a ello la L.O. 15/2003 introduce un tercer párrafo relacionado al fraude informático en sus actos preparatorios.</p> <p>En estos delitos se actua de oficia.</p>
<b>ITALIA</b>	<p>La legge N° 57 del 23-12-1993 en Italia contempla todas las tipologías de agresiones informáticas. El frode informático se encuentra previsto en el art. 640ter del Codice Penale: “el que de cualquier modo altere el funcionamiento de un sistema informático o telemático o interviniendo sin derecho con cualquier modalidad sobre los datos, informaciones o programas contenidos en un sistema informático o telemático o a ellos concernientes, procurando para sí o a otro un injusto provecho con daño para otro, será castigado</p>

	<p>con reclusión de seis meses a tres años y con multa de 51 euros a 1.032 euros”.</p> <p>En estos delitos se actúa solo previa querrela del ofendido.</p>
<b>ARGENTINA</b>	<p>Es conocido como estafa informática y lo encontramos en el art. 173 inciso 16 del Código Penal Argentino, introducida mediante Ley N° 26.338 B.O. 25/06/2008, el que incorpora en las disposiciones relativas a los casos de defraudaciones especiales <i>al que defraudara a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos</i>. Esta nueva figura constituye una figura especializada con relación al delito de estafa previsto y sancionado en el art. 172 del Código Penal Argentino.</p>
<b>CHILE</b>	<p>En el ordenamiento jurídico chileno actualmente no se han contemplado figuras como el hacking ni el fraude informático. La Ley N° 19223 prevé figuras típicas mediante el empleo de uso informático en la Ley N° 19223, la misma que establece 4 conductas específicas relativas a un sistema de información:</p> <ul style="list-style-type: none"> <li>- Quien maliciosamente destruya o inutilice, impida o entorpezca o varíe su funcionamiento.</li> <li>- Quien mediante ánimo de apropiarse, usa o conoce o bien intercepta o acceda a él.</li> <li>- Quien dolosamente cambia o daña o elimine la información.</li> </ul>

	<ul style="list-style-type: none"> <li>- Quien dolosamente revela o bien difunde la información contenida en un sistema de información.</li> </ul>
<p><b>COLOMBIA</b></p>	<p>La ley N° 1273 del año 2009 contemplo e incorporo los delitos informáticos, dicha Ley incorpora varios artículos y figuras:</p> <ul style="list-style-type: none"> <li>- Ingreso indebido a un sistema informatico</li> <li>- Obstrucción indebida de sistema informático.</li> <li>- Interceptación de información informática</li> <li>- Daño informático</li> <li>- Empleo doloso de programas</li> <li>- Vulneración de datos personales</li> <li>- Hurto por medios informáticos.</li> <li>- Traslado de recursos económicos de las cuentas, y otros.</li> </ul> <p>Las figuras que más se asemejan al fraude informático son el art. 269 I el Hurto por medios informáticos y semejantes y el art. 269 J Transferencias no consentidas de activos, ambos tipos penales lo que buscan es obtener un provecho ilícito mediante el empleo de las herramientas informáticas.</p>

**Tabla 1**

*Denuncias ingresadas en el año 2021 por el delito de Fraude Informático*

FISCALIA PROVINCIAL PENAL CORPORATIVA DE LURIN	CANTIDAD DE DENUNCIAS INGRESADAS
1° DESPACHO	14
2° DESPACHO	21
3° DESPACHO	17
4° DESPACHO	19
TOTAL	71

Fuente: Elaborado por el analista del Distrito Fiscal de Lima Sur

**Tabla 2**

*Denuncias atendidas en el año 2021 por el delito de Fraude Informático*

FISCALIA PROVINCIAL PENAL CORPORATIVA DE LURIN	CANTIDAD DE DENUNCIAS ATENDIDAS
1° DESPACHO	14
2° DESPACHO	21
3° DESPACHO	17
4° DESPACHO	19
TOTAL	71

Fuente: Elaborado por el analista del Distrito Fiscal de Lima Sur

**Tabla 3***Denuncias archivadas en el año 2021 por el delito de Fraude Informático*

FISCALIA PROVINCIAL PENAL CORPORATIVA DE LURIN	CANTIDAD DE DENUNCIAS ARCHIVADAS
1° DESPACHO	11
2° DESPACHO	19
3° DESPACHO	11
4° DESPACHO	16
TOTAL	57

Fuente: Elaborado por el analista del Distrito Fiscal de Lima Sur

**Tabla 4***Denuncias consentidas en el año 2021 por el delito de Fraude Informático*

FISCALIA PROVINCIAL PENAL CORPORATIVA DE LURIN	CANTIDAD DE DENUNCIAS (ESTADO:ARCHIVO CONSENTIDO)
1° DESPACHO	11
2° DESPACHO	18
3° DESPACHO	11
4° DESPACHO	14
TOTAL	54

Fuente: Elaborado por el analista del Distrito Fiscal de Lima Sur

**Tabla 5***Denuncias formalizadas en el año 2021 por el delito de Fraude Informático*

---

<b>FISCALIA PROVINCIAL PENAL CORPORATIVA DE LURIN</b>	<b>CANTIDAD DE DENUNCIAS FORMALIZADAS</b>
1° DESPACHO	0
2° DESPACHO	0
3° DESPACHO	0
4° DESPACHO	0
<b>TOTAL</b>	<b>0</b>

---

Fuente: Elaborado por el analista del Distrito Fiscal de Lima Sur

**Tabla 6***Acusaciones fiscales formuladas en el año 2021 por el delito de Fraude Informático*

---

<b>FISCALIA PROVINCIAL PENAL CORPORATIVA DE LURIN</b>	<b>CANTIDAD DE ACUSACIONES</b>
<b>1° DESPACHO</b>	<b>0</b>
<b>2° DESPACHO</b>	<b>0</b>
<b>3° DESPACHO</b>	<b>0</b>
<b>4° DESPACHO</b>	<b>0</b>
<b>TOTAL</b>	<b>0</b>

---

Fuente: Elaborado por el analista del Distrito Fiscal de Lima Sur

### 3.2 RESULTADOS DE LA ENCUESTA

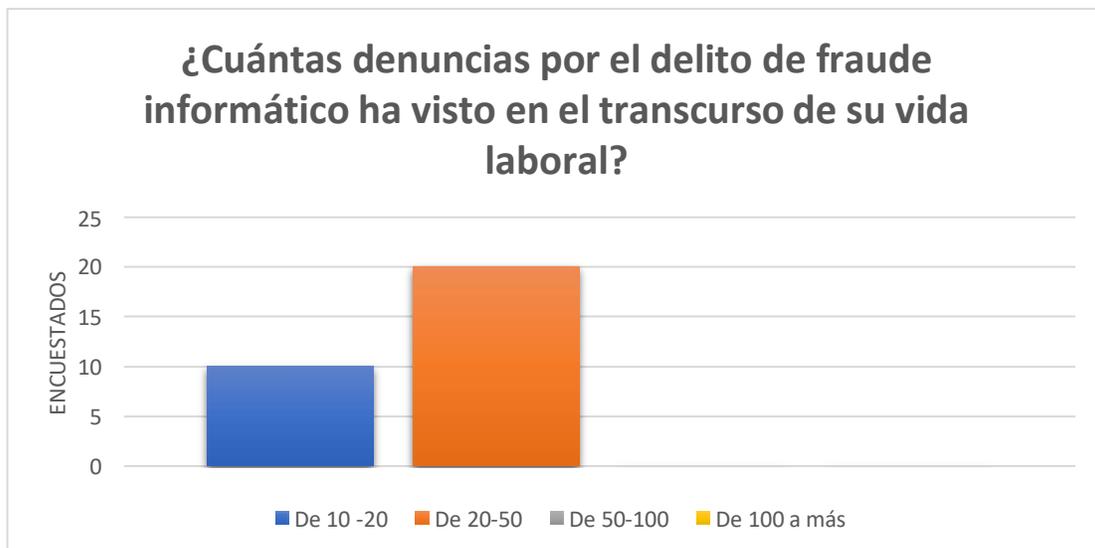
Se aplicó una encuesta que fue dirigida al personal que labora en los Despachos de la Fiscalía Provincial Penal Corporativa del Distrito Fiscal de Lima Sur.

La información obtenida fue analizada e interpretada mediante cuadros estadísticos, así como en gráficos.

**PREGUNTA N° 01:** ¿Cuántas denuncias por el delito de fraude informático ha visto en el transcurso de su vida laboral?

ALTERNATIVAS	RESPUESTAS	%
De 10 – 20	10	33.33
De 20 – 50	20	66.67
De 50 – 100	0	0
De 100 a más	0	0

Fuente: Elaborado por la tesista



**Figura 1.** Cantidad de denuncias vistas durante el transcurso de la vida laboral

**PREGUNTA N° 02:** ¿En qué porcentaje aquellas denuncias que ha investigado han sido formalizadas?

<b>ALTERNATIVAS</b>	<b>RESPUESTAS</b>	<b>%</b>
De 0 a 10%	30	100
De 11 a 20%	0	0
De 21 a 50%	0	0
De 50 a 100%	0	0

Fuente: Elaborado por la tesista

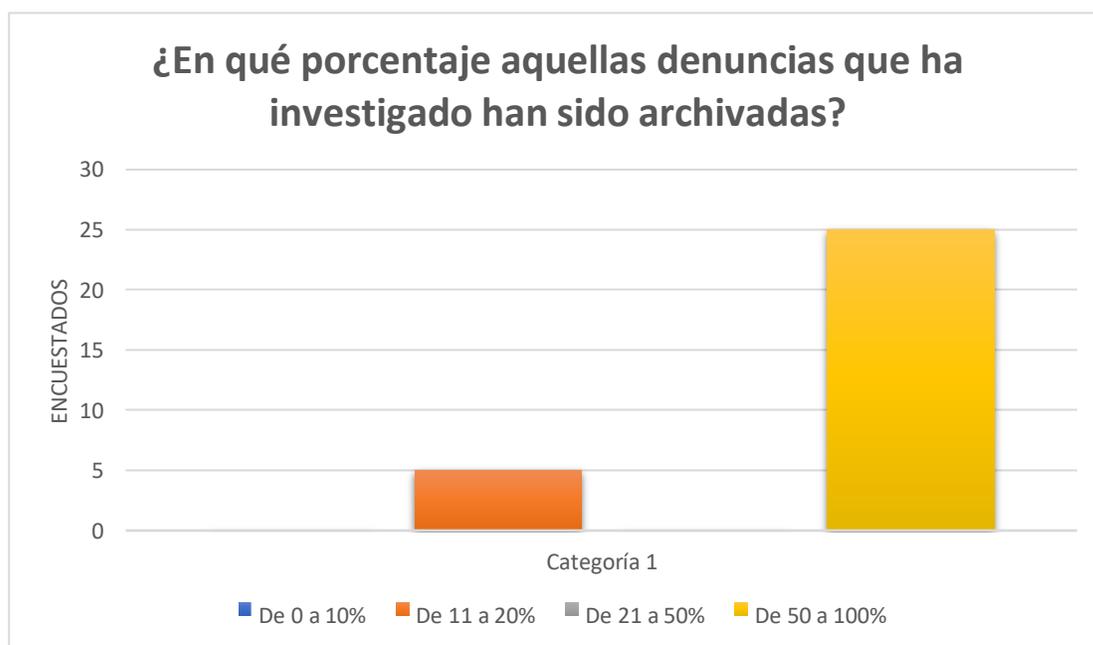


**Figura 2.** Porcentaje de denuncias formalizadas

**PREGUNTA N° 3:** ¿En qué porcentaje aquellas denuncias que ha investigado han sido archivadas?

<b>ALTERNATIVAS</b>	<b>RESPUESTAS</b>	<b>%</b>
De 0 a 10%	0	0
De 11 a 20%	5	16.67
De 21 a 50%	0	0
De 50 a 100%	25	83.3

Fuente: Elaborado por la tesista

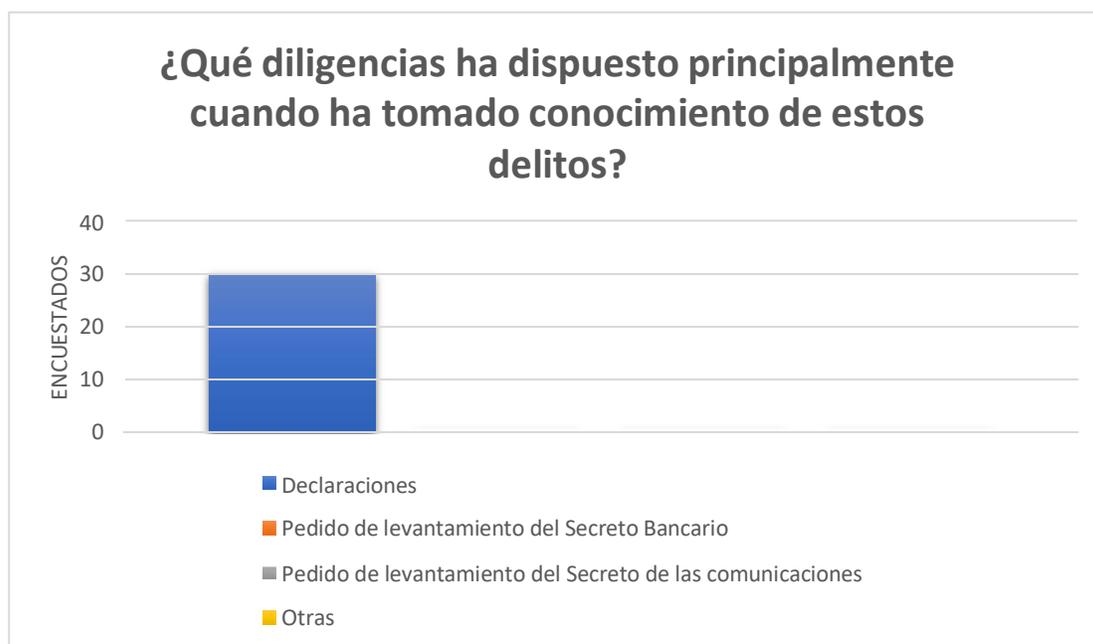


**Figura 1.** Cantidad de denuncias vistas durante el transcurso de la vida laboral

**PREGUNTA N° 4:** ¿Qué diligencias ha dispuesto principalmente cuando ha tomado conocimiento de estos delitos?

<b>ALTERNATIVAS</b>	<b>RESPUESTAS</b>	<b>%</b>
Declaraciones	30	100
Pedido de levantamiento del Secreto Bancario	0	0
Pedido de levantamiento del Secreto de las comunicaciones	0	0
Otras	0	0

Fuente: Elaborado por la tesista

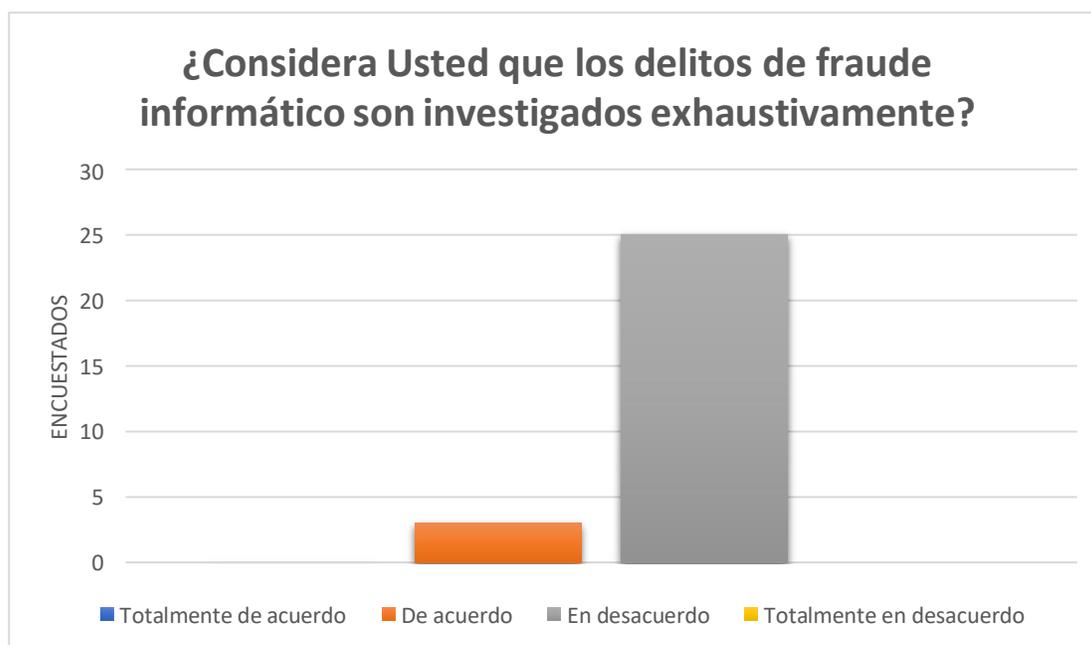


**Figura 3.** Diligencias realizadas en la investigación del delito de fraude informático

**PREGUNTA N° 5:** ¿Considera Usted que los delitos de fraude informático son investigados exhaustivamente?

<b>ALTERNATIVAS</b>	<b>RESPUESTAS</b>	<b>%</b>
Totalmente de acuerdo	0	0
De acuerdo	3	10
En desacuerdo	25	83.33
Totalmente en desacuerdo	2	6.67

Fuente: Elaborado por la tesista

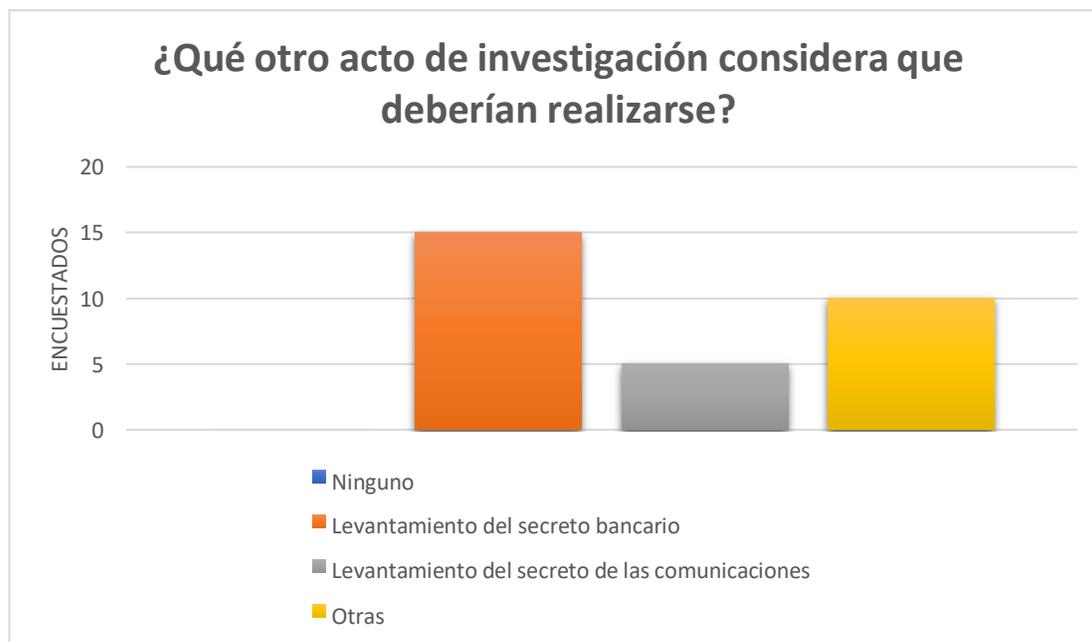


**Figura 5.** Nivel de conformidad respecto a la forma de investigación de los delitos de fraude informático

**PREGUNTA N° 6:** ¿Qué otro acto de investigación considera que deberían realizarse?

ALTERNATIVAS	RESPUESTAS	%
Ninguno	0	0
Levantamiento del Secreto Bancario	15	50
Levantamiento del Secreto de las comunicaciones	5	16.67
Otras	10	33.33

Fuente: Elaborado por la tesista

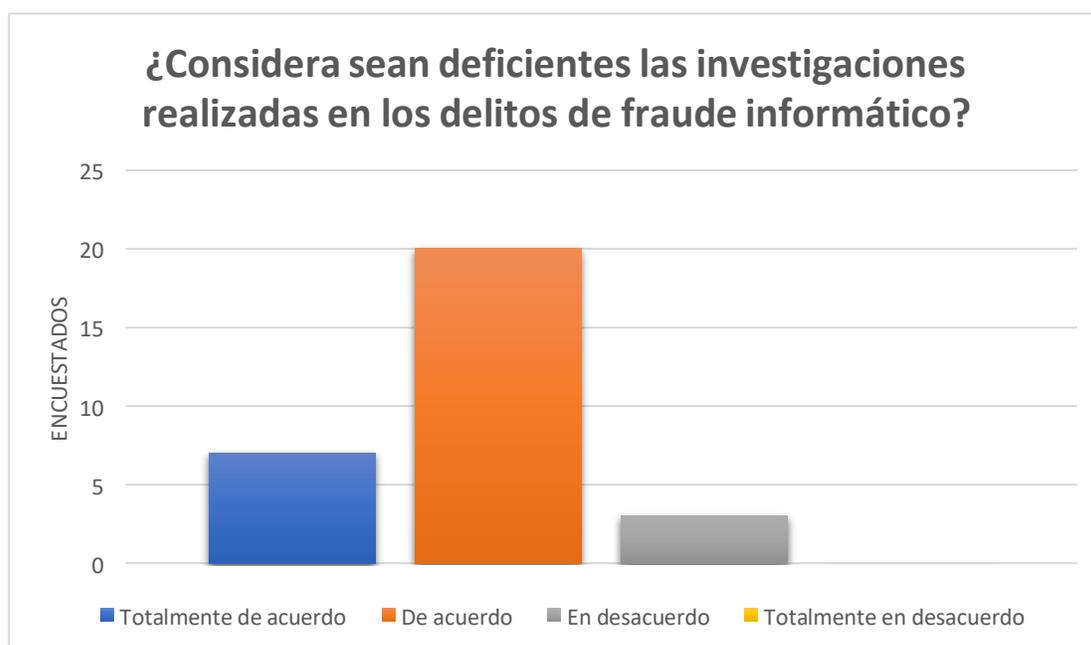


**Figura 6.** Actos adicionales a realizarse durante la investigación de delitos de fraude informático

**PREGUNTA N° 7:** ¿Considera sean deficientes las investigaciones realizadas en los delitos de fraude informático?

ALTERNATIVAS	RESPUESTAS	%
Totalmente de acuerdo	7	23.33
De acuerdo	20	66.67
En desacuerdo	3	10
Totalmente en desacuerdo	0	0

Fuente: Elaborado por la tesista

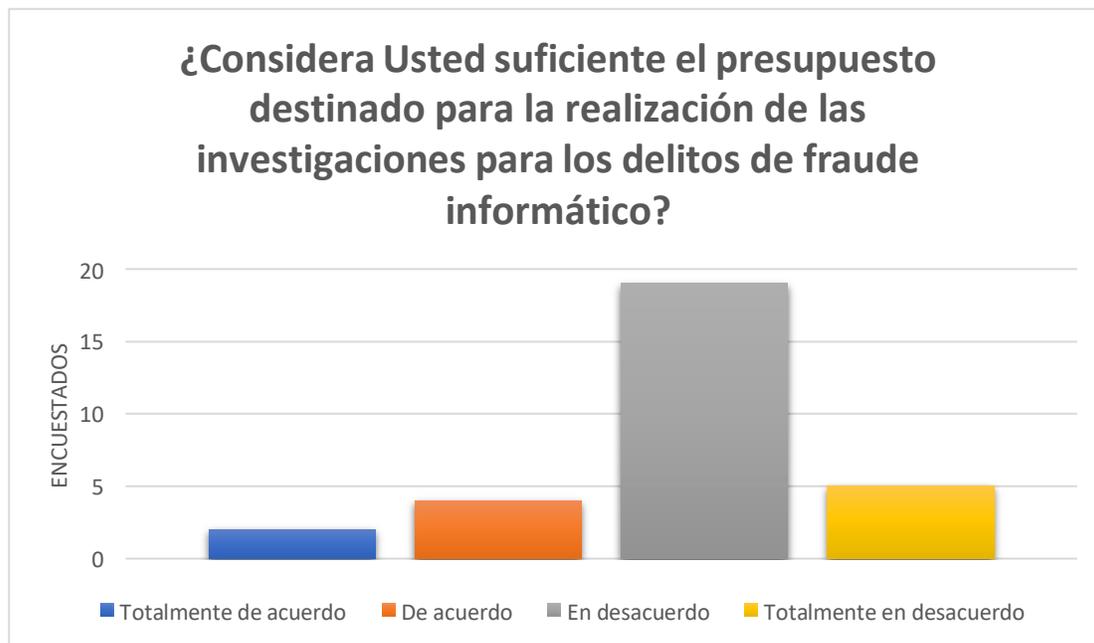


**Figura 7.** Nivel de conformidad respecto a la suficiencia de actos de investigación realizados en los delitos de fraude informático

**PREGUNTA N° 8:** ¿Considera Usted suficiente el presupuesto destinado para la realización de las investigaciones para los delitos de fraude informático?

<b>ALTERNATIVAS</b>	<b>RESPUESTAS</b>	<b>%</b>
Totalmente de acuerdo	2	6.67
De acuerdo	4	13.33
En desacuerdo	19	63.33
Totalmente en desacuerdo	5	16.67

**Fuente:** Elaborado por la tesista



**Figura 8.** Presupuesto destinado para la investigación de los delitos de fraude informático

**PREGUNTA N° 9:** ¿Considera Usted que es suficiente el plazo otorgado por ley para la investigación de los delitos de fraude informáticos?

<b>ALTERNATIVAS</b>	<b>RESPUESTAS</b>	<b>%</b>
Totalmente de acuerdo	0	0
De acuerdo	16	53.33
En desacuerdo	14	46.67
Totalmente en desacuerdo	0	0

Fuente: Elaborado por la tesista



**Figura 9.** Plazo otorgado a las investigaciones por el delito de fraude informático

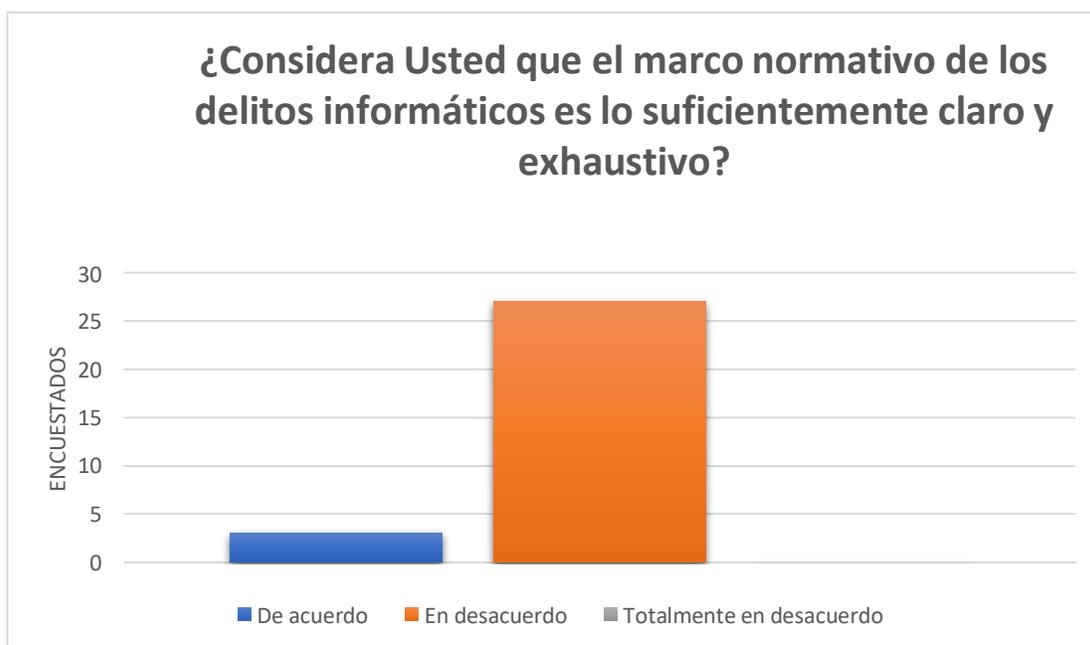
**PREGUNTA N° 10:** ¿Considera Usted que el marco normativo de los delitos informáticos es lo suficientemente claro y exhaustivo?

---

<b>ALTERNATIVAS</b>	<b>RESPUESTAS</b>	<b>%</b>
Totalmente de acuerdo	0	0
De acuerdo	3	10
En desacuerdo	27	90
Totalmente en desacuerdo	0	0

---

Fuente: Elaborado por la tesista



**Figura 10.** Marco normativo de los delitos informaticos

**PREGUNTA N° 11:** ¿Considera Usted que la Prueba Digital tiene mayor dificultad de obtención respecto a la prueba en un delito común?

<b>ALTERNATIVAS</b>	<b>RESPUESTAS</b>	<b>%</b>
Totalmente de acuerdo	2	6.67
De acuerdo	28	93.33
En desacuerdo	0	0
Totalmente en desacuerdo	0	0

Fuente: Elaborado por la tesista

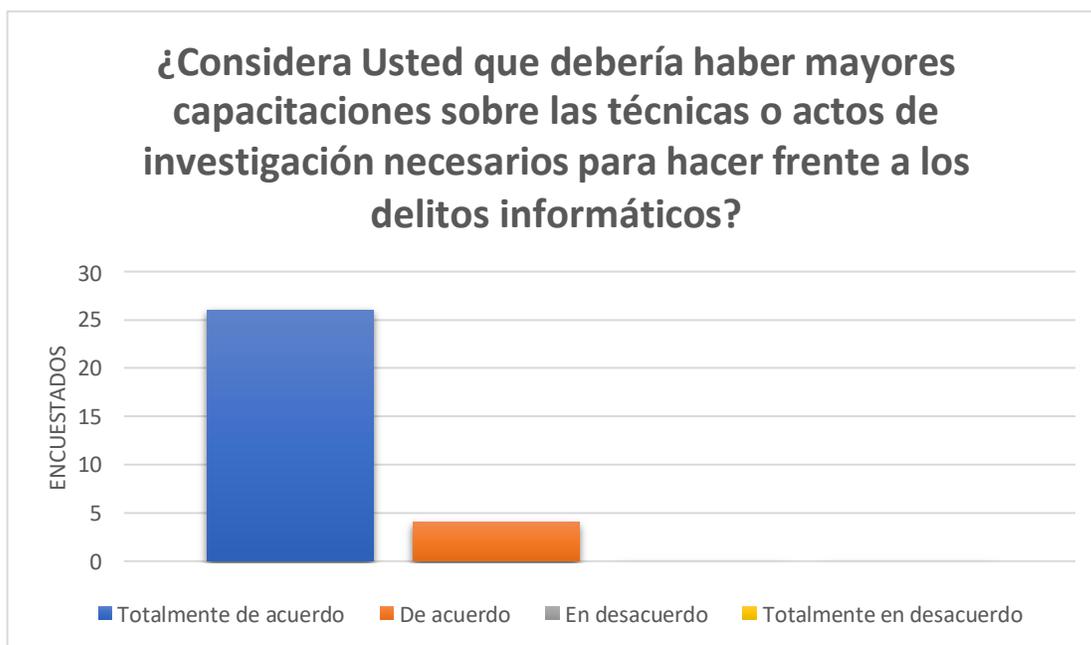


**Figura 11.** La dificultad de la prueba digital en los delitos de fraude informático

**PREGUNTA N° 12:** ¿Considera Usted que debería haber mayores capacitaciones sobre las técnicas o actos de investigación necesarios para hacer frente a los delitos informáticos?

<b>ALTERNATIVAS</b>	<b>RESPUESTAS</b>	<b>%</b>
Totalmente de acuerdo	26	86.67
De acuerdo	4	13.33
En desacuerdo	0	0
Totalmente en desacuerdo	0	0

**Fuente:** Elaborado por la tesista

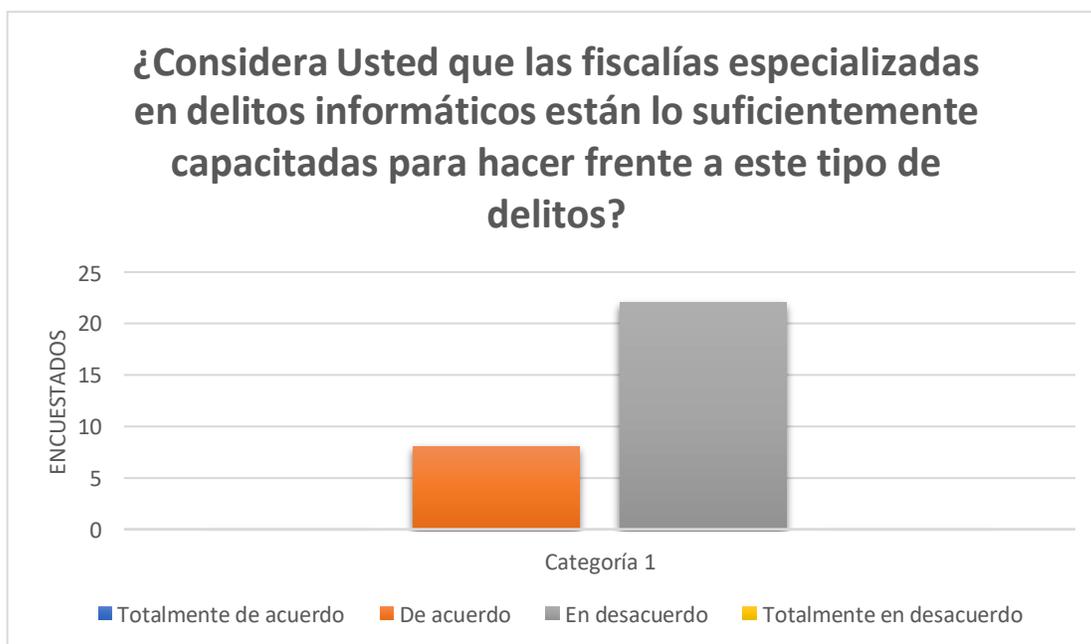


**Figura 12.** Capacitaciones sobre las técnicas o actos de investigación en los delitos de fraude informático

**PREGUNTA N° 13:** ¿Considera Usted que las fiscalías especializadas en delitos informáticos están lo suficientemente capacitadas para hacer frente a este tipo de delitos?

<b>ALTERNATIVAS</b>	<b>RESPUESTAS</b>	<b>%</b>
Totalmente de acuerdo	0	0
De acuerdo	8	26.67
En desacuerdo	22	73.33
Totalmente en desacuerdo	0	0

Fuente: Elaborado por la tesista

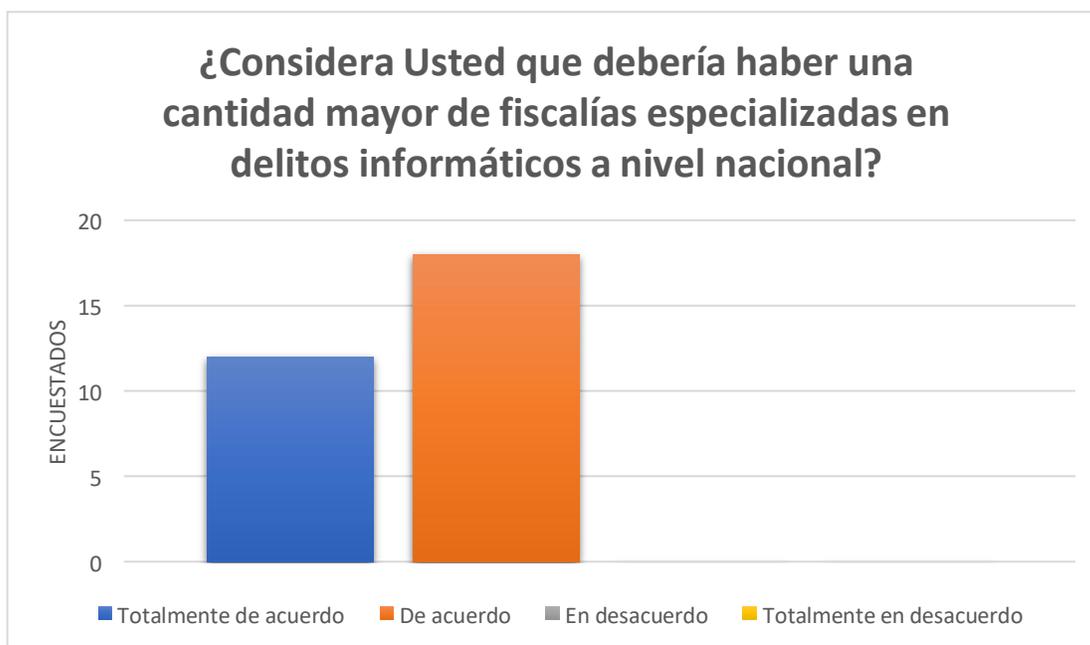


**Figura 13.** Fiscalías especializadas en delitos informáticos

**PREGUNTA N° 14:** ¿Considera Usted que debería haber una cantidad mayor de fiscalías especializadas en delitos informáticos a nivel nacional?

<b>ALTERNATIVAS</b>	<b>RESPUESTAS</b>	<b>%</b>
Totalmente de acuerdo	12	40
De acuerdo	18	60
En desacuerdo	0	0
Totalmente en desacuerdo	0	0

Fuente: Elaborado por la tesista



**Figura 14.** Cantidad de fiscalías especializadas en los delitos de fraude informático

**PREGUNTA N° 15:** ¿Considera Usted que debería haber una mayor Cooperación Internacional en la lucha Contra estos delitos informáticos?

ALTERNATIVAS	RESPUESTAS	%
Totalmente de acuerdo	26	86.67
De acuerdo	4	13.33
En desacuerdo	0	0
Totalmente en desacuerdo	0	0

Fuente: Elaborado por la tesista



**Figura 15.** Cooperación Internacional en la lucha Contra los delitos informáticos

## **4. ANALISIS Y DISCUSIÓN**

Ahora se desarrollan los resultados obtenidos mediante el empleo de la técnica de análisis documental y de la encuesta realizada.

### **4.1. Análisis y discusión de la técnica análisis documental**

Conforme se desprende del cuadro N°01, con relación a las definiciones de Fraude Informático se tiene que una primera definición fue proporcionada por el Convenio de Budapest, el cual establece los alcances del delito de Fraude Informático en su art. 8. El delito de fraude informático también es conocido como criminalidad mediante computadoras, delincuencia informática, delincuencia informática y criminalidad informática, y se define desde un punto de vista estricto al estar vinculado a acciones como la de diseñar, introducir, alterar, borrar, suprimir, clonar datos informáticos o manipular el funcionamiento de un sistema informático, de un perjuicio de índole económico para la persona titular de la fuente informática, y desde un punto de vista amplio al incluirse al interior del fraude informático conductas que no crean un perjuicio patrimonial directo, sino la obtención de información. Las características más relevantes del delito objeto de estudio son: la intangibilidad de los datos informáticos, el anonimato que favorece a las personas que están detrás de estos delitos, la dificultad en la obtención de las pruebas, los desafíos no solo físicos sino también jurídicos en el seguimiento, procesamiento y enjuiciamiento de estos delitos, cuya persecución y sanción debe ser tratado a nivel internacional.

Con respecto al cuadro N° 02 tenemos las definiciones de actos de investigación, resultando oportuno realizar una distinción entre actos de investigación y actos de prueba, teniendo los primeros la tarea de observar, identificar, recaudar, analizar y obtener los medios probatorios necesarios para

sustentar la posición de las partes en el juicio oral, material probatorio que al ser llevado a juicio es considerado prueba y que sirve no solo de sustento a la teoría de las partes sino es el sustento básico de toda decisión judicial. Los actos de investigación se encuentran justificados en la necesidad de encontrar elementos materiales probatorios, en ese sentido restringen derechos y garantías fundamentales solo cuando sean necesarios y trascendentes en respeto y observando las normas constitucionales y legales impuestas. Estos actos de investigación son llevados a cabo por la Fiscalía, quien en colaboración con peritos y policías se encargan de recabar todo el material probatorio necesario para esclarecer los hechos y determinar la autoría y responsabilidades de los implicados.

En el cuadro N° 03 se realiza un análisis comparado del delito objeto de estudio en algunos países vecinos y europeos, en ese sentido encontramos que España es considerado como una tipología de cibercrimen, conocido también como estafa telemática y estafa por computación, para lograr su fin se emplean medios informáticos y medios para realizar transferencias de recursos económicos a favor del autor del hecho y se encuentra regulado al interior del Código Penal Español de 1995 en su artículo 248 numeral 2, siendo considerado como una modalidad de estafa, así también mediante la L.O. 15/2003 se introdujo un tercer párrafo que considera como sancionable los actos preparatorios en el fraude informático. La particularidad de estos delitos es que se actúa de oficio y no a impulso de parte.

En la legislación italiana se tiene que mediante Ley N° 57 del 23 de diciembre de 1993 se introdujo las distintas tipologías de agresiones informáticas, la más semejante a la figura delictiva de fraude informático es la denominada en dicha legislación como “frode informático” que prevé en su artículo 640ter del Código Penal que quien emplee o afectar el funcionamiento de un sistema informático o telemático o entorpecer sin derecho alguno sobre

las informaciones o programas de un sistema informático o telemático procurando para si o para otro será castigado con reclusión de 6 a 3 años y con multa de 51 a 1032 euros. Estos delitos tienen como peculiaridad que a diferencia de la Legislación Española aquí necesariamente debe haber una querrela previa del ofendido para que se mueva el aparato estatal.

En Sudamérica se tiene a la legislación argentina la que no conocemos al delito como fraude informático sino como estafa informática prevista y sancionada en el art. 173 inciso 16 del Código Penal Argentino estableciendo que esta acción consiste en cometer fraude a otro mediante cualquier técnica de manipulación informática apta para producir dicho efecto.

En el país vecino Chile no existe aún un delito específico que incorpore como tal al delito de fraude informático, sin embargo en la Ley N° 19223, establece figuras típicas mediante el empleo y uso de herramientas informáticas, la misma que establece 4 conductas típicas relacionadas al sistema de información que son objeto de sanción: el que maliciosamente destruya o inutilice, impida o obstruir o varia su funcionamiento; el que mediante ánimo de apoderarse, usa o conoce o bien interfiera o acceda a él; el que maliciosamente altere o dañe o destruya la información; quien dolosamente revela o bien difunda información contenida en un sistema de información.

En Colombia en el año 2009 se promulgó la Ley N° 1273, la misma que incorpora distintas modalidades de delitos informáticos tales como la obstrucción ilegítima a un sistema informático, la interceptación de información contenida en soportes informáticos, la intervención abusiva a un sistema informático, la alteración de un informático, el uso doloso de programas, la vulneración de información personal, el hurto por medios informáticos y semejantes, la transferencia sin autorización de fondos personales, y otros. Pudiendo concluir que las figuras que más se asemejan al

delito de fraude informático, son el art. 269-I que prevé el Hurto por medios informáticos y semejantes y el art. 269-J que prevé las transferencias no consentidas de activos, tipos penales que buscan obtener un provecho ilícito mediante el uso de herramientas informáticas.

Ahora, pasare a analizar la información relativa a las carpetas fiscales que ingresaron en los Despachos Penales de la Fiscalía Provincial Penal Corporativa de Lurín, en el Distrito Fiscal de Lima Sur durante el año 2021.

Con respecto a la tabla N° 01, se puede ver el número total de denuncias ingresadas y asignadas por Despacho Fiscal e ingreso total de denuncias en la Corporativa Penal de Lurín, sumando un total de 71 de denuncias ingresadas en el año 2021.

En la tabla N° 02 se puede verificar la cantidad de denuncias atendidas de manera individual por cada Despacho Fiscal, así como la cantidad total de denuncias atendidas en la Corporativa Penal de Lurín, sumando un total la cantidad de denuncias que han sido atendidas durante el año 2021.

Realizando un análisis comparativo entre la tabla 01 y la tabla 02 podemos afirmar que el total de denuncias que ingresaron fueron atendidas en su totalidad durante el año 2021.

En la tabla N° 03 tenemos la cantidad de denuncias archivadas durante el año 2021 de manera individual por Despacho Fiscal, así como el total, siendo este último 57 las denuncias que han sido archivadas durante el año 2021

La tabla N° 04 nos muestra cantidad de denuncias consentidas durante el año 2021 de manera individual por Despacho Fiscal, así como el total, siendo

este último 54 las denuncias que han sido archivadas y consentidas durante el año 2021

Realizando nuevamente un análisis comparativo de la tabla 03 y 04 se puede ver que en su totalidad 54 han sido archivadas y consentidas, sin embargo 03 aún quedan pendiente por consentir. Asimismo, se puede verificar que, de las 71 denuncias ingresadas durante el año 2021 en la Fiscalía Provincial Penal Corporativa de Lurín, 57 han sido ya archivadas, lo que equivale a un 80% de las denuncias que se recibieron.

La tabla N° 05 muestra la cantidad de denuncias que han sido formalizadas tanto de manera individual como Despacho como en su totalidad la Corporativa Penal de Lurín, sumando un total de 0 las denuncias que han sido formalizadas durante el año 2021.

En la tabla N° 06 tenemos la cantidad de denuncias ingresadas y sobre las que se ha formulado acusación durante el año 2021 de manera individual por Despacho Fiscal, así como el total considerándolo como Corporativa Penal de Lurín, sumando un total de 0.

Realizando nuevamente un análisis comparativo de la tabla 05 y 06 se puede ver que ninguna denuncia ingresada durante el año 2021 ha sido formalizada ni se ha presentado acusación alguna, sumando inclusive 0 ambas informaciones.

#### **4.2 Análisis y discusión de la técnica encuesta**

En base a los resultados estadísticos recabados de la encuesta, se tiene que, de la primera pregunta formulada, se observa según el gráfico N° 01 que

el 66.67% de los especialistas encuestados han conocido un aproximado de 20 a 50 denuncias por el delito de fraude informático durante el transcurso de su vida laboral en el Despacho donde labora, mientras que el 33.33% de los especialistas ha respondido haber visto entre 10 a 20 denuncias durante el transcurso de su vida laboral en el Ministerio Público. Habiéndose entrevistado a personal Fiscal en función que labora desde hace al menos 01 año en la Institución, por ello es razonable que la cantidad de denuncias no sean actualmente las que priman en estos Despachos, sin embargo, es necesario precisar que dichas denuncias se encuentran en constante aumento a nivel nacional en todos los Distritos Fiscales, siendo los delitos Contra el Patrimonio, en particular el delito de fraude informático el que tiene mayor incidencia entre los delitos informáticos, situación que se refleja no solo en los Despachos de la Fiscalías de Lima Sur sino a nivel nacional conforme a los boletines estadísticos del Ministerio Público.

Con respecto a la pregunta N° 02, se observa que el 100% de los especialistas encuestados indican que las denuncias formalizadas han sido entre el 0 al 10% de los casos vistos, lo que denota que la totalidad de los especialistas encuestados no han formalizado las denuncias ingresadas y que le fueron asignadas. De lo que se colige que las denuncias son principalmente archivadas.

Con respecto a la pregunta N° 03, el 83.3% de las personas encuestadas indica que el porcentaje de las denuncias archivadas han sido entre el 50 al 100% de las denuncias vistas, sin embargo, solo el 16.67% de las personas encuestadas ha indicado que las denuncias archivadas han sido entre el 11 y el 20% de casos vistos. De lo que se desprende que las denuncias en su gran mayoría son principalmente archivadas, no pudiéndose arribar a identificar las responsabilidades de los investigados por estos ilícitos penales, generando un perjuicio económico irreparable para las personas afectadas.

Con respecto a la pregunta N° 04, el 100% de los especialistas encuestados manifiesta que las diligencias que han realizado durante sus investigaciones por el delito de fraude informático han sido únicamente declaraciones. Situación que pone de manifiesto que las diligencias que se actúan en estos delitos se basan únicamente en declaraciones, sin tenerse en consideración la complejidad del delito y otros actos de investigación que podrían realizarse a fin de determinar los hechos, autorías y responsabilidades.

Con relación a la pregunta N° 05, el 83.33% de los especialistas encuestados afirman que se encuentran en desacuerdo en afirmar que los delitos de fraude informático son investigados exhaustivamente, el 10% de los encuestados está de acuerdo en afirmar que los delitos de fraude informático son investigados exhaustivamente, mientras que el 6.67% sostiene que está totalmente en desacuerdo en afirmar que los delitos de fraude informático son investigados exhaustivamente. De lo que se desprende que en su mayoría los especialistas no están de acuerdo en sostener que los delitos de fraude informático sean investigados exhaustivamente, de hecho, respecto a la pregunta anterior, el 100% de los encuestados confirma que únicamente se realizan diligencias tales como toma de declaraciones, diligencia que no es suficiente para esclarecer los hechos, generándose una deficiente investigación.

A la pregunta N° 06 formulada en la encuesta, el 50% de los especialistas en el tema afirman que como acto de investigación adicional que debería realizarse en una investigación por el delito de fraude informático es el Levantamiento del Secreto Bancario, el 33.33% sostiene que deberían realizarse otros actos de investigación sin especificarse precisamente a cuales hagan mención, mientras que el 16.67% afirma que debería de actuarse la diligencia de Levantamiento del Secreto de las comunicaciones. De dicho resultado se corrobora una vez más que los especialistas consideran que deban actuarse otras diligencias a las declaraciones que normalmente se practican,

tales como el levantamiento del secreto bancario, diligencia que permitiría verificar y dar seguimiento a los movimientos y transacciones que se hubieran generado, el levantamiento del secreto de las comunicaciones a fin de determinar si existen mensajes llamadas, entre las posibles personas sindicadas que puedan constituir elementos de convicción suficiente para determinar responsabilidades o bien ampliar las investigaciones.

En la pregunta N° 07 los especialistas están de acuerdo en afirmar en un 66.67% que las indagaciones realizadas en el marco de estos delitos son deficientes, el 23.33% está totalmente de acuerdo con que las investigaciones son llevadas a cabo de manera deficiente, mientras que solo un 10% está en desacuerdo en que las investigaciones sean llevadas de manera deficiente. Dichos resultados demuestran que los mismos especialistas en su gran mayoría sostienen que las investigaciones que se llevan a cabo durante la búsqueda del esclarecimiento de las denuncias por los delitos de fraude informático son deficientes al realizarse pocos actos de investigación, en efecto las declaraciones no son suficiente para esclarecer los hechos, teniendo en cuenta además la complejidad de los delitos informáticos, resultan relevante que se actúen otros actos de investigación ya mencionados anteriormente.

Por otro lado, a la pregunta N° 08 formulada el 63.33% está en desacuerdo en afirmar que el presupuesto destinado para la realización de las investigaciones para los delitos de fraude informático sea suficiente, asimismo el 16.67% está totalmente en desacuerdo en que sea suficiente el presupuesto destinado para la realización de las indagaciones de las denuncias presentadas por el delito de fraude informático, mientras que el 13.33% está de acuerdo en afirmar que el presupuesto destinado para las investigaciones de estos delitos es suficiente, y el 6.67% está totalmente de acuerdo. Un factor importante y determinante para el esclarecimiento de los hechos es el presupuesto que se destina para la realización de las investigaciones, al ser deficiente este elemento

y teniendo en consideración la complejidad del delito es un factor que influye negativamente en las investigaciones.

Respecto a la pregunta N° 09, el 53.33% considera en estar de acuerdo que es suficiente el plazo otorgado por ley para realizar las investigaciones de estos delitos, mientras que el 46.67% está en desacuerdo en afirmar que sea suficiente el plazo otorgado por ley para la indagación de los delitos de fraude informático. Concluyéndose que más del 50% de los especialistas considera ser suficiente el plazo que por ley se otorga a las investigaciones por estos delitos.

Con relación a la pregunta N° 10, el 90% de los especialistas que fueron encuestados están en desacuerdo en afirmar que es suficientemente claro y exhaustivo el marco normativo por los delitos informáticos vigente, mientras que el 10% está de acuerdo con que sea lo suficientemente claro y exhaustivo el marco normativo vigente en los delitos informático. En ese sentido, un factor adicional que contribuye a una adecuada persecución de estos delitos es el marco normativo que regula los delitos informáticos, sin embargo, éste no es lo suficientemente claro ni exhaustivo, lo que genera que se encuentren inclusive lagunas, contradicciones en su normativa actual. Siendo latente la existencia de combatir esta forma delictual, con medidas jurídico especializadas, que vayan más allá de los moldes tradicionales del derecho vigente y permitan la adopción de leyes precisas, oportunas y acordes con las exigencias actuales.

A la pregunta formulada N° 11, los especialistas en un 93.33% están de acuerdo en que la prueba digital tiene mayor dificultad de obtención respecto a la prueba en un delito común, en ese mismo sentido el 6.67% sostiene estar totalmente de acuerdo en que la obtención de la prueba digital tiene mayor complejidad respecto a la obtención de la prueba común. Sin lugar a duda, el delito de fraude informático acarrea mayores dificultades, en términos de

investigación, por ello debe ser necesariamente abordado de manera distinta a los delitos comunes, lo que implica una mayor especialización en los actos de investigación, técnicas especiales, mayores recursos económicos, fiscalías especializadas que se avoquen en dichos delitos.

En la pregunta N° 12, el 86.67% de las personas encuestadas se encuentran totalmente de acuerdo con que deberían realizarse más capacitaciones sobre las técnicas o actos de investigación necesarios para hacer frente a los delitos informáticos, asimismo el 13.33% están de acuerdo en que deberían realizarse mayores capacitaciones para el correcto abordaje e investigación de estos delitos. Los resultados demuestran que los especialistas necesitan capacitarse sobre todas las técnicas necesarias para realizar investigaciones exhaustivas en la persecución de los cibercrimenes, en ese sentido juega un papel importante las capacitaciones respecto a las técnicas especiales y actos de investigación a realizarse durante el esclarecimiento de estas denuncias.

Respecto a la pregunta N° 13, los especialistas están en desacuerdo en que la fiscalía especializada en delitos informáticos están lo suficientemente capacitadas para combatir los delitos informáticos, mientras que el 26.67% están de acuerdo en que las fiscalías se encuentran lo suficientemente capacitadas para hacer frente estos delitos. En su gran mayoría los especialistas afirman que, a pesar de existir fiscalías especializadas, no se está a la vanguardia, ni se va de la mano con el progreso de la tecnología, lo que tampoco permite que se persigan adecuadamente estos delitos.

A la pregunta N° 14 que se formuló, los especialistas en un 60% está de acuerdo con que debería haber una cantidad mayor de fiscalías especializadas en los delitos informáticos a nivel nacional, asimismo el 40% está totalmente de acuerdo en que debería haber una cantidad mayor de fiscalías especializadas

en la materia. En esa línea, con las respuestas dadas por los especialistas, pese a los avances que se han realizado con respecto a la implementación de la fiscalía especializada en cibercrímenes, aun se requiere de una mayor presencia y distribución en todo el país, siendo las fiscalías especializadas en la materia las más aptas para avocarse únicamente a estos delitos, y ello está justificado debido al alto índice de los delitos informáticos, en particular el delito de fraude informático que se ve incrementado con el pasar de los años en todo el territorio nacional.

Con respecto a la pregunta N° 15, el 86.67% de los especialistas están totalmente de acuerdo en afirmar que deberían actuarse medidas de cooperación internacional en la lucha contra los cibercrímenes, así también el 13.33% de los especialistas está de acuerdo en que debería haber una mayor cooperación entre Estados en la lucha contra estos delitos informáticos. Aunado a la complejidad que acarrea la persecución de estos delitos, que se traduce en la falta de identidad de las personas que cometen estos delitos al realizarse mediante el uso de herramientas informáticas, se suma la ubicación respecto a la comisión de los delitos, en ese sentido es vital que se realice una persecución unificada, teniendo en cuenta que los efectos de estos delitos se producen en lugares distintos respecto al lugar donde se origina o tiene lugar el autor, por lo que la cooperación internacional en la lucha de estos delitos es inevitable a fin de debilitar y reducir o erradicar los perjuicios de los delitos informáticos.

## 5. CONCLUSIONES Y RECOMENDACIONES

De los resultados conseguidos en la investigación se han sustraído las conclusiones que a continuación se exponen:

El delito de fraude informático, conocido también como criminalidad mediante el uso de computadoras, delincuencia informática o criminalidad informática, está relacionado a acciones que pueden ser un introducir, alterar, clonar, borrar, suprimir, o diseñar datos informáticos o manipular el funcionamiento de un sistema informático que genera un perjuicio económico en la persona que es titular de la fuente vulnerada, cuya característica principal es la intangibilidad de la información, el anonimato de los autores y las limitaciones jurídicas y físicas para su procesamiento.

En los delitos de fraude informático las indagaciones tienen como finalidad recabar las pruebas para generar certeza sobre la existencia de los hechos que se afirman, buscando efectivizar la responsabilidad jurídico-penal de los sindicados. No se habla de una prueba común, sino de la prueba digital, también llamada prueba electrónica o tecnológica, determinante para el esclarecimiento de estos ilícitos. En ese sentido, los medios de prueba digitales son recogidos en soportes electrónicos, como las computadoras, Tablet, laptops, teléfonos móviles, discos duros, USB, y son los modernos instrumentos tecnológicos que encierran información al interior de páginas web, mensajería instantánea, redes sociales, tales como Facebook y WhatsApp entre otros. Actualmente las personas dejan evidencias de los acontecimiento, hechos o dichos, en imágenes, textos, audios, videos, sonidos de voz y grabaciones que pueden ser objeto de pericias.

Resulta importante realizar pericias informáticas a los datos almacenados en estos dispositivos para que sean extraídos mediante un

procedimiento que permita asegurar la información y garantizar su cadena de custodia, con la finalidad de identificar al autor, la actividad llevada a cabo con el dispositivo, recuperar datos eliminados y toda la información publicada de internet.

Con relación al marco normativo nacional e internacional existe discrepancia respecto al termino correcto del delito, en países como España, se habla de estafa telemática o por computación y se sancionan también los actos preparatorios, delitos que revisten particularidad al impulsarse de oficio y no necesariamente a impulso de parte. En esa misma línea la legislación argentina también habla de estafa informática; en Colombia en vez existen distintas modalidades de delitos informáticos, donde se habla en vez de Hurto por medios informáticos. Como podemos ver cada legislación contempla para los delitos informáticos, distintas modalidades y existe cierta discrepancia respecto a la terminología, no encontrándose una legislación uniforme a nivel internacional sobre estas modalidades delictivas, donde en algunos países se denomina estafa informática, en otros hurtos informáticos, y en países como el nuestro se denomina de manera muy genérica fraude informático.

De las estadísticas obtenidas por los Despachos Fiscales objeto de análisis se concluye que las denuncias presentadas por el delito de fraude informático, son atendidas rápidamente, sin embargo, son casi en su totalidad archivadas, no existiendo acusación ni formalización de las denuncias que fueron presentadas durante el año 2021, estadísticas que son ratificadas por los mismos encuestados, quienes sostienen que las denuncias que han visto durante su vida laboral han sido en su gran mayoría archivadas, no siendo suficientes los actos de investigación que se disponen durante las diligencias primigenias.

En esa misma línea, los especialistas han opinado con respecto a las diligencias que se disponen durante la persecución de los delitos informáticos, concluyendo que es absolutamente insuficiente las diligencias que se realizan

actualmente, el 100% de los encuestados sostuvo que únicamente se toman declaraciones, se puede concluir entonces que los actos de investigación llevados a cabo durante las diligencias preliminares son insuficientes para el esclarecimiento de los delitos de fraude informático en el Distrito Fiscal de Lima Sur, durante el año objeto de estudio. Además, en los casos en que se disponen ciertas diligencias a nivel fiscal estas resultan no ser determinantes a fin de esclarecer o averiguar los hechos y los autores de dichos ilícitos, siendo por lo tanto las investigaciones dispuestas deficientes.

Las razones a la falta de exhaustividad durante las investigaciones en el delito de fraude informático son debidas principalmente a los escasos recursos destinados, a las dificultades en la obtención de la prueba electrónica, a la falta de capacitaciones sobre las técnicas especiales o actos de investigación idóneos a la averiguación de estos delitos, a la falta de fiscalías especializadas en delitos informáticos distribuidas a nivel nacional, a la falta de un marco normativo coherente, claro y exhaustivo y a la ausencia de una cooperación internacional uniforme en la materia.

Con relación al marco normativo vigente en la materia existen discrepancias respecto al termino correcto a emplearse, además al interior del mismo delito de fraude informático se incluyen varias modalidades de delitos, situación que hoy en día genera incertidumbre jurídica y dificultad para su persecución amparados en la norma penal confusa y no bien desarrollada como debiera ser, aunado a ello la complejidad que reviste la persecución de este ilícito penal cometido mediante el empleo de herramientas tecnológicas, cuya fuente principal de prueba es la prueba digital, aún muy poco estudiada y desarrollada en nuestra legislación o por la doctrina peruana.

Recomiendo dar mayor importancia a estos delitos que están en constante aumento en particular modo al delito de fraude informático, que está afectando el patrimonio de las familias y al Estado. El derecho no puede quedarse indiferente frente a los enormes avances de la tecnología de la

información y su uso indebido, más aún si con mayor frecuencia la prueba documental es recogida en soportes electrónicos. En esa línea es oportuno llevar a cabo una serie de medidas necesarias que doten de mayor capacidad y conocimiento especializado sobre los actos de investigación y los pasos o procedimientos para la obtención de la prueba electrónica a quienes están en primera línea al momento de investigar, siendo los órganos persecutores de estos delitos, Fiscalía y Policía Nacional principalmente.

Asimismo, se instauren a nivel nacional Fiscalías Especializadas en la materia, se revise nuevamente la normativa nacional vigente a fin de no abarcar en un tipo penal distintas modalidades delictivas, situación que genera actualmente impunidad. Y a las autoridades pedirles que realicen un trabajo conjunto con los otros Estados pertenecientes al Convenio de Budapest a fin de que se materialicen las cooperaciones internacionales en la materia, logrando identificar a los responsables independientemente del lugar donde se cometa el ilícito penal.

## **6. AGRADECIMIENTOS**

A Dios, por protegerme dándome vida y salud para alcanzar este objetivo. Gracias por bendecirme durante todos estos años.

A mi madre, quien siempre ha sido para mí un ejemplo de perseverancia. Muchas gracias por todo el esfuerzo, amor y enseñanzas. Nada sería posible sin tus sabias palabras, ni tu formación que fue y es aún hasta el día de hoy la base que me asiste día a día en cada paso que doy.

A los docentes de la Universidad donde transcurrí 6 largos años, gracias por la paciencia, me queda claro que sin disciplina no se logran los objetivos.

Agradecer a todos aquellos que hicieron parte de mi camino, gracias por estar a mi lado y por contribuir en mi formación, gracias por las lecciones de vida.

A cada uno de ustedes, mil gracias.

## 7. Referencias

- Acurio, D. S. (s.f.). *Delitos informáticos: generalidades*. Recuperado de [http://www.oas.org/juridico/spanish/cyb\\_ecu\\_delitos\\_inform.pdf](http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf)
- Carrera Peña, I. d. R. (2021). *Deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021* (Tesis de Maestría). Universidad Cesar Vallejo, Lima, Perú. Recuperado de [https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/71492/Carrera\\_PIDR-SD.pdf?sequence=1&isAllowed=y](https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/71492/Carrera_PIDR-SD.pdf?sequence=1&isAllowed=y)
- Condori Ccori, R. (2020). *Implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020* (Tesis de posgrado). Universidad Cesar Vallejo, Lima, Perú. Recuperado de [file:///C:/Users/x/Downloads/Condori\\_CR-SD.pdf](file:///C:/Users/x/Downloads/Condori_CR-SD.pdf)
- PdP. (30 de diciembre de 1993). Constitución Política del Perú. *Congreso Constituyente Democrático*. Perú
- Custodio Cumpa, Y. (2021). *Las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático* (Tesis de pregrado). Universidad Cesar Vallejo, Lima, Perú. Recuperado de [https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/74797/Custodio\\_CY-SD.pdf?sequence=1&isAllowed=y](https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/74797/Custodio_CY-SD.pdf?sequence=1&isAllowed=y)
- Dellepiane, A. (1994). *Nueva teoría de la prueba*, Santa Fe de Bogotá, Colombia: Editorial Temis S.A.
- Fernández, H (2014). *Manual de derecho informático*, Buenos Aires, Argentina: 1ª ed. Edición: Abeledo Perrot.
- Gracia Serrano, O. A. (2019). *Los actos de investigación en la etapa de investigación inicial del procedimiento penal acusatorio* (Tesis de pregrado). Universidad de

- Mexicali, Baja California. Recuperado de <https://repositorioinstitucional.uabc.mx/bitstream/20.500.12930/3679/1/DER018942.pdf>
- Grenni, L. R. (2018). *La previsión normativa del tipo penal de Grooming en la Argentina*. Recuperado de <https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf>
- Hidalgo Pazmiño, J.A. (2018). *Los delitos informáticos y su afectación sobre los bienes jurídicos* (Tesis de titulación). Universidad Católica de Santiago de Guayaquil, Ecuador.
- Mayer, L. (2020). El delito de fraude informático: concepto y delimitación. *Revista chilena derecho tecnológico* (vol. 9). Recuperado de [https://www.scielo.cl/scielo.php?script=sci\\_arttext&pid=S071925842020000100151](https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S071925842020000100151)
- Mendoza Rodríguez, I. C. (2021). *Los actos de investigación virtual y su impacto en el debido proceso en la Fiscalía Provincial Especializada en Delitos de Corrupción de Funcionarios Del Santa, 2020–2021* (Tesis de Maestría). Universidad Cesar Vallejo, Lima, Perú. Recuperado de [https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/73449/Mendoza\\_RIC-SD.pdf?sequence=1&isAllowed=y](https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/73449/Mendoza_RIC-SD.pdf?sequence=1&isAllowed=y)
- Montalvo Gabilano, L. R. (2020). *La investigación del delito de estafa y su archivamiento en el Ministerio Público sede Lima, 2018* (Tesis de pregrado). Universidad Cesar Vallejo, Lima, Perú. Recuperado de [https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/70671/Montalvo\\_GLR-SD.pdf?sequence=1&isAllowed=y](https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/70671/Montalvo_GLR-SD.pdf?sequence=1&isAllowed=y)
- Pardo Vargas, A. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018* (Tesis de Maestría). Universidad

- Cesar Vallejo, Lima, Perú. Recuperado de <https://repositorio.ucv.edu.pe/handle/20.500.12692/20372>
- Posada, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. Recuperado de <file:///C:/Users/x/Downloads/DialnetElCibercrimenYSusEfectosEnLaTeoriaDeLaTipicidad-6074006.pdf>
- Quiles Mollá, L (s.f.). *Las nuevas tecnologías como medio de prueba en el proceso penal* (Tesis de Maestría). Universidad Miguel Hernandez, Alicante, España. Recuperado de <http://dspace.umh.es/bitstream/11000/4226/1/TFG%20QUILES%20MOLL%C3%81%20LAURA.pdf>
- Quispe Huaylla, J. L. (2020). *La conducción jurídica del Ministerio Público en los actos de investigación del nuevo proceso penal – Perú* (Tesis de Maestría). Universidad Nacional Federico Villareal, Lima, Perú. Recuperado de <http://repositorio.unfv.edu.pe/handle/UNFV/4371>
- Reyna, L. (2015). *El Proceso Penal Acusatorio Fundamentos - Funcionamiento - Cuestiones trascendentes*. Recuperado de <https://bibliotecadigital.oducal.com/Record/KOHA-OAI-TEST:28586/Details>
- Rivera Collazos, G. (2019). *La ineficacia de los miembros de la policía nacional del Perú en la investigación del delito de violación de la libertad sexual - Tingo María, 2016 - 2017* (Tesis de pregrado). Universidad de Huánuco, Huánuco, Perú. Recuperado de <http://repositorio.udh.edu.pe/bitstream/handle/123456789/2189/RIVERA%20COLLAZOS%2c%20Gisela.pdf?sequence=1&isAllowed=y>
- Rodríguez Cerna, F. (2019). *Valoración de prueba indiciaria no postulada por el Fiscal y el tipo penal de conspiración al tráfico ilícito de drogas* (Tesis de pregrado). Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú. Recuperado de <https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/7913/BC428%20RODRIGUEZ%20CERNA.pdf?sequence=1&isAllowed=y>

- Tellez, J. (2003). *Derecho Informático*. Recuperado de <https://clauditha2017.files.wordpress.com/2017/09/derecho-informatico-cuarta-edicion-julio-tc3a9llez-valdc3a9z.pdf>
- Torres Sanchez, K. G. (2021). *Carencia de actos de investigación en el proceso inmediato en casos de flagrancia juzgados de investigación preparatoria Canta 2021* (Tesis de Maestría). Universidad Cesar Vallejo, Lima, Perú. Recuperado de <https://hdl.handle.net/20.500.12692/75297>
- Zarzosa Cadillo, E. S. (2018). *Tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao -2017* (Tesis de Maestría). Universidad Cesar Vallejo, Lima, Perú. Recuperado de <https://repositorio.ucv.edu.pe/handle/20.500.12692/21042>

## 10. Anexos

Anexo A: Encuesta

**Universidad San Pedro – Sede Huacho**

**Facultad de Derecho y Ciencias Políticas**

### **ENCUESTA REALIZADA AL PERSONAL FISCAL DE LAS FISCALIAS PROVINCIAL PENAL CORPORATIVAS DEL DISTRITO FISCAL DE LIMA SUR**

La presente encuesta está dirigida al personal que labora en los Despachos de la Fiscalía Provincial Penal Corporativa del Distrito Fiscal de Lima Sur, quienes ocupan el cargo de asistente administrativo, asistente en función fiscal, Fiscales adjuntos y Fiscales Provinciales que laboran desde hace más de 01 año en el Ministerio Público.

**Instrucciones:** Distinguido encuestado/a, el siguiente cuestionario presenta una serie de preguntas relacionadas a la importancia y relación de los actos de investigación en los delitos de fraude informático en el Distrito Fiscal de Lima Sur, preguntas todas relevantes únicamente para fines de investigación. Por lo que deberá pensar de manera razonada y responder de manera libre a las preguntas marcando con una cruz (x) la respuesta que sea de su agrado.

Se hace de su conocimiento, que el investigador garantiza el debido tratamiento y la confidencialidad de los valiosos datos aportados por usted, siendo esta información anónima.

1. ¿Cuántas denuncias por el delito de fraude informático ha visto en el transcurso de su vida laboral?
  - a. De 10-20
  - b. De 20-50
  - c. De 50-100
  - d. De 100 a más
  
2. ¿En qué porcentaje aquellas denuncias que ha investigado han sido formalizadas?
  - a. De 0 a 10%
  - b. De 11 a 20%
  - c. De 21 a 50%

- d. De 50 a 100%
3. ¿En qué porcentaje aquellas denuncias que ha investigado han sido archivadas?
- a. De 0 a 10%
  - b. De 11 a 20%
  - c. De 21 a 50%
  - d. De 50 a 100%
4. ¿Qué diligencias ha dispuesto principalmente cuando ha tomado conocimiento de estos delitos?
- a. Declaraciones
  - b. Pedido de levantamiento del Secreto Bancario
  - c. Pedido del levantamiento del Secreto de las comunicaciones
  - d. Otras
5. ¿Considera Usted que los delitos de fraude informático son investigados exhaustivamente?
- a. Totalmente de acuerdo
  - b. De acuerdo
  - c. En desacuerdo
  - d. Totalmente en desacuerdo
6. En base a la pregunta anterior, ¿Qué otro acto de investigación considera que deberían realizarse?
- a. Ninguna
  - b. Levantamiento del Secreto Bancario
  - c. Levantamiento del Secreto de las comunicaciones
  - d. Otras

7. ¿Considera sean deficientes las investigaciones realizadas en los delitos de fraude informático?
- a. Totalmente de acuerdo
  - b. De acuerdo
  - c. En desacuerdo
  - d. Totalmente en desacuerdo
8. ¿Considera Usted suficiente el presupuesto destinado para la realización de las investigaciones para los delitos de fraude informático?
- a. Totalmente de acuerdo
  - b. De acuerdo
  - c. En desacuerdo
  - d. Totalmente en desacuerdo
9. ¿Considera Usted que es suficiente el plazo otorgado por ley para la investigación de los delitos de fraude informáticos?
- a. Totalmente de acuerdo
  - b. De acuerdo
  - c. En desacuerdo
  - d. Totalmente en desacuerdo
10. ¿Considera Usted que el marco normativo de los delitos informáticos es lo suficientemente claro y exhaustivo?
- a. Totalmente de acuerdo
  - b. De acuerdo
  - c. En desacuerdo
  - d. Totalmente en desacuerdo

11. ¿Considera Usted que la Prueba Digital tiene mayor dificultad de obtención respecto a la prueba en un delito común?
- a. Totalmente de acuerdo
  - b. De acuerdo
  - c. En desacuerdo
  - d. Totalmente en desacuerdo
12. ¿Considera Usted que debería haber mayores capacitaciones sobre las técnicas o actos de investigación necesarios para hacer frente a los delitos informáticos?
- a. Totalmente de acuerdo
  - b. De acuerdo
  - c. En desacuerdo
  - d. Totalmente en desacuerdo
13. ¿Considera Usted que las fiscalías especializadas en delitos informáticos están lo suficientemente capacitadas para hacer frente a este tipo de delitos?
- a. Totalmente de acuerdo
  - b. De acuerdo
  - c. En desacuerdo
  - d. Totalmente en desacuerdo
14. ¿Considera Usted que debería haber una cantidad mayor de fiscalías especializadas en delitos informáticos a nivel nacional?
- a. Totalmente de acuerdo
  - b. De acuerdo
  - c. En desacuerdo
  - d. Totalmente en desacuerdo

15. ¿Considera Usted que debería haber una mayor cooperación internacional en la lucha contra estos delitos informáticos?
- a. Totalmente de acuerdo
  - b. De acuerdo
  - c. En desacuerdo
  - d. Totalmente en desacuerdo

Muchas Gracias por su valioso aporte.

Anexo B: Fichas de Validación

FICHA DE VALIDACIÓN

I. DATOS GENERALES:

TITULO: "Actos de Investigación y Tratamiento Normativo en los delitos de Fraude Informático, Distrito Fiscal de Lima Sur, 2021"	
Nombres y Apellidos	Luis Alberto Pecho Pecho
Institución donde labora	Ministerio Público
Cargo	Fiscal Adjunto
Autor del Instrumento	Shirley Carolina Tacache Rodriguez

II. ASPECTOS DE LA VALIDACIÓN

1. Deficiente	2. Baja	3. Regular	4. Buena	5. Muy buena
---------------	---------	------------	----------	--------------

INDICADORES	CRITERIOS	1	2	3	4	5
Claridad	Está formulado con lenguaje apropiado					X
Objetividad	Está expresado en conductas observables					X
Actualidad	Está acorde a los aportes recientes en la disciplina de estudio					X
Organización	Hay una organización lógica					X
Suficiencia	Comprende las dimensiones de la investigación en cantidad y calidad					X
Intencionalidad	Es adecuado para valorar la variable seleccionada					X
Consistencia	Está basado en aspectos técnicos y científicos					X
Coherencia	Hay relación entre indicadores, dimensiones e índices					X
Metodología	El instrumento se relaciona con el método planteado en el proyecto					X
Aplicabilidad	El instrumento es de fácil aplicación					X

III. OPINIÓN DE LA APLICABILIDAD

El instrumento evaluado responde a las características de las variables, indicadores y dimensiones de las variables a ser investigados, concluyendo que es apto para su aplicación.

Promedio de evaluación 5

IV. OBSERVACIONES

-----  
 -----  
 -----

FECHA: 27/05/2022

FIRMA: 

## FICHA DE VALIDACIÓN

### I. DATOS GENERALES:

TÍTULO: "Actos de Investigación y Tratamiento Normativo en los delitos de Fraude Informático, Distrito Fiscal de Lima Sur, 2021"	
Nombres y Apellidos	Lizbeth H. Guínez Velázquez
Institución donde labora	F.P.P.C. LURIN
Cargo	FISCAL ASESORA
Autor del Instrumento	Shirley Carolina Tacuche Rodríguez

### II. ASPECTOS DE LA VALIDACIÓN

1. Deficiente	2. Baja	3. Regular	4. Buena	5. Muy buena
---------------	---------	------------	----------	--------------

INDICADORES	CRITERIOS	1	2	3	4	5
Claridad	Está formulado con lenguaje apropiado				X	
Objetividad	Está expresado en conductas observables					X
Actualidad	Está acorde a los aportes recientes en la disciplina de estudio					X
Organización	Hay una organización lógica					X
Suficiencia	Comprende las dimensiones de la investigación en cantidad y calidad					X
Intencionalidad	Es adecuado para valorar la variable seleccionada					X
Consistencia	Está basado en aspectos teóricos y científicos					X
Coherencia	Hay relación entre indicadores, dimensiones e índices					X
Metodología	El instrumento se relaciona con el método planteado en el proyecto					X
Aplicabilidad	El instrumento es de fácil aplicación					X

### III. OPINIÓN DE LA APLICABILIDAD

El instrumento evaluado responde a las características de las variables, indicadores y dimensiones de las variables a ser investigados, concluyendo que es apto para su aplicación.

Promedio de evaluación

4,9

### IV. OBSERVACIONES

FECHA:

25/05/2022

FIRMA:



## FICHA DE VALIDACIÓN

### I. DATOS GENERALES:

<b>TÍTULO:</b> "Actos de Investigación y Tratamiento Normativo en los delitos de Fraude Informático, Distrito Fiscal de Lima Sur, 2021"	
<b>Nombres y Apellidos</b>	Luis PAUL SAMANIEGO RARRE
<b>Institución donde labora</b>	MUNICIPALIDAD PÚBLICA
<b>Cargo</b>	FISCAL PROSECUTOR
<b>Autor del Instrumento</b>	Shirley Carolina Tacuche Rodríguez

### II. ASPECTOS DE LA VALIDACIÓN

1. Deficiente	2. Baja	3. Regular	4. Buena	5. Muy buena
---------------	---------	------------	----------	--------------

INDICADORES	CRITERIOS	1	2	3	4	5
Claridad	Está formulado con lenguaje apropiado					X
Objetividad	Está expresado en conductas observables				X	
Actualidad	Está acorde a los aportes recientes en la disciplina de estudio				X	
Organización	Hay una organización lógica					X
Suficiencia	Comprende las dimensiones de la investigación en cantidad y calidad				X	
Intencionalidad	Es adecuado para valorar la variable seleccionada					X
Consistencia	Está basado en aspectos teóricos y científicos				X	
Coherencia	Hay relación entre indicadores, dimensiones e índices					X
Metodología	El instrumento se relaciona con el método planteado en el proyecto				X	
Aplicabilidad	El instrumento es de fácil aplicación				X	

### III. OPINIÓN DE LA APLICABILIDAD

El instrumento evaluado responde a las características de las variables, indicadores y dimensiones de las variables a ser investigados, concluyendo que es apto para su aplicación.

Promedio de evaluación 4.4

### IV. OBSERVACIONES

FECHA: 31/05/2022

FIRMA:



## FICHA DE VALIDACIÓN

### I. DATOS GENERALES:

TÍTULO: "Actos de Investigación y Tratamiento Normativo en los delitos de Fraude Informático, Distrito Fiscal de Lima Sur, 2021"	
Nombres y Apellidos	Karina Anastegui Rojas
Institución donde labora	Ministerio Público
Cargo	Fiscal Adjunta
Autor del Instrumento	Shirley Carolina Tacuche Rodríguez

### II. ASPECTOS DE LA VALIDACIÓN

		1. Deficiente	2. Baja	3. Regular	4. Buena	5. Muy bueno
INDICADORES	CRITERIOS	1	2	3	4	5
Claridad	Está formulado con lenguaje apropiado				X	
Objetividad	Está expresado en conductas observables				X	
Actualidad	Está acorde a los aportes recientes en la disciplina de estudio				X	
Organización	Hay una organización lógica					X
Suficiencia	Comprende las dimensiones de la investigación en cantidad y calidad					X
Intencionalidad	Es adecuado para valorar la variable seleccionada					X
Consistencia	Está basado en aspectos teóricos y científicos			X		
Coherencia	Hay relación entre indicadores, dimensiones e índices				X	
Metodología	El instrumento se relaciona con el método planteado en el proyecto				X	
Aplicabilidad	El instrumento es de fácil aplicación					X

### III. OPINIÓN DE LA APLICABILIDAD

El instrumento evaluado responde a las características de las variables, indicadores y dimensiones de las variables a ser investigados, concluyendo que es apto para su aplicación.

Promedio de evaluación: 4.3

### IV. OBSERVACIONES

FECHA: 25/05/2022.  
 FIRMA: 