FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

TESIS

EL TRATAMIENTO PENAL DE LOS DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO DE LAS PERSONAS NATURALES Y JURÍDICAS EN LA CORTE SUPERIOR DE JUSTICIA DEL SANTA - CHIMBOTE

PARA OPTAR EL TÍTULO PROFESIONAL

DE ABOGADO

Autor:

Bach. Delgado Benites, Francisco Javier
https://orcid.org/0000-0002-1263-3855

Asesora:
Mg. Delgado Fernández, Rosa Elizabeth
https://orcid.org/0000-0001-6995-3609

Línea de investigación:

Ciencias Jurídicas

Pimentel – Perú

2022

EL TRATAMIENTO PENAL DE LOS DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO DE LAS PERSONAS NATURALES Y JURÍDICAS EN LA CORTE SUPERIOR DE JUSTICIA DEL SANTA – CHIMBOTE

Aprobación del Jurado:

Mg. Cabrera Leonardini Daniel Guillermo

PRESIDENTE

Mg. Delgado Fernández Rosa Elizabeth

SECRETARIO

Mg. Rodas quintana Carlos Andree

VOCAL

DEDICATORIA

A mi madre Aurora Benites, que, a pesar de sus largos años, me motiva a lograr una nueva profesión.

A mi esposa Esther Camones Maldonado y mis hijos Francisco y Aurora Delgado Camones, quienes me han demostrado su apoyo, dedicación y perseverancia para lograr lo deseado.

In memorian a mi padre Francisco y mi hermana Elizabeth, quienes desde el cielo me guían mi camino para seguir adelante.

AGRADECIMIENTO

A los docentes de Facultad de Derecho y Humanidades de la Universidad Señor de Sipán, que con mucha dedicación fueron mis profesores durante los 5 años y medio que duró mi carrera profesional, así mismo al profesor Dr. Jorge Idrogo Pérez y mi asesora de tesis la Dra. Rosa Delgado Fernández.

A mi madre y hermanos, por su gran apoyo incondicional y confianza para hacer en mí un profesional del Derecho.

RESUMEN

La presente investigación tuvo como objetivo general determinar los efectos jurídicos de la modificatoria de la ley de delitos informáticos para proteger el patrimonio de las personas naturales y jurídicas en la Corte Superior de Justicia del Santa, Chimbote.

Para el cual, se utilizó métodos propios de la investigación. Se aplicó como técnica el cuestionario con su respectivo instrumento de recolección de datos, con el cual se recopiló información, llegándose a conclusiones precisas.

Se concluyó que el tratamiento penal de los delitos informáticos contra el patrimonio es deficiente, toda vez que no se percibe dentro de fraude informático todo los tipos o modalidades de delitos informáticos contra el patrimonio, generando una confusión en la interpretación de la norma que no permite la sanción efectiva de los delitos informáticos contra el patrimonio.

Se encomienda que el Congreso de la República modifique el Artículo 8 de Ley de delitos informáticos, así como debe tipificar los delitos informáticos contra el patrimonio, diferenciando claramente las modalidades, sean éstos los delitos de fraude, estafa, sabotaje o hurto informático, se debe crear fiscalías especializadas en delitos informáticos para velar el patrimonio de las personas naturales y jurídicas.

Palabras claves: Delito informático, tratamiento penal, patrimonio, fraude informático, estafa informática, sabotaje informático y hurto informático.

ABSTRACT

The general objective of this investigation was to determine the legal effects of the modification of the computer crime law to protect the assets of natural and legal persons in the Superior Court of Justice of Santa, Chimbote.

For which, own research methods were used. The questionnaire with its respective data collection instrument was applied as a technique, with which information was collected, reaching precise conclusions.

It was concluded that the criminal treatment of computer crimes against property is deficient, since all types or modalities of computer crimes against property are not perceived within computer fraud, generating confusion in the interpretation of the norm that does not allow the effective sanction of computer crimes against property.

The Congress of the Republic is entrusted to modify Article 8 of the Law on computer crimes, as well as to classify computer crimes against property, clearly differentiating the modalities, whether they are crimes of fraud, fraud, sabotage or computer theft, it must create specialized prosecutors for computer crimes to watch over the assets of natural and legal persons.

Keywords: Computer crime, criminal treatment, property, computer fraud, computer fraud, computer sabotage and computer theft.

ÍNDICE

I. INTRODUCCIÓN

Los delitos informáticos surgieron con el uso del computador que es un dispositivo electrónico digital capaz de memorizar, elaborar o recuperar información o datos. Es una herramienta muy técnica y sofisticada, de enorme aplicación práctica. Es la única máquina programable, tiene una capacidad instalada que constituye su sistema general para interpretar y determinar la magnitud de su aplicación objetiva, mediante la inserción de una serie de datos o instrucciones que constituyen los programas informáticos.

Actualmente, dentro de la llamada era de la revolución tecnológica o automatización que identifica al mundo contemporáneo desde la década de los 50 del siglo pasado, no existe un solo sector de la sociedad que no se vea afectado por la evolución alcanzada por la informática. Una de las principales causas de este fenómeno es el empleo generalizado y globalizado de la Internet, admitida como un sistema transnacional de comunicación que, gracias a unos estándares comunes y usando tecnologías y redes de telecomunicación, permite el intercambio y la creación de información mediante el uso de disímiles modalidades de comunicación en línea.

Todo este desarrollo tecnológico ha traído como consecuencia el cibercrimen o llamado también ciberdelincuencia a nivel internacional y nacional que engloba las actividades delictivas utilizando medios tecnológicos que tienen como fin atacar a personas, empresas, organizaciones y gobiernos con el objetivo de interrumpir sus procesos de trabajo, robar datos y realizar otros ataques por medio de sus dispositivos, entre otras cosas. Los ataques digitales, conocidos como ciberataques, son realizados por ciberdelincuentes utilizando para ellos sofisticados métodos y técnicas contra el patrimonio de personas naturales y jurídicas.

El objetivo de este trabajo de investigación es implementar políticas que ayuden a recoger notabilidad jurídica y académica, toda vez que trata de un tema de la actualidad que viven las todas personas naturales y jurídicas en el país, con relación de las infracciones informáticas hacia el patrimonio, que causa bastante daño.

Se evidencia que la actual Ley N° 30096, presenta desconocimientos en su fundamentación por lo que ocasiona desconcierto en los ejecutores de justicia y

los perjudicados, causando bastantes periodos que estas peligrosas infracciones no se revelen y no se pueda encontrar a los auténticos criminales.

1.1. Realidad Problemática.

1.1.1. A nivel Internacional

La informática comienza internacionalmente a mitad de los cincuenta del siglo pasado, la primera generación del computador se desplegó en los años de 1951 y 1958, eran computadores que trabajaban demasiadas lentas, demasiadas grandes y concebían considerable calor. Pero al pasar los tiempos el progreso de la informática no ha dejado de perfeccionar debido a las innovadoras tecnologías, teniendo en cuenta diversos componentes electrónicos.

Actualmente las TIC (tecnologías de la información y comunicación) desempeñan un rol definitivo en el progreso social y en la producción de las naciones. En los estados avanzados y otros en vías de adelanto, los gobiernos han concebido como herramientas que favorecen al beneficio de profundos propósitos nacionales, como columna de políticas nacionales y proyectos de avance. Las TIC son un mecanismo preciso para enfrentar problemas que nacen de la confusión del mundo actual, debido a estos resultados se ha abreviado la labor artesanal y en cierto tiempo la utilización del computador es imprescindible, ante esta irrefutable y enormemente significativa mejora florecen algunos aspectos perjudiciales como los acreditados delitos o infracciones informáticas.

Uno de las magnas contribuciones de la globalización fue el incremento de la utilización de nuevas tecnologías a nivel mundial, principalmente las que hacían rutina intensivamente del Internet. Agradecemos al avance tecnológico y los negocios en el ciberespacio, se excluyeron límites y percepciones de tiempo al admitir a las personas y las instituciones empresariales una comunicación o información rápida desde diversas partes y en el momento requerido. Así mismo, aportó beneficios en el área de salud, educación, comercio, trabajo y otros rubros que hallaron en la web un medio virtual para desplegarse a un equilibrio más eficaz.

En estos últimos tiempos la ciberdelincuencia es una dificultad internacional que asciende cada día. Internacionalmente se ha vivido secuelas como la inmovilización de trabajos en corporaciones e instituciones empresariales por medio de programas ransomware o secuestro de datos o información para conseguir utilidades.

La Convención de Budapest - Hungría (2001) que viene hacer la primera convención internacional de lucha frontal a la ciberdelincuencia, encuadrándose las nuevas infracciones o delitos informáticos, infracciones que son contra los sistemas informáticos, los datos, el patrimonio y la fe pública, la impunidad y libertad sexual y la intimidad y el secreto de las comunicaciones. La Convención establece esquemas legales, por lo que compete que las naciones afiliadas confirmen, por medio de una consideración reflexiva, si sus referidas leyes penales nacionales obedecen con este patrón o si se requieren correcciones para mejorar los estándares. Por lo tanto, es necesario afirmar que el tratado internacional, al constituir un estándar imperceptible que facilita su universalización, se induce solamente por el castigo de los comportamientos dolosos, es necesario indicar de aquellos realizados con sensatez y voluntad de ejecutar el acto condenable y de alcanzar el efecto pernicioso.

Así mismo, la ONU (2019) las TIC (tecnologías de la información y comunicación) erigieron circunstancias para los ciberdelincuentes y dieron término a un acrecentamiento del tipo y la diversidad de las infracciones o delitos ejecutados en el universo virtual y a través de ello. Como no se tiene montos representativos que expresen los resultados de estas infracciones, la OEA proyecta que la cibercriminalidad causa gastos de alrededor de 575,000 millones de dólares al año, cantidad que alcanza a personalizar el 0.5% del PBI universal y precisa que en América Latina y el Caribe estos gastos son de alrededor de 90,000 millones de dólares anuales. (OEA 2016, p. IX).

Los delitos informáticos han hecho que los países colindantes del Perú adopten algunas medidas para enfrentarse a este delito que está

incrementándose. Apreciamos las siguientes regulaciones de dichos países vecinos.

En el país del Ecuador la Ley Nº 67/2002 reglamenta las Firmas y Mensajes de datos y el Comercio Electrónico. Dicha norma, considera en el Capítulo I, Título V, inscrito "De las infracciones informáticas", el art. 57 alega lo siguiente. "Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley". En el subsiguiente artículo, añade y cambia diversos artículos del Código Penal, anexando diversas formas de las transgresiones informáticas.

El país de Colombia la Ley Nº 1.273, del 2009, cambia el Código Penal, instituyendo un novedoso bien jurídico providencial llamado "de la protección de la información y de los datos". Donde alega que dicho procedimiento legal rebusca resguardar totalmente los sistemas que usen las TIC. Por medio de esta afiliación, cita al Capítulo I, llamado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", de este modo se reglamenta una sucesión de apartados penales que inician en el Art. 269A hasta 269J. Además, se agrega el Art. 58, atendiendo como desventaja usual "si la realización de alguna de las conductas punibles, se realicen utilizando medios informáticos, electrónicos o telemáticos".

El vecino Brasil la Ley Nº 12.737, del año 2012, donde se orienta la categorización delictiva de las infracciones o delitos informáticos y otros. En su reglamento une innovaciones para los Art. 154-A, 154-B, así mismo, el 266 y 298. Sin embargo, la Ley Nº 11.829 sistematiza el Estatuto de la niñez y la adolescencia, con la finalidad de corregir en forma frontal la lucha de la fabricación, distribución y comercialización de pornografía infantil, además normalizar como infracción la obtención y posicionamiento del material y otras conductas concernientes a la pedofilia en la web.

En Bolivia la Ley Nº 1.768 hace una transformación al Código Penal. Donde agrega el Capítulo XI, Título XII, Libro Segundo del Código Penal, concerniente a "Delitos informáticos". Adentro de ese acápite,

se juntan dos Art. 363 bis y ter, en dichos párrafos se plasma algunas infracciones informáticas.

En el país del sur Chile la Ley Nº 19.223 dicha norma “Relativa a Delitos Informáticos”, donde reglamenta cuatro artículos, desde los cuáles se representan varias infracciones informáticas. La Ley Nº 20.009 regulariza el compromiso para las modalidades de hurto, robo y pérdida de tarjetas de crédito, en su argumento se penan algunos comportamientos coherentes con estos hechos. La Ley Nº 18.168 que fue reformada por diversos procedimientos, reglamenta de modo general las telecomunicaciones, añadiendo algunas características penales correspondiente a la captación o interferencia ilícita de signos de comunicación o información.

Algunos países sudamericanos como Argentina, Chile y Paraguay, están bien posicionados a este tipo de delitos informáticos, lo han entendido con mucha responsabilidad y han optado por crear fiscalías especializadas en delitos Informáticos.

1.1.2. A nivel Nacional

En Perú en el año 1994, se colocó el primer locutorio público de Internet por Red Científica Peruana (RCP) dicha Asociación fue en el año de 1991 con el objetivo de suscitar y ampliar el Internet en nuestro país. La empresa nacional Entel Perú que fue privatizada a la compañía Telefónica del Perú S.A.A. de España, comenzó a fomentar la utilización de Internet comercialmente en los domicilios peruanos desde el año 1996 con la prestación Infovía. Desde ahí sobrevino la popularización de los locutorios públicos en toda la patria desde el año 1999. La evolución de las TICs y su predominio en casi todos los rubros del aspecto social, ha florecido una serie de conductas ilegales, apelados delitos informáticos y desde ahí se dio el comienzo al surgimiento de los criminales informáticos conocido como cibercriminales o ciberdelincuentes en el país.

Los acelerados progresos en las TIC, han aperturado variados espacios a nuevos métodos delictivos que en el siglo pasado eran imposibles, las maniobras de las diversas computadoras, ahora con

objetivos lucrativos, el desarrollo de nuevas aplicaciones de software exterminadores de bases de datos, la introducción anónima y el empleo indebido de la información que perturba claramente la intimidad de las instituciones empresariales, principalmente de los ciudadanos, con su uso ilícito logran causar difíciles perjuicios, materiales, económicos, así mismo morales. No solo la importancia de los daños causados comúnmente por lo habitual, está en acción, eminentes sucesos que estas infracciones no alcancen a revelarse, como conocemos nos afrontamos a personas especializadas en delitos, expertos en informática que son idóneos de desaparecer todo vestigio de los hechos efectuados contra el patrimonio.

En Latinoamérica el Perú fue uno de las naciones que a comienzos de este siglo XXI presentó contenidos de delitos o infracciones informáticas en su Código Penal añadiendo artículos respectivos al acceso de modo ilícito de sistemas informáticos, base de datos y redes para lograr un provecho o crear perjuicios. Esta voluntad obtiene competencia y motivo de gestión nacional, sin obtener una contestación resuelta y segura cuando las infracciones son realizadas desde un lugar que está en el exterior del Perú.

En el siglo pasado el CPP no poseía capítulos afines con los Delitos Informáticos concretamente. En el año 2000, el 17 de julio, debido a la Ley Nº 27309 donde se añade al Título V un capítulo novedoso, X sobre Delitos Informáticos del Libro Segundo de dicho Código Penal; los artículos correspondientes a estos delitos son: Nº 207- A, 207- B y 207- C. Por lo tanto, el Art. Nº 207- A está caracterizado el hacking, espionaje o pirata informático; el Art. Nº 207- B el daño o sabotaje y el Art. Nº 207- C el modo agravada - agravantes.

Luego en el mes de mayo del 2012, aproximadamente 12 años, se logra presentar un proyecto legislativo para cambiar el Art. 207- C del CP añadiendo la infracción de robo de identidad virtual, y añadir un novedoso Art. 207- D concerniente a la infracción informática agravada. Es así que el actual CPP, en el Libro Segundo, en el acápite Especial. Delitos, Título V. Delitos contra el patrimonio. Capítulo X - Delitos Informáticos; los artículos concernientes a las infracciones

informáticas siendo los Art. Nº 207- A, 207- B, 207- C y 207- D.

Debido a dicha iniciativa se plantea una Ley de manera restringida a renovar y agregar un artículo nuevo; inicia una discusión de obtener una Ley que sea coherente de contemplar penalidades de las nuevas infracciones informáticas que se presenta a nivel nacional e internacional, consolidándose una nueva ley que se publicó el 2013, el 22 de octubre, en el diario oficial El Peruano, la Ley de Delitos Informáticos Nº 30096, derogándose los artículos 207-A, 207-B, 207-C y 207-D del CPP, floreciendo una Ley especial.

Al haber prosperado con las normalizaciones para sancionar las nuevas infracciones informáticas en el Perú, sin embargo, continúa en discusión y comentario de las personas expertas, tanto jurídicas y especialistas vinculados con las tecnologías informáticas, a finales del año 2013 se propuso la Ley 30171, una ley que cambia la Ley 30096, Ley de Delitos Informáticos.

Esta norma última plantea efectuar el cambio de los sucesivos Art. 2, 3, 4, 5, 7, 8 y 10 de la Ley Nº 30096, Ley de Delitos Informáticos, por indiscutible imprecisión o noción de su argumento en los artículos mencionados. En el año 2014, en febrero, el Congreso subscribió la innovación a Ley de Delitos Informáticos. En marzo de ese mismo año, fue publicado en El Peruano las transformaciones a los artículos alusivos mediante la Ley Nº 30171; asimismo se anuló el artículo 6 y se agregó un artículo nuevo el 12 a dicha Ley de Delitos Informáticos.

El propósito de la Ley Nº 30096 que se encuentra en vigencia es advertir y castigar los comportamientos ilícitos que alteran los bienes jurídicos y los sistemas informáticos de notabilidad penal, ejecutadas por medio del empleo de las TIC, cuyo objetivo es certificar la lucha frontal y eficiente contra la delincuencia informática.

El Jefe de Estado del Perú, certifica el “Convenio sobre la Ciberdelincuencia”, con DS (Decreto Supremo) Nº 010-2019-RE. En el Considerando dice: “Que, el “Convenio sobre la Ciberdelincuencia” fue amparado el 23 de noviembre de 2001 en la ciudad de Budapest, Hungría, y certificado por Resolución Legislativa N° 30913, de fecha 12 de febrero de 2019. Que, es beneficioso a los

intereses del Perú la ratificación del citado Convenio. De conformidad con lo dispuesto por los Art. 56° y 118° inciso 11 de la Constitución Política del Perú y el Art. 2 de la Ley Nº 26647".

En el Perú se registra casos de ciberdelitos contra el patrimonio en las instituciones empresariales y personas naturales que crearon enormes daños económicos en los postreros tiempos. El tratamiento penal, no regulariza del todo las conductas delictivas procedentes de la utilización de los denominados contactos virtuales (Internet, sitio web, Facebook, Instagram y otros); únicamente se toman en cuenta las infracciones informáticas, en ciertos procesos como representaciones concursales mediales, habiendo la infracción de falsedad pública o estafa, etc., las infracciones informáticas en el Perú han ido creciendo, se exhorta nuevas políticas para penar los sucesos delincuenciales con el manejo de la tecnología informática.

Según la información de la Oficina de Racionalización y Estadística, remitido a la OFAEC por medio del email el 18 de agosto de 2020, se toma como informe el periodo 2018 a julio 2020, siendo el 2018 (1652), 2019 (3215), julio del 2020 (1134), donde se registra el 37.8% (6001) de las infracciones informáticas se reconoce como infracción específica el Art. 8 (Fraude informático) de la Ley N°30096.

En el año 2020, las denuncias por infracciones informáticas se incrementaron en 39.78% en relación al año anterior. La División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la PNP reconoció más de 300 casos cada mes, la mayoría afines a suplantación de identidad, fraudes informáticos, y otros.

En total, se investigaron 4,162 casos en el 2020. Los meses con más denuncias registradas fueron setiembre y diciembre.

El Ministerio Público dispuso el 01 de enero del 2021 la creación de una Unidad Fiscal Especializada en Ciberdelincuencia, con competitividad nacional, tiene entre sus objetivos específicos cumplir la orientación técnico - jurídica en las indagaciones de los delitos cometidos por medios tecnológicos, desde la identidad y preservación de la certeza virtual, que obedecerá administrativa y operativamente de la Fiscalía de la Nación.

Dicho módulo fiscal, ha empezado a desempeñarse el 15 de febrero del 2021, donde ofrecerá un procedimiento especializado y un asesoramiento competente a los fiscales en la pesquisa de las infracciones informáticas y en procesos en los que la fabricación de prueba digital sea concluyente para la pesquisa.

Igualmente deberá consolidar juicios en las operaciones y estrategias de averiguación en materia de delincuencia informática, originar la estructuración entre el MP y la PNP, conjugar con las redes internacionales (CiberRed, RedCoop, AIAMP), eximir aclaraciones y presentar informes sobre el tema, entre otras funciones.

La Fiscalía de la Nación dispuso el funcionamiento de la Red de fiscales en ciberdelincuencia en todo el país, integrado por 64 fiscales (34 titulares y 30 alternos), que serán los puntos de relación entre los distritos fiscales y la mencionada unidad. Todos ellos compondrán la red en complemento a las funciones que actualmente vienen eximiendo.

1.1.3. A nivel Local

En Chimbote y toda la provincia del Santa, con la aparición del Internet y las TICs, se han acrecentado los delitos informáticos, por eso muchos especialistas informáticos, así mismo, criminólogos han promovido a notificar que la noción de los delitos informáticos debe modificarse porque las nuevas infracciones están siendo cometidas en diversos sitios virtuales consiguiendo aperturar nuevas líneas de indagación.

El diario El Correo de Chimbote menciona que la comisión de infracciones informáticas se ha desarrollado a partir que inició la pandemia sanitaria debido al COVID-19. Los últimos meses, el Departamento de Investigación Criminal (Depincri) de Chimbote ha recibido hasta 50 denuncias por este tipo de modalidad criminal**.** El jefe del Depincri, comdt. PNP José Santillán Pérez mencionó: “En esta pandemia han aumentado las infracciones informáticas, tenemos denuncias en diversas modalidades como son las compras por

Facebook en páginas que se denominan ‘mercado libre’, ‘venta de gamarra’, entre otras”.

En Chimbote existe otro modus operandi como la remisión de mensajes y la ejecución de llamadas telefónicas, donde los ciberdelincuentes requieren actualización de indagación personal y hacen entender a las personas que han obtenido una recompensa o un premio.

La infracción de fraude informático es la que más denuncias alcanzó, esencialmente por procedimientos o entregas electrónicas o de patrimonios no acreditados.

Los cibercriminales en Chimbote y en la provincia del Santa usan el phishing para mentir a los interesados con páginas simuladas que fingen ser las páginas web de las identidades financieras o bancos. Los perjudicados ingresan sus datos personales y, con esa información, las bandas criminales efectúan depósitos sin autorización de las cuentas bancarias.

La intensificación de los delitos informáticos ejecutados con las actuales tecnologías informáticas en estos tiempos, exige al gobierno a amparar una norma punitiva severa donde se acate el procedimiento constitucional que sustenta el Derecho Penal. Le corresponde perfeccionar las presentes tipificaciones penales conocidas en la Ley de Delitos Informáticos para no continuar utilizando términos confusos que admitan sancionar la actuación frecuente de las garantías civiles de las personas jurídicas y naturales.

Se debe promover la comunicación y el diálogo con las autoridades políticas, que permitirán engrandecer la lucha contra este nuevo flagelo delictivo internacional, nacional, regional y local para poder impedir que los cambios normativos se ejecuten a espaldas de las personas técnicas y sin la contribución u opinión ciudadana. Por otro lado, es necesario hacer partícipes esta plática con la sociedad civil, porque ellos son los están inseguros a estas infracciones y ellos serán los que revelen y ayuden con las autoridades para aclarar los sucesos punibles. Es indispensable promoverla para practicar

desenvueltamente los derechos e impulsar que se consideren las cauciones de las personas jurídicas y naturales.

Actualmente la provincia del Santa en lo referido a ciberdelincuencia, según la información de la Oficina de Racionalización y Estadística, remitido a la OFAEC por medio del email, fecha 18 de agosto de 2020 las denuncias por infracciones informáticas inscritas en Fiscalías Penales Comunes y Fiscalías Mixtas, de octubre 2013 a julio 2020 en del Santa, siendo la siguiente: 0 (2013), 3 (2014), 3 (2015), 6 (2016), 36 (2017), 20 (2018), 90 (2019), 27 (julio 2020), siendo un total de 185 denuncias, equivalente al 0.85% a nivel nacional.

1.2. Antecedentes de estudio.

1.2.1. A nivel Internacional

En relación al trabajo de indagación hay diferentes antecedentes a nivel internacional, dentro de ellos tenemos:

Quevedo (2017), efectuó la tesis *"*Investigación y prueba del ciberdelito*"* sustentada en el Programa de Doctorado en Derecho y Ciencia Política de la Universidad de Barcelona de España, para conseguir el grado académico de Doctor en Derecho, los propósitos de este trabajo de investigación son, primero especificar el concepto de este clase de delito o infracción y su respectiva regulación actual, sustantiva y procesal, y segundo, definir cómo guiar la indagació, estudiando los métodos fundamentales para la obtención de pruebas, los datos destacados en la indagación del hecho e identificación del responsable y cómo obtener los mismos con todas las garantías y respeto a los derechos primordiales para que pueda ser considerados como prueba sin el menor atisbo de falta de licitud o fiabilidad del material probatorio. (pp. 11, 12).

Con la cibercriminalidad, el Derecho Penal se enfrenta a una red delincuencial más organizada y dañina, que necesita de instrumentos procesales para hacerle frente, en el trabajo de investigación se puntualiza cómo debe realizarse las investigaciones con todas las

medidas y garantías de investigación, para servir de prueba ante los tribunales.

El investigador analiza disímiles procedimientos de cibercriminalidad que se realizan con demasiada continuidad, observándose el avance en técnicas, métodos o instrumentos que se han desarrollado para facilitar los delitos informáticos. En Colombia las normas faltan que alcance a comprender todos los recintos de seguridad informática, que causan daños en todos los medios de mejora y desarrollo de dicho país.

Según los autores Alarcón y Barrera (2017), ejecutaron la tesis “Uso de Internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016”, defendida en la Universidad Norbert Wiener, Escuela de Posgrado, para lograr el grado de Maestro en Informática Educativa, donde asumieron como objetivo de investigación, instaurar la concordancia del uso del Internet con las infracciones informáticas en los estudiantes colombianos.

La representación de las tecnologías actuales no consiguen ser ente de desilusión formativo y personal, estas conforman un medio para conseguir a un fin, por lo que resulta de importante valor examinar cual es la relación de la utilización del Internet y las infracciones informáticas, para saber los disímiles aspectos que se implican y a partir de este certificado delinear técnicas que surtan a los alumnos de materias que les faculta determinar el rol de la información que circula por Internet y sobre todo por las redes sociales, así como, lo que involucra hacer mal empleo de la información en la comisión de delitos informáticos. (pp.31, 34).

La utilización del Internet con fines de investigación académica se convierte en un aliado para el conocimiento, es necesario direccionar voluntades desde las instituciones educativas para fortalecer las competencias de información y de este modo favorecer al enfoque sistémico del empleo de la tecnología como medio necesario para el conocimiento científico y no hacer mal uso que implican cometer delitos.

Ruiz (2016), realizó la tesis titulada “Análisis de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos tiene como objeto dar una visión clara sobre los delitos informáticos en especial sobre la violación de los derechos constitucionales de los ciudadanos”, sostenida en la Universidad Nacional Loja - Ecuador. Para conseguir el Título de Abogada, cuya finalidad de la investigación es dar una visión precisa sobre infracciones informáticas en específico la violación de los derechos constitucionales de las personas que se crean por el uso de TIC, como las servicios financieros, comercio electrónico, el correo electrónico y el uso de las redes sociales; se examina y conceptualiza la naturaleza de los delitos informáticos y sus tipificaciones de acuerdo a sus particularidades principales y se constituyen opciones de soluciones para condenar las infracciones informáticas y evitar la vulneración de los derechos constitucionales del ofendido. (p. 2).

La legislación penal ecuatoriana, debe incluir en su normativa la caracterización de la infracción informática, como la intimidad personal y la usurpación de la información en las redes sociales y debe ser causa de sanción, las TIC actualmente están en constante adelanto y es necesario prevenir y así evitar la infracción informática.

Así mismo el autor Rincón (2015), plasmó la tesis “El delito en la cibersociedad y la justicia penal internacional” defendida en la Universidad Complutense de Madrid de España, Facultad de Derecho, para lograr el grado académico de Doctor, teniendo como propósito del estudio, plantear la plataforma de una obtención teórica desde el dogmatismo penal internacional que acceda dialogar sobre la necesidad de contener la investigación y juzgamiento de las infracciones informáticas, electrónicos y de las telecomunicaciones en la aptitud del estatuto de Roma. (p.21).

El investigador manifiesta que la utilización de las tecnologías y la coherencia de la ciencia admite establecer un nuevo modelo con el cual las personas entran en un nuevo periodo, de manera tal que la noción

y tecnología se cristianizan, prontamente, en el mejor socio de la manufactura de riqueza. El organismo mundial más apropiado que debe tener capacidad para corregir las infracciones informáticas siendo CPI (Corte Penal Internacional), y el procedimiento a prolongado término, como un sitio de inicio en el castigo internacional de las infracciones informáticas siendo la reforma del estatuto de Roma.

Por otro lado, Piccirilli (2015), hizo la tesis “Protocolos a aplicar en la forensia Informática en el marco de las nuevas tecnologías (Pericia – Forensia y Cibercrimen)” que defendió en la Universidad Nacional de La Plata, Facultad de Informática, con el desenlace de obtener el grado académico de Doctor en Ciencias Informáticas, teniendo el propósito este trabajo de investigación doctoral, desarrollar un proyecto metodológico para puntualizar reglas de base a emplear en la utilización de la forensia usada al procedimiento de la seguridad digital, en el escenario de las TICs.

La criminalidad ha descubierto en la cibernética una herramienta muy ventajosa para el cometido de diferentes clases de infracciones, pero además la justicia reconoce la utilidad de las pruebas digitales que pueden ser adquiridas a través de los instrumentos informáticos. Por ello, una conversación virtual entre personas a través de las redes sociales, o un archivo de texto, o una imagen una planilla de datos, o un correo electrónico, se han convertido en el propósito de análisis para constituir una verdadera “prueba”. (p.1).

El investigador argentino efectúa un estudio de la prueba desde la requisa hasta la examinación pericial útil, la perspectiva procedimental empleada en el desarrollo de la indagación que es analítica, asevera que es suficiente alto el nivel de la delincuencia informática, y que el permanente perfeccionamiento de la amenaza es la que estimula inventar nuevos hechos.

1.2.2. A nivel Nacional

Los trabajos previos de investigación a nivel nacional con respecto al problema objeto de investigación son los siguientes:

Soto (2019), formalizó la tesis “Regulación jurídica de la cooperación internacional en el marco del convenio de Budapest en el Perú” que sostuvo en la Universidad Andina del Cusco, Facultad de Derecho y Ciencia Política, con el fin de lograr el título de Abogado, donde está encaminado en la obligación de efectuar un apropiado sistema legal que nos admita compensar y abordar la dificultad de la cibercriminalidad, los textos de jurisdicción y sus leyes ajustables si bien es cierto no son novedosos; Internet transgrede los principios internacionales y otras normas que tradicionalmente se manejaban por la justicia para hacer frente a los problemas transfronterizos donde muchas veces nos encontramos con dificultades y limitaciones como los disímiles sistemas jurídicos o vacíos legales por lo que para procesar a los transgresores virtuales se requiere necesariamente de la cooperación internacional y regional. (p. v).

La investigación realizada por el autor trata sobre el Convenio de Budapest que tiene como intención fundamental concertar los procedimientos para la aprensión y seguimiento de las infracciones informáticas proponiendo un esquema pequeño donde se debe adoptar los medios necesarios para notificar la infracción penal en el Perú.

Según Tenorio (2018) hizo la tesis “Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia” sustentada en la Academia Diplomática del Perú “Javier Pérez de Cuéllar” del programa de Maestría en Diplomacia y Relaciones Internacionales, tuvo como objetivo proporcionar los transcendentales asuntos de ciberdelitos que ocurrieron desde comienzo de los años 90 y las pérdidas generadas por los mismos; así como: los trascedente del Convenio de Budapest sobre la Ciberdelincuencia para los Estados Parte; los retos a prevalecer tras una futura adhesión al Convenio y las circunstancias que serán de gran ayuda para la población, empresas e instituciones en el Perú, las cuales son más dependientes del ciberespacio y los servicios que están disponibles.(p. 2).

El estudio investigativo concluye que las TIC en este universo globalizado digital, donde se ofrece mejores instrumentos al estado para resguardar los datos y sistemas informáticos, la red de las personas jurídicas y naturales del Perú, donde se hace el empleo del Convenio de Budapest correspondiente a la ciberdelincuencia para constreñir el crimen informático sin límite.

Por otro lado, Hacco (2018), realizó la tesis titulada “La tipificación del bien jurídico protegido en la estructura del tipo penal informático como causas de su deficiente regulación en la Ley 30096, Perú – 2017” que defendió en la Universidad Nacional San Agustín de Arequipa, Facultad de Derecho, para conseguir el título de Abogado, se basa en el bien jurídico preservado en la organización de la clase penal informática como fundamentos de su defectuosa regulación en la Ley 30096, de modo, se asume como rastreo y revisión de los inconvenientes de espontaneidad y faltas de técnicas de redacción legislativa, que intentan regular a través de la ley especial, formas que en varios argumentos ya se encuentran resguardados en nuestro ordenamiento jurídico por otras tipos penales, así mismo, conseguimos suponer también que es inconveniente que la pena sea desproporcional respecto a otros ilegítimos análogos. (p. iii).
El trabajo realizado por el autor permite manifestar cómo la incompleta caracterización del bien legal que excede en la inexactitud de obligación, en la inexactitud de competitividad y en la exagerada figura de clase penal informática que sistematiza la Ley 30096 de las infracciones informáticas.

Según Romero (2017), realizó la tesis “Delitos informáticos cometidos a través de redes sociales y su tratamiento en el ministerio público en la ciudad de Huánuco, 2016” que sustentó en la Universidad de Huánuco, Facultad de Derecho y Ciencias Políticas, con el desenlace de lograr el Título de Abogada, donde describe las conductas que se pueden conocer como infracciones informáticas en las redes y como se está acomodando la legislación en el Perú, a este incremento continuo

de las TIC para prevenir, proteger y establecer una apropiada administración. Las actuales destrezas delictuosas en el Perú están a acorde del uso del avance tecnológico, a pesar de esto en el país coexisten los principios legales a partir de las cuales se puede emprender a batallar los disparejos modos de infracciones informáticas, examinando y dilucidando la ley existente para identificar su eficacia, consiguiendo así elementos de juicio para desplegar políticas y estrategias en este tema. (p. viii).

La investigadora indica que el incremento de TIC y la finalidad del trabajo de investigación es tipificar las infracciones informáticas ejecutados por intermedio de las redes sociales y conocer la figura de procedimiento que el Ministerio Público de Huánuco, brinda a las personas afectadas.

Así mismo, Espinoza (2017), hizo la tesis “Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control”, que defendió en la Universidad Nacional del Altiplano de Puno, Facultad de Ciencias Jurídicas y Políticas, para conseguir el título de Abogado, la finalidad del estudio es precisar el Derecho Penal Informático, para brindar al juzgador, al académico y al legislador, un enfoque deshabilitado del poder punitivo que subsiste escondido en la sociedad de la información, esta proyecto ayuda a delatar que nos encontramos en una Sociedad de Control, en la que el poder de vigilancia trasgrede la privacidad de las personas, y nos exhibe a un peligro de disipar nuestros espacios de libertad, y lo malo desistir que se construya un Estado de Policía, que sin limitación puede desligar genocidios.(p.14).

En el trabajo de investigación, el autor exhorta que se expongan planteamientos legislativos teniendo en cuenta a las nociones universales de Derechos Humanos con respecto a la atención de las informaciones, estableciéndose fiscalías especializadas para controlar las infracciones informáticas.

Morales (2016), realizó la tesis “La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos

informáticos en el Perú - 2015", que sustentó en la Universidad Señor de Sipán, Facultad de Derecho, para alcanzar el título de Abogado, siendo la finalidad de la investigación, exponer el saber de ser de las infracciones informáticas, como ha evolucionado hasta la actualidad, dando un aproximación sobre el contexto que ocurre en el medio, el problema que aqueja a la sociedad y la correspondencia con la utilización de la informática como recurso, para la comisión de infracciones, por lo tanto, otorga compendios de pesquisa inevitables, para alcanzar una discernimiento social beneficioso a propósito de poder desplegar políticas de seguridad informática. Facilitar una promesa real de labor para el Legislador, con el objetivo de que sus recursos humanos y materiales se aproximen al estudio, análisis y evaluación de esta problemática delictuosa, desplegando los cursos convenientes para no ser asombrados y excedidos por este nuevo contexto nacional y mundial. (p. 27).

La legislación del país debe examinar determinados artículos de la normatividad jurídica, la legislación debe auxiliar a una excelente reglamentación para suplir a los vacíos legales que existen, no siendo conveniente continuar adherido a representaciones propias que no solucionen una incertidumbre particular para una educada reciprocidad entre los representantes de la sociedad peruana.

1.2.3. A nivel Local

Los trabajos previos son escasos respecto al problema objeto de investigación, siendo las investigaciones las siguientes:

Huaney (2019), efectuó la tesis "El Derecho Informático aplicado al Derecho Penal en el Perú 2019" que sustentó en la Universidad San Pedro de Chimbote, Facultad de Derecho y Ciencias Política, para conseguir el título de Abogado, teniendo el propósito de conocer hasta dónde se llegar, en su término jurídicamente y poder lidiar a estas personas. Si bien es innegable, que la tecnología prospera a pasos gigantescos en el universo, se ve creciendo un recelo formidable por el control de este fenómeno, que nos violenta, en todos los espacios de

nuestras vidas, las infracciones informáticas, causados por personas como: los crackers, hackers, carding, phreaking, o sus disímiles modalidades, con mediano o alto grado de conocimiento de esta tecnología. El objetivo es dar a conocer algunos de los diferentes tipos de delitos informáticos. No pretende hacer de esta investigación una recapitulación de las leyes peruanas o de otros países, pero si se hará alguna mención de legislaciones que se van dando en el tiempo progresivamente en el Perú. (pp.1, 2).

La actualidad en el Perú, los especialistas del Derecho toman en consideración las pruebas aportadas al proceso penal por los peritos en infracciones informáticas, por otra parte, que con dicha estimación se perturben derechos primordiales de las personas.

Según el autor Vilca (2018), realizó la tesis "Los hackers: Delito informático frente al código penal peruano" sustentado en la Universidad Nacional Santiago Antúnez de Mayolo - Huaraz, Facultad de Derecho y Ciencias Políticas, obteniendo el título de Abogado, siendo su propósito del trabajo investigativo, saber el vacío legal en el actual CP, las comunicaciones electrónicas comerciales, establecer su notabilidad jurídica desde el margen de sus resultados nocivos en la sociedad de manera amplia y de manera específica en la jurisprudencia esencial a la vida íntima, en virtud a ello se implantan medidas y se instan progresos con el propósito de lograr su regulación. (p. vi).

En la investigación se valora que el desarrollo de las TIC y sus efectos en la vida social, han creado comportamientos ilegales llamados delitos informáticos, donde la propuesta de la investigación tiene el propósito la ordenación penal de las cualidades antijurídicas que valoramos más peligrosas como posterior recurso para impedir su arbitrariedad.

Por otro lado, Zorrilla (2018), realizó la tesis titulada "Inconsistencias y ambigüedades en la ley de delitos informáticos ley Nº 30096 y su modificatoria ley Nº 30171, que imposibilitan su eficaz cumplimiento" que defendió en la Universidad Nacional Santiago Antúnez de Mayolo de Huaraz, para conseguir el título profesional de Abogado, teniendo

como propósito investigativo, demostrar las debilidades e imprecisiones de la norma, aclarando la regulación normativa sobre las infracciones informáticas y construir claridades en relación a las fragilidades y tergiversaciones con respecto a la Ley 30096 y su transformada Ley 30171 entre el CPP y el contexto real. Por lo tanto, es significativo valuar cada acápite de la aludida norma actual. (p.23).

En la investigación se puede apreciar que la Ley 30096 y su cambio Ley 30171, ciertos artículos que muestran ambigüedades en su transcripción, los cuales ocasionan incertidumbre en los ejecutores de justicia, así como, en los afectados, causando numerosas veces que estas comprometidas infracciones no se evidencien o en su menoscabo no se pueda hallar a los auténticos criminales.

Sifuentes (2018), realizó la tesis titulada “Nivel de conocimiento de los operadores de justicia para la persecución del delito de Grooming - Chimbote 2017” que defendió en la Universidad San Pedro de Chimbote, para alcanzar el título profesional de Abogado, teniendo como intención saber el nivel de conocimientos que tienen los ejecutores de justicia para el seguimiento de la infracción de Grooming en la ciudad de Chimbote durante el año 2017. En cierre, se alcanzó que el nivel de saberes que prevaleció en los operarios de justicia con respecto al delito de Grooming fue de nivel bajo, alcanzando en un 58%. (p.2).

El autor del trabajo de investigación sobre Grooming que es un delito informático que es penado penalmente, donde los especialistas de justicia de Chimbote, conocen medianamente, siendo el nivel bajo, esperando con el transcurrir del conozcan o se informen más sobre este delito.

De la Cruz (2017), realizó la tesis “Aplicación de metodologías y herramientas de la informática forense para reducir el riesgo de la seguridad informática en la Dirección Nacional de comunicación y criminalística de la Policía Nacional del Perú – Huaraz - 2015” que sostuvo en posgrado de la Universidad Nacional Santiago Antúnez de

Mayolo de Huaraz, con el desenlace de lograr el grado académico de Maestro en Ciencias e Ingeniería., donde tiene como objetivo, establecer la correspondencia de seguridad informática y la informática forense de la DIRCRI de la PNP, Huaraz.

La PNP tiene como finalidad prevenir y auxiliar a las personas, por lo tanto, se piensa que el incremento de la entidad debe ser indestructible y estar en entera modernización, cada vez más la TIC se ha trasformado en una herramienta para ejecutar infracciones. El personal policial es sensato, que las amenazas habituales como la infracción informática que se causan en Perú, exigen muchos retos en las pesquisas, se han logrado certezas como los computadores, celulares, unidades de almacenaje, softwares o cualquier clase de hardware que demandan de saberes, estrategias e instrumentos de Informática Forense para que se pueda efectuar una restablecimiento, examen y afirmación de la trasgresión de un modo apropiada y alcanzar al criminal. (pp. 2, 3).

El autor de la investigación examina los procedimientos y los equipos que la PNP para ser encaminada, auxiliada a maniobrar un suceso del crimen, siendo comprendidos los procedimientos informáticos y de comunicación, con la finalidad de recuperar las evidencias digitales que se realizan por Internet como transacciones de compra, venta, pagos, depósitos, etc.

1.3. Teorías relacionadas al tema.

1.3.1 Delitos informáticos

1. Definición

Fuentes, Mazún y Cancino (2018) dicen que es el conjunto de comportamientos que genera delito penal y, que debe ser tratado legalmente ya que el mismo tiene por objeto daños a terceras personas, ocasionando diferentes lesiones y, en algunos casos pérdidas de bienes jurídicos. Es necesario aclarar, que esta manera de infracciones acontece en el ciberespacio. (pp. 1-8).

Se logra confirmar que las infracciones informáticas vienen hacer comportamientos antijurídicos que son delitos penales y que deben tratarse de acuerdo a normativa vigente.

Torres (2017) manifiesta que existe una fuerte tendencia a que los hechos delictivos se concentren hacia la parte empresarial, siendo este un blanco elegido por los antisociales, en muchos casos, por descuidos en cuanto al sistema de seguridad de las mismas organizaciones. (p. 104).

Se ratifica que las infracciones informáticas son hechos delictivos hacia el patrimonio jurídico, cometidos por medios o recursos informáticos.

OCDE - Organización para la Cooperación y el Desarrollo Económico (2015) expresa que la infracción informática viene dado al comportamiento de manera ilegal que es contraria a la ética y, no es autorizada si divulgación y transmisión de datos de la red.

Según lo indicado la infracción informática viene hacer comportamiento propio, culpable y antijurídico no autorizado, se usan recursos informáticos para cometerlo.

Besares (2015) dice sobre el delito o infracción informática que es el comportamiento o conducta típica antijurídica y responsable que perturba el derecho humano y la seguridad informática de la amistad de los ciudadanos, utilizando el procedimiento fraudulento de datos, que se diferencian de otros aparentes los denominadas infracciones electrónicas o computacionales. (p. 53).

Por lo manifestado se asevera que las infracciones informáticas actualmente son sancionadas por el código penal porque infringen y vulneran los derechos de las personas con fines lucrativos o no.

Estrada (s/f) expresa refiriéndose al delito o infracción informática que involucra acciones delictivas, un primer instante las naciones han convenido de incluir en figuras propias de carácter tradicional,

tales como fraudes, falsificaciones, sabotajes, robos o hurto, estafas, perjuicios, etc. Sin embargo, debe enfatizarse que la utilización de los métodos informáticos ha instaurado nuevos sucesos del empleo ilícito de los computadores, que ha favorecido a su vez la insuficiencia de ordenación por el Derecho.

Así mismo, el tratadista revela que la infracción o delito informático actualmente la normativa debe actualizarse para sancionar dichas actividades ilícitas y delincuenciales.

Villavicencio (2014) (citando a Miro Linares) entiende a la criminalidad informática a aquellos comportamientos dirigidos a engañar los aplicativos de seguridad, es decir, invasiones a computadores, sistemas o correos de datos por medio de un anagrama de acceso; comportamientos típicos que exclusivamente pueden ser ejecutadas a través del avance tecnológico, en un sentido amplio, alcanza a todos aquellos comportamientos en las que las TICs es el propósito, el intermedio de realización, aunque afecten a bienes jurídicos diferentes; y que planea dificultades criminológicas y penales, causados por las particularidades únicas de la zona de comisión. (p. 286).

Tellez (2008) expresa refiriéndose a los delitos informáticos que son conductas ilícitas que poseen a los computadores como herramienta o fin (concepto atípico) o los comportamientos típicos, antijurídicos y culpables que poseen a los computadores como herramienta o fin (concepto típico).

Esta clase de acciones muestran las siguientes características importantes:

1. Son labores ocupacionales en cuanto que muchas veces se realizan cuando el sujeto está trabajando.
2. Son labores de oportunidad porque se aprovecha una ocasión creada o altamente intensificada en el campo de las funciones y organizaciones del sistema tecnológico y económico.

3. Inducen serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan.
4. Prometen facilidades de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin una necesaria presencia física.
5. Prometen a los menores de edad facilidades para su comisión.
6. Son muchos los casos y pocas las denuncias, debido a la falta de regulación jurídica a nivel internacional.
7. Son muy sofisticados y relativamente frecuentes en el ámbito militar.
8. Presentan grandes dificultades para su comprobación, por su carácter técnico.
9. En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales.
10. Son comportamientos criminales de cuello blanco, white collar crimes, en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden cometerlas.
11. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica en el ámbito internacional. (p.188).

Tal como indica el autor que la infracción informática en representación típica y atípica, deduciendo por el primero a los comportamientos típicos como antijurídicos y culpables y por el segundo a los comportamientos atípicos como actitudes ilícitas, ambas representaciones tienen a los computadores, laptops o móviles como elemento esencial. Por otro lado, debe señalarse que se han enunciado diversas calificaciones para demostrar los comportamientos ilícitos en las que se usa el computador, tales como infracciones informáticas, infracciones electrónicas, infracciones coherentes con los computadores, transgresiones por computador, delincuencia concerniente con el computador.

Pero se conoce que la infracción informática es cometida por personas que tienen conductas delictivas, haciendo uso del

computador o algún dispositivo electrónico como el celular, actualmente en el Perú se está acrecentando dicha modalidad de delitos conforme al avance de las nuevas tecnologías, por lo que deben ser sancionadas ejemplarmente por el código penal porque vulneran el patrimonio de las personas.

Finalizamos definiendo que las infracciones informáticas son todos aquellos comportamientos ilegales y delictivos que hacen utilización de dispositivos electrónicos y que son capaces de ser sancionadas o penadas por la ley penal del país. Por otro lado, el trabajo de investigación tiene objeto la regulación penal de aquellas conductas o comportamientos antijurídicos que preciamos más peligrosos como posterior recurso para impedir su impunidad.

1.1. Clasificación de los delitos informáticos

Los delitos o infracciones informáticas, podemos ver varias formas de clasificación, tal como mostramos a continuación.

Según Loredo y Ramírez (2013) (citado a INTERPOL) numeran como infracciones informáticas:

a. Botnets, que son las redes de equipos infectados vigilados por usuarios remotos.
b. Ataques contra los softwares y los datos informáticos.
c. Estafas a través de Internet.
d. Comercialización de iconografías de abusos sexuales contra los menores de edad.
e. Difusión de virus.
f. Phishing que son la adquisición fraudulenta de información personal íntima.
g. Infracción en servicios bancarios o financieros en línea.
h. Usurpación de la identidad. (pp. 45-46).

Téllez (2008) a los delitos o infracciones informáticas los clasifica como:

Instrumento o medio: en este tipo están los comportamientos delictivos que utilizan a los computadores como medio, método o distintivo en la comisión del ilegal:

1. Diversificación de los pasivos y activos en el contexto contable de las corporaciones o empresas.
2. Falsificación de documentos vía computarizada como las tarjetas de crédito, cheques, etc.
3. Robo de tiempo de computadora.
4. Lectura, sustracción o copiado de información personal.
5. Uso no autorizado de programas de cómputo.
6. Planeación y simulación de infracciones convencionales como robo, homicidio, fraude, etc.
7. Innovación de datos o información tanto en el ingreso como también en la salida.
8. Diversificación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
9. Transformación en el funcionamiento de los sistemas, a través de los virus informáticos.
10. Aprovechamiento indebido o violación de un código para ingresar a una aplicación o sistema con instrucciones inadecuadas.
11. Obtención de información residual impresa en papel luego de la ejecución de trabajos.
12. Intervención en las líneas de comunicación de datos o teleproceso.
13. Penetración de instrucciones que inducen "interrupciones" en la lógica interna de los aplicativos o softwares, a fin de conseguir beneficios.
14. Ingreso a sitios computarizadas de manera no autorizada o ilícita.

*Fin u objetivo***:** en este tipo, se considera los comportamientos delictivos que van encaminados contra los computadores, softwares o accesorios como objeto físico, ejemplo:

1. Destrucción de programas por cualquier método.

2. Ataque físico contra el computador o sus dispositivos.
3. Complot político o subversión para que se elimine o salga una comisión de los lugares principales informatizados.
4. Programación de instrucciones que originan un cerco total al software.
5. Daño a los periféricos de almacenamiento.
6. Retención de dispositivos magnéticos entre los que figura información meritoria con propósitos de coerción, cancelación de liberación, etc. (pp. 190,191).

Estrada (s/f), (citando a Lima, M.), muestra la tipificación, denomina "delitos electrónicos", expresando que preexisten tres clases, los que usan la tecnología electrónica, a conocer como:

- Medio**:** comportamientos criminógenos en donde para efectuar una infracción o delito usan un computador como recurso o medio.
- Método: comportamientos criminógenos en donde las personas usan procedimientos electrónicos para conseguir a una infracción ilícita.
- Fin: comportamientos criminógenos dirigidos contra el ente físico del objeto o computador electrónico o su material con el propósito de dañarlo.

2. Tratamiento penal

El tratamiento penal, es el procedimiento teórico, doctrinario, dogmático, jurisprudencial y normativo, especialmente en el objeto de estudio de las infracciones informáticas contra el patrimonio, con realce en los modos de fraude, estafa, hurto, y sabotaje informático. Este procedimiento penal se consigue tratar en: tratamiento procesal y tratamiento normativo.

2.1. Tratamiento procesal

El tratamiento procesal de las infracciones informáticas hacia el patrimonio en los ciudadanos jurídicos y naturales en el

modo de estafa, fraude, sabotaje y hurto informático hace reseña a los hechos de pesquisa de estas infracciones, donde se señala, el procedimiento de las consideraciones jurídicas para la penalidad de las infracciones informáticas. Estos tipos de delitos son muy graves por las características especiales que tiene cada uno de ellos, es indicar, la realización de las infracciones informáticas se consigue ejecutar sin admitir en circunspección las restricciones virtuales.

2.2. Tratamiento normativo

El tratamiento normativo son las diversas normas, vigentes como derogados referentes a las infracciones informáticas hacia el patrimonio de las personas naturales y jurídicas, ya sea de trascendencia nacional o internacional.

En el Perú tenemos consignadas en el CP, en la Ley de infracciones informáticas y sus respectivos cambios, por otra parte, a altura universal se cuentan con las leyes de las otras naciones, y en específico al tratado de Budapest o de ciberdelincuencia, siendo el primer acuerdo de importancia internacional, imputable a todos los países que suscribieron dentro de ellos el Perú. Dicho convenio internacional es del 2001, se debe actualizar el contenido conforme al contexto de los países en la actual circunstancia y al progreso de las nuevas TIC.

3. Tratamiento penal de los delitos informáticos

El tratamiento penal de las infracciones informáticas hacia el patrimonio es deficiente en el Perú, debido a que comprende solo el fraude informático, generando inseguridad en el análisis de la normatividad que no reconoce la penalidad efectiva de los delitos o infracciones informáticas hacia el patrimonio.

El tratamiento penal de las infracciones informáticas hacia el patrimonio en su particularidad de robo o hurto es defectuoso, en la mesura que la normatividad del Perú no se regulariza de manera clara la infracción informática hacia la propiedad, por lo que concibe

problemas en la indagación y penalidad de las infracciones informáticas de robo, cuando no se efectúa con el principio de tipicidad.

En la peculiaridad de la infracción de fraude es incompleto, dentro de esta peculiaridad delictiva se percibe todos los modos de infracciones informáticas hacia el patrimonio, y al ser esta figura penal muy accesible y confusa no admite el firme castigo de dichas infracciones informáticas en su manera de fraude.

En la particularidad de la infracción de estafa es imperfecto, debido a que la reglamentación del Perú no legaliza explícitamente, este ilegítimo penal, porqué al no plasmarse con el principio de tipicidad, obstaculiza la exploración, la penalidad de dichas infracciones informáticas en su modo de estafa.

En la peculiaridad de la infracción de sabotaje también sigue siendo incompleto, de modo que en la actual reglamentación se castiga la pérdida de los datos, no se regula de manera precisa y explicita la alteración al patrimonio mediante software informáticos, con o sin intenciones rentables, lo que concibe protección de los sucesos de sabotaje hacia las instituciones empresariales o personas naturales hacia subyugar su competencia.

Así mismo, la debilidad es el menoscabo de estabilidad, en la totalidad de los juicios, se requiere de la solidez de alguna materia o herramienta para efectuar una organización con él, de lo contrario, dicho arreglo además concederá debido a su debilidad, obedeciendo del ambiente que lo sitia, las variables que lo afectan y los sentidos que se emplean para poder concebir cómo funciona dicho artículo.

La legislación peruana como latinoamericana en general es bastante pobre en cuanto a técnicas legislativas relacionadas a los delitos informáticos. Aparentemente se pretende subsumir este delito como uno más del título destinado a la protección del patrimonio de personas naturales y jurídicas, lo cual es un incorrecto ya que solo se puede agredir ese bien jurídico a través de los medios informáticos.

La legislación penal peruana en la comisión de delitos, tiene un gran reto por delante, que consiste en prevenir la criminalidad informática; puesta que ello, representa la fortaleza de crimen organizado actualmente.

Los delitos e infracciones informáticas es una temática de gran interés y de preocupación nacional y por tener un carácter trasnacional los delitos cometidos mediante el computador, sería necesario establecer tratados de asistencia recíproca entre las naciones que accedan establecer elementos sincronizados para la apuesta en empuje de herramientas de colaboración global para neutralizar efectivamente la delincuencia informática.

Finalmente, visto la enunciación correspondiente de los delitos informáticos que comprende el artículo 8, es necesario proponer la modificatoria de dicho artículo contra el patrimonio de la Ley Nº 30096 para proteger a las instituciones empresariales y ciudadanos, con la finalidad de hacer valida y con el mejor tratamiento penal.

4. Modalidades de delitos informáticos contra el patrimonio

Las infracciones informáticas son aquellos comportamientos delictivos conducentes a burlar los procedimientos de seguridad, por medio del anagrama de ingreso, daño o destrucción a la base información o datos y aplicativos, etc., siendo materia de estudio hacia la propiedad, en los modos de sabotaje, estafa, fraude y hurto.

4.1. Fraude informático

Esta modalidad de infracción informática es el ingreso ilícito a los datos o algún bien inmaterial o material con costo propio desairando las políticas de garantía de los sistemas informáticos, redes y dispositivos electrónicos con la finalidad de beneficio ilegal de las utilidades de la acción engañosa. Este delito es reconocido como una treta a las reglas de seguridad de los sistemas para el beneficio prohibido, y a divergencia de la estafa que es admitida como el empleo de medios informáticos para mentir a los ciudadanos. Las modalidades frecuentes de fraude tenemos:

a. Manipulación de datos de entrada

Esta manera de infracción informática es la resta de códigos y claves que el afectado usa para tener acceso al acopio de datos, a software. La cualidad de esta infracción es que la adquisición de la información se realiza cuando el afectado ingresa a determinados aplicativos, sistemas, sitios web, donde anticipadamente se han organizado los sistemas para la manipulación o substracción de los datos e información, esto acontecede cuando se clona el sitio web de una identidad bancaria con resultados de conseguir la información o datos de las tarjetas de crédito del perjudicado.

b. Manipulación de los datos de salida

Esta infracción o delito informático trasgrede en los datos o información que el afectado consigue del procedimiento informático, esta aparente pesquisa admite a los ciberdelincuentes beneficiarse del yerro en que se halla el perjudicado como resultado de adquirir concluyentes favores.

c. Manipulación de aplicativos

En esta infracción informática se explora que los aplicativos que tiene instalados la computadora del perjudicado ejecuten diligencias sistemáticas por el agente de la infracción escudriñando categórico favor, para ello, va a perturbar el funcionamiento de aplicaciones informáticas con el objetivo de lograr alguna clase de beneficio.

d. Técnica del Salami

Este tipo de infracción informática se comprueba por la reclusión de sumas de dinero en pocos importes que retiran de una cuenta financiera a otra. El desfalco es en sumas de dinero progresivos por el afectado, para efectos de no levantar recelos sobre la trasgresión. Se ejecuta mediante la entrada de software que se establecen en las computadoras de los perjudicados, realizando los servicios financieros en pequeñas cantidades, pero cuando el desfalco aqueja a una

diversidad de perjudicados, los criminales consiguen grandiosas ganancias.

e. Phishing

Este modo de delito informático radica en la remisión de presumidas promociones y ofrecimientos comerciales que el afectado debe acceder colocando su información personal en los formularios apócrifos que remitirán los datos solicitados a los ciberdelincuentes, con todo esto lograrán patrocinios con menoscabo del afectado, cuando analice su estado de cuenta, recientemente se sorprenderá de la infracción del cual ha sido perjudicado.

4.2. Estafa informática

Esta conducta delictiva que viene hacer la utilización de los medios informáticos para mentir al afectado con la finalidad de que se despegue de su propiedad y el beneficio ilícito del sujeto activo de dicha pertenencia. Los compendios característicos de esta infracción informática son considerablemente iguales a la infracción de estafa frecuente, con la específica peculiaridad de que, en la estafa, para establecer la inexistente situación en el perjudicado de la trasgresión se usa medios virtuales. Es señalar, para hacer sucumbir en yerro al perjudicado se utilizan los medios virtuales, las maneras usuales de estafa tenemos:

a. Hacking

Esta modalidad de delito informático se fundamenta en el ingreso indebido a los datos o sistemas digitales incluidos en un aplicativo para permitir a las claves con el propósito de estafar, transgrediendo las reglas de seguridad de los sistemas y con abandono de la venia de su cargo, consumando así una infracción de penetración informática.

b. Spear Phishing

Esta infracción informática se realiza por la remisión de emails o correos electrónicos engañosos enviados a personas jurídicas con el propósito de acceder la vía a información privada, nombres de usuarios, contraseñas o

información propia con la finalidad principal de conseguir acceso al sistema. El ciberdelincuente se destina personalmente a cualquier ciudadano con compromiso o cargo específico en la institución, supliendo la identificación de alguno de los trabajadores de la empresa para la misión de la infracción.

c. Pharming.

Esta manera de delito o infracción informática gravita en el disimulo de la página web de una institución financiera, por medio de una remisión intensa de mailing o información publicitaria, el interesado subscribe a su agencia financiera online colaborando toda la información que son solicitados, número del DNI, contraseñas, cuenta del banco y número de tarjeta de crédito, etc. La virtud de esta estafa se debe a que el ciberdelincuente maniobra el DNS o nombre del dominio web de la institución financiera, acopiando un código malicioso en el computador del perjudicado para que cambie el código URL de la institución financiera oficial en una conexión de la página web falsa y, así, el perjudicado pretenderá que ingresa a su oficina online, en escenario ingresa a la IP de la página web fraudulenta.

4.3. Sabotaje informático

Esta modalidad radica en el uso no autorizado de centros de cómputos o instalaciones informáticas donde alteran y destruyen el hardware y software.

Villavicencio (2014), sostienen que el sabotaje informático; que se fundamenta elementalmente en suprimir, borrar, alterar y modificar sin permiso las funciones o información a los computadores con mira de entorpecer la actividad correcta del software, denominado frecuentemente como virus informático. (p. 293).

Se concibe esta modalidad de infracción informática a la alteración o destrucción de información y la depredación hacia

un sistema virtual. Los modos más frecuentes son las siguientes.

a. Bomba lógica

Esta modalidad de delito informático se fundamenta en la entrada en un software cuya finalidad es arruinar datos del computador hacia al posterior. Perdura oculto en el computador a la expectativa que se plasmen con las circunstancias que agilizan su planificación destructora del perjudicado, por ejemplo, puede subsistir en un computador a la expectativa que se incruste una dirección, un nombre, se concluya un formulario.

b. Virus

Este delito que son software creados con el propósito de acceder a un software, perturbando su proceso, asimismo tiene la particularidad de propagarse y perturbar el aplicativo al que suscriben, actúan infectando de un programa a otro y modifican en cuanto al nivel de destrucción.

c. Gusanos

Este tipo de delito son software que poseen la acción perspicaz de multiplicar archivos de forma confusa haciendo desplomar el sistema informático por rebosamiento, además de otros resultados perniciosos al sistema informático, así tenemos, la pesadez del computador, la evasión de los datos e información.

4.4. Hurto informático

El hurto informático es el acceso y apropiación de hardware y software ajeno, donde retiran archivos informáticos, para almacenarlo su contenido en un soporte propio

Según el tratadista Rodríguez (2013) dice interiormente de los sucesos que alteran al hardware (físico) o al software (lógico) se hallan las infracciones hacia la posesión, el perjuicio al software o hardware, por lo que, se estipula de incautación oculta de estos dispositivos que forman el aplicativo, robo, de conformidad a la caracterización del acto jurídico que efectúa el CP. (p.110).

Los modos más frecuentes de hurto:

a. Hurto de servicios

Esta modalidad de delito informático radica en desfalcar los datos personales de ente jurídico o natural, despojando un plagio o toda la información, este comportamiento ilegal se numera en los tipos:

Hurto de tiempo de la computadora

Se ejecuta cuando se emplea un computador pertenencia de una institución empresarial sin autorización cuyo objetivo es efectuar labores de índole personal; actualmente poco se usa este modo de infracción puesto que es muy accesible tener un computador.

Parasitismo informático

Este delito viene hacer el ingreso de software parásitos en el sistema del perjudicado con el propósito de obtener ingreso ilegal a los soportes físicos o aplicativos, siendo utilizados en favor del ciberdelincuente. Se asocia a esta infracción la de reemplazar al individuo.

Analizando todas estas diversas modalidades de delitos o infracciones informáticas que se muestran en el país, es necesario la modificatoria de dicho artículo, porque va más allá. En la legislación peruana, la debilidad en los indicios que se muestran logra ser un causal de culpa en el asunto que se pretenda con estas definir una ingenuidad. Es señalar, si los indicios no son lo adecuadamente precisas, no se conoce a ciencia segura cual será fundamento de las propias, no se tiene una clara perspectiva de la situación de estas con respecto a su autenticidad.

Flores (2020) en un artículo titulado Los ciberdelitos: la otra pandemia que avanzó en silencio en el Perú, con fecha 14 de octubre del 2020, donde manifiesta:

El coronavirus en Perú también ha tenido una señal negativa en conocimientos de ciberseguridad en el Perú. De acuerdo a las cifras más estrenadas, las infracciones cibernéticas acrecentaron un 59% durante los seis primeros meses, respecto al mismo periodo del año

pasado, debido a que la pandemia promovió la utilización de los procedimientos virtuales y agregado a la necesidad de quedarse en casa y hacer un mayor empleo de las tecnologías exhibiendo nuestra información personal debido a la utilización de softwares, redes sociales, Internet de las cosas, siendo utilizado por los cibercriminales.

El malware, viene hacer el robo de información, estafas, etc., vienen hacer diversas las variedades delictivas, puede cambiar la utilización de Internet siendo un genuino riesgo si no se toman indudables precauciones (…).

El fraude informático que son las estafas ejecutadas a través de Internet para lograr ganancia económica, viene hacer una de las infracciones más frecuentes, existe de toda clase: desde los dolos más artificiosos a ardides más simples que pueden ejecutar inclusive fuera de Internet. Predominan las personas dedicadas a esta infracción, se adecúan a cualquier acontecimiento para perpetrar infracciones contra las empresas o hacia los individuos.

Presentemente existen estafas siendo principalmente frecuentes, y cada día mejoran y están acondicionadas para hacer transitar por algo efectivo. Algunas acreditadas son:

- El fraude romántico, las concernientes con las compras online;
- El phishing que permite captar contraseñas o números de tarjetas de crédito imitando correos electrónicos de organismos u organizaciones oficiales;
- La estafa nigeriana, las concernientes con los premios, loterías y concursos;
- ONG, causas protectoras, y dinero para emergencias, entre otros muchos.

Todos los días en esta situación percibimos en los noticieros televisivos e informativos que los ciberdelincuentes ejecutan diferentes fraudes en menoscabo de las personas que muchas veces fían en la publicidad del Internet, sitios web de compras online, correos electrónicos, redes sociales, WhatsApp, mensajes de texto y otras cosas virtuales, manipulando sus tarjetas de débito y crédito

o ejecutando traspasos electrónicos para pagar los bienes o servicios.

Es indiscutible que estas infracciones informáticas de fraudes se realizaban antes de la pandemia causada por el COVID-19, a partir de la declaratoria de Emergencia Nacional, los centros comerciales y empresas medianas y pequeñas que vendían ropa, equipos de oficina, computadores, diferentes productos de electrodomésticos, e insumos en general, se encontraban cerrados, impulso conveniente, el Ecommerce se convirtió en el importante medio de adquisición de bienes y servicios.

Los fraudes informáticos han crecido de manera sustancia en el país, por tal razón, se exhorta evitar acceder a sitios webs que piden datos bancarios, porque el delincuente informático pretenderá de cualquier manera que el perjudicado le conceda su información con trampas para apoderarse de sus datos y cometer el delito, afectando el patrimonio natural y jurídico.

Según Diario El Peruano de fecha 09 de setiembre del 2022 manifiesta las cifras del 2021, el fraude informático y la suplantación de identidad son los ciberdelitos más frecuentes. Cada vez se registran más denuncias por delitos informáticos en el país (Perú). Según cifras del Ministerio Público, en el 2021 recogieron 18 mil 596 denuncias de casos de cibercrimen, lo que simboliza un incremento porcentual de 92,9% en comparación con el 2020.

Estos datos fueron acopiados en una información estadística sobre ciberdelitos divulgado por el Observatorio Nacional de Política Criminal del Ministerio de Justicia y Derechos Humanos (Minjusdhs). Uno de los factores que revelan el aumento de estas denuncias es la instalación de la Unidad Fiscal Especializada en Ciberdelincuencia a inicios del 2021.

Así mismo, la Policía Nacional del Perú (PNP) registró 14 mil 671 denuncias por delitos informáticos durante el año 2021. Esto representa un aumento de 65% de casos más que el año anterior (8 897 denuncias en 2020).

Según Trujillo en línea del 18 de octubre del 2022, indica que Santiago Barranzuela, gerente de Seguridad de la compañía Grupo EULEN, revela tres delitos de ciberdelincuencia que se realizan con mayor frecuencia en el país y que atentan contra el patrimonio.

Compras fraudulentas. Los ciberdelincuentes ofertan productos en sitios web o redes sociales a muy bajos precios. Los usuarios son engañados para realizar los pagos en línea o transferencias a cuentas personales, y luego los perfiles de los vendedores son desactivados.

Páginas clonadas falsa. A través del phishing, los delincuentes o estafadores en línea engañan a los usuarios con páginas falsas que simulan ser los sitios web de las entidades financieras. Las víctimas registran sus datos personales y, con esa información, las organizaciones criminales realizan depósitos sin autorización de las cuentas bancarias.

Falsas ofertas en línea. La falsificación de ofertas o descuentos de reconocidas tiendas en línea es cada vez más frecuente. Los usuarios reciben mensajes de texto o notificaciones y acceden a sitios web clonados para realizar pagos en línea.

5. Aspectos de los delitos informáticos

En el Perú influyen aspectos en las infracciones informáticas que viene hacer los siguientes:

5.1. Social y económico

El Perú es un país consumista, las tecnologías informáticas, computadores, laptops, teléfonos móviles, tablets y otros es cada vez más frecuente y habitual. Gran parte de la población de nuestro país no tiene acceso al Internet y a dichos dispositivos electrónicos, principalmente los que residen en lugares donde las redes de comunicación aún no llegan o por asuntos económicos.

Actualmente, estamos viviendo en una colectividad donde los niños y jóvenes son nativos en la utilización de las TIC, así

mismo, son además los más sensibles y proclives a ser perjudicados por las infracciones informáticas.

5.2. Político

En el Perú, actualmente en lo que respeta al contexto político, ha habido propósitos y proyectos legislativos diversos para la lucha contra la política criminal virtual y la cibercriminalidad, de los cuales se hallan proyectos de ley archivadas y la que progresó fueron solamente la Ley 30096 y la Ley 30171.

5.3. Cultural

El Perú es un país multicultural, a lo largo de sus tres regiones, siendo su geografía uno de los componentes que circunscriben la intercomunicación, de ahí son las aberturas de acceso al Internet y a los sistemas informáticos, por lo agreste de algunos lugares no hay una trayectoria plena de las compañías de telecomunicaciones, por lo que constituye las prohibiciones del acceso a la educación de los habitantes.

Actualmente la patria ha estado intensamente afligido por una corrupción administrativa y estatal, por tal razón, ha sido inverosímil saber entonces la efectiva magnitud de los delitos o infracciones informáticas, la mayoría de estas infracciones no son declarados o revelados a los ejecutivos formales, en esto se añade la escasez de normas o el ambiguo uso de las actuales con la finalidad de resguardar a los perjudicados de estas infracciones; la escasez de capacitación de los ejecutivos para entender, averiguar y emplear el procedimiento legal apropiado a este problema; el miedo por parte de las instituciones empresariales de revelar este clase de ilegítimos por el descrédito que esto logrará causar a su entidad y las perseverantes desventajas monetarias y otras, acarrea como resultado que los datos estadísticos de esta forma de comportamientos se ampare de la denominada cifra negra u oculta.

Muchas pesquisas han confirmado que, en diversas naciones de Latinoamérica, la impunidad y corrupción han tolerado a bandas criminales, instaurar y desarrollar auténticas disposiciones de

poder paralelos. Lo preliminar, se explora que para obtener un prejuicio efectivo de la ciberdelincuencia se exhorta, en primera medida, un examen real de la escasez de amparo y de las referencias de riesgo. Una ayuda efectiva hacia la cibercriminalidad ratifica los perjudicados comprendan los oportunos procedimientos de administración, así como sus representaciones de ocultación.

1.3.2. Análisis de la legislación

1. Ley de delitos informáticos internacional

1.1. Chile

El país de Chile siendo el primero en Latinoamérica en penar una Ley contra Delitos Informáticos. Siendo la Ley 19223 publicada el 7 de junio de 1993, en el Diario Oficial (similar del diario oficial peruano) manifiesta, la destrucción o inutilización de un sistema de procedimiento de información debe ser penada con prisión de un año y medio a cinco.

1.2. México

En México en su CPF, ofrece un capítulo del noveno título de su segundo libro denominado ingreso ilegítimo a sistemas y equipos de informática, donde constituye el amparo de las comunicaciones. En principio fue insuficiente la normatividad penal del tema, pero esclarecemos, que existe estados federales mexicanos que poseen sus autónomas categorizaciones al contenido, a lo que no consignaremos en decisión a la prolongación que involucraría examinar una por una.

1.3. Colombia

En Colombia el Congreso de la República ratificó el 5 de enero de 2009, la Ley 1273 que, a través de ello, se cambia el Código Penal, creándose un novedoso bien jurídico tutelado llamado de la Protección de la información y de los datos, se patrocinan integralmente los sistemas que usen las TIC, entre otras instrucciones

Teniendo dicho procedimiento, la pesquisa se cristianizó en un bien titulado y de este modo, se consigue constituir un esquema regularizador para comportamientos delictivos coherentes con la tecnología o que siendo perpetrados por medios informáticos. Colombia transitó a ser precursor en altura universal en cuestión de normatividad de las infracciones informáticas.

Dichos delitos son sancionados severamente, la Ley 1273 vislumbra condenas de prisión desde los 48 a 120 meses y sanciones de hasta 1.000 salarios mínimos legales mensuales actuales.

Lo que se puede manifestar, mientras se profesen leyes para agredir este modo de infracciones virtuales, florecen tecnologías nuevas para reírse y los cibercriminales sigan impunes ante la sociedad global.

1.4. Argentina

El país de Argentina existe la Ley de delitos informáticos Nº 26.388, siendo la ley no es especial que reglamenta esta manera de infracciones en un cuerpo legal apartado del CP con marcos autónomos y específicos, es una norma que cambia, suplanta y reúne formas típicas a diferentes artículos todavía en utilidad, con la finalidad de regularizar las nuevas tecnologías como medios de comisión de infracciones advertidos en el CP. Esencialmente contiene textos, distribución y posesión con propósitos de colocación de violación de correos electrónicos, pornografía infantil, acceso fraudulento a sistemas virtuales, daño informático y distribución de códigos maliciosos y perturbación de comunicaciones.

El diario La República en un artículo titulado Ciberdelitos generará costos de más de un billón de dólares para economía global, revela:

Una indagación publicada el lunes 7 de diciembre, donde McAfee Corp. y el CSIS (Centro de Estudios Estratégicos e Internacionales) concluye que la delincuencia informática ocasionará un precio de más de un billón de dólares para la capital global.

Esta suma constituye un 50% más que en 2018, y creará significativas señales no monetarias. Contiene destacar que el precio de la acción criminal en línea es de más del 1% de la producción financiera global.

Las agresiones de mayor afluencia contienen al randomware, phishing, spyware, robo de criptomonedas y el secuestro de emails de las empresas. La extensión de estos mismos puede imputarse a una menor garantía debido a las labores virtuales remotas, sin el amparo de las dependencias.

El peligro y la continuidad de los ciberataques a las instituciones empresariales acrecientan conforme avanzan las metodologías. Las innovaciones nuevas en las tecnologías abren más lugares para nuevas coerciones y el entorno de la labor se divulga a ambientes domésticos y remotos, expresó el director técnico de McAfee, Steve Grobman.

El sondeo se elaboró con base en una encuesta verificada a 1500 especialistas de la tecnología en los sectores público y privado de Reino Unido, Alemania, Japón, Canadá, Australia y Estados Unidos.

La señal de los cibercrímenes circunscribió perjuicios en materia de activos monetarios y pertenencia intelectual, al igual que los egresos que originan la inacción del sistema y los perjuicios al realce de una organización, dice la referencia.

Los ciberdelitos que vienen hacer un flagelo en el mundo vienen causando pérdidas millonarias en componente de activos monetarios y propiedad intelectual durante el 2020, tal como indica dicho informe señalado.

2. Ley de delitos informáticos en el Perú

La actual ley de delitos informáticos en el artículo 1º señala que el propósito de la ley es prevenir y sancionar las actitudes indebidas que aquejan los sistemas, los datos informáticos, y otros bienes jurídicos de notabilidad punitiva, como el patrimonio, la fe pública, la libertad sexual, etc., que obtengan ser presuntuosos por medio del manejo de las TICs, con la intención de avalar los escenarios mínimos para que los ciudadanos disfruten del derecho al desarrollo y a la libertad. La norma pretende certificar la disputa enérgica hacia la delincuencia informática o cibercriminalidad.

2.1. Teoría jurídica

La infracción informática en su comienzo se hallaba representado en el Art. 186, inciso 3, segundo párrafo del CP de 1991. La medida no estaba adecuada de una infracción autónoma, sino como un perjuicio de la infracción de robo o hurto. A continuación, las infracciones informáticas son agregados por la Ley 27309 y quedaban establecidos en el Cap. X del CP: los Art. 207- A concerniente a la interferencia, acceso o copia ilícita contenida en base de datos, 207- B referido a la alteración, daño o destrucción de base de datos, 207 - C referidos a las circunstancias cualificantes agravantes, 207- D concerniente al tráfico ilegal de datos, y en las normas penales especiales.

Las normas jurídicas, se hallan en la Ley Nº 30096 (2013), de infracciones informáticas. La Ley comprende siete capítulos que se organizan como: Capítulo I, Finalidad y objeto de la Ley; Capítulo II, delitos contra datos y sistemas informáticos; Capítulo III, delitos informáticos contra la indemnidad y libertad sexual; Capítulo IV, delitos informáticos contra la intimidad y el secreto de las comunicaciones; Capítulo V, delitos informáticos contra el patrimonio; Capítulo VI, delitos informáticos contra la fe pública y Capítulo VII, las disposiciones comunes.

Después se publicó la Ley Nº 30171, el propósito de la norma fue apropiar la Ley 30096 a los patrones normativos del

tratado referente a la ciberdelincuencia, al añadir en su trascripción representativa de los Art. 2, 3, 4, 7, 8 y 10 de la concerniente norma, la posibilidad de realizar la infracción intencional e ilegalmente. Reformas de la Ley Nº 30171 (2014), está en relación a las infracciones informáticas, son:

- Art. 1; Modificación de los Art. 2, 3, 4, 5, 7, 8 y 10 de la Ley Nº 30096.
- Art. 2; Modificación de la tercera, cuarta y undécima disposiciones complementarias finales de la Ley 30096.
- Art. 3; Incorporación del artículo 12 a la Ley 30096.
- Art. 4; Modificación de los artículos 158, 162 y 323 del CP.
- Art. 5; Incorporación de los artículos 154 - A y 183 - B del CP.

La única Disposición Complementaria Derogatoria; Anula el Art. 6 de la Ley 30096.

3. Objeto de estudio: Delitos informáticos contra el patrimonio

El capítulo V contiene el Art. 8 referente a fraude informático, que castiga el ejercicio de introducir, diseñar, alterar, borrar, suprimir y clonar datos informáticos en detrimento de un tercero. Tal como expresa.

Art. 8°. “El que deliberadamente 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”.

El artículo actual resulta un injusto penal contra el patrimonio porque sanciona diversas conductas delictivas, entre ellos, que para su

mejor interpretación haremos uso de la RAE (2019) para su mejor comprensión:

Diseño (proyecto, plan que configura algo),

Introducción (introducir: entrar, ingresar en un lugar),

Alteración (alterar: dañar, estropear, descomponer),

Borrado (borrar: quitar, desvanecer, hacer que desaparezca algo),

Supresión (suprimir: hacer desaparecer, hacer cesar*)*,

Clonación (clonar: producir clones*)*

De datos informáticos o cualquier interferencia, o manipular (operar con las manos o con cualquier herramienta*)* el funcionamiento de una aplicación informática, para procurar (adquirir o conseguir algo) un favor para uno o para otro en menoscabo de una tercera persona; y por el modo como está redactado, trae desconcierto al momento de interpretarla, y los comportamientos inadecuados, “diseñar, introducir, alterar, borrar y suprimir” así no enlazan en la infracción de fraude, estos comportamientos son adecuados de la infracción de daño, que viene hacer una infracción de efecto porque no es necesario desempeñar con modo penal para que se ejecute la infracción de fraude, que también, es ineludible que ese quehacer marche sucesivo de una consecuencia alejada del mismo comportamiento que radica en causar un perjuicio a tercero, de otra manera, la infracción quedaría en tentativo. En el tema de la clonación de tarjetas del banco de la nación*,* el fraude informático afecta las personas vulnerables que están recibiendo el bono frente al COVID 19, consignados al soporte social.

Este Art. 8 de la ley especial es conforme el Art. 8 del Tratado de Budapest (2001), uno y otro de los artículos condenan la utilización indebida de datos informáticos, la manipulación de la actividad del sistema mismo.

Pero dicho artículo hace referencia tal y conforme manifiesta en su contexto de los delitos informáticos en materia de estudio contra el patrimonio.

1.3.3. Análisis jurisprudencial o casuística

1. Internacional

Análisis de la Sentencia Núm. 159/2018

El Tribunal Supremo de la Sala de lo Penal con fecha de sentencia: 05-04-2018. Tipo de procedimiento: Recurso Casación, número del procedimiento: 1061/2017.

Los hechos nacen en un caso en ESPAÑA de Estafa piramidal. Asociación ilegal. Donde los acusados Raquel y Blas establecieron una organización con la que enriquecieron indebidamente y ocultaron las ganancias así conseguidas, por medio de la puesta en marcha de un sistema defraudatorio, a través de Internet, que afectó a una gran elevada representación de individuos en todos los países. La sociedad organizada captaba a clientes e inversores bajo el ofrecimiento de altísimos créditos, a quienes se pagaban unos falsos beneficios con las contribuciones de los nuevos inversores, sin que en situación preexistiera ninguna labor financiera o comercial que originara renta alguna.

Según la sentencia castiga a los dos demandantes como autores comprometidos de una infracción continuada de estafa agravada por el importe de la defraudación, en concurso absoluto con una infracción de apariencia en escrito oficial. Potencialmente pena a los recurrentes como autores comprometidos de una infracción de blanqueo de capitales y otra de asociación ilegal.

Sin embargo, los dos demandantes establecen una objeción conjunta en la que deliberan en los dos primeros motivos, la correcta enervación de su derecho primordial a la presunción de inocencia, desde el aspecto de la trasgresión en la producción de la prueba, y consiguientemente, desde la inopia de la estrecha labor probadora.

Como antes ya detallados los sucesos y el procedimiento de la sentencia, se demuestra en el fallo que se desecha el recurso de Casación introducido por el representante procesal de don Blas y doña Raquel, contra sentencia decretada el día 10 de marzo de 2017 en causa seguida contra ellos mismos y otros, por delitos de

estafa, blanqueo de capitales, falsificación en documento mercantil y asociación indebida.

Acusan a los culpables el pago por mitad de los gastos producidos en el vigente exhorto.

2. Nacional

Análisis de la R. N. N.° 2041-2018 – Lima de la Corte Suprema de Justicia de la República. Sala penal permanente.

Se trata de los recursos de nulidad interpuestos por los encausados Luis Miguel Salinas Torrez y Jesús Alberto Horna Salazar y por la Procuraduría Pública de Orden Público del Ministerio del Interior contra la sentencia del dieciocho de septiembre de dos mil dieciocho (foja 647), en el extremo en el que determinó la reparación civil solidaria en S/ 30000 a favor del Estado y en S/ 16000 a favor de la empresa Selme S. A. C., sin detrimento de reembolsar la suma ilegalmente transferida a la empresa agraviada. De acuerdo en parte con lo juzgado por el señor fiscal supremo en lo penal. La Sala Penal Permanente de la Corte Suprema de Justicia de la República tomando la siguiente decisión: I. Haber Nulidad en la sentencia del dieciocho de septiembre de dos mil dieciocho (foja 647), en el extremo en el que estableció en S/ 16000 el monto de la reparación civil que deberán abonar solidariamente Luis Miguel Salinas Torrez y Jesús Alberto Horna Salazar, con el condenado Ángel Stiven Orozco Ramos, a favor de la empresa Selme S. A. C.; Reformándola, fijaron en S/ 4000 la reparación civil solidaria a favor de la empresa Selme S. A. C., sin deterioro de restituir la suma indebidamente transferida a la referida empresa. II. No Haber Nulidad en la acotada sentencia, en cuanto a que fijó la reparación civil solidaria en S/ 30000 a favor del Estado; con lo demás que al respecto tiene y es materia del recurso.

Análisis de la sentencia 1100/2020 del Tribunal Constitucional.

La sentencia del 16 de junio de 2017, se sancionó al beneficiario a diez años de pena privativa de la libertad efectiva, que resultó de la sumatoria siguiente: ocho años por la infracción de fraude informático y dos años de pena privativa de la libertad efectiva y falsificación de firma en documento privado. Consecutivamente, según la Resolución de 26 de diciembre de 2017, lo redujo el castigo a seis años de pena privativa de la libertad efectiva, por ambos delitos.

Además, se establece que se condenó al beneficiario a través de una normativa que no se hallaba vigente al instante que se realizaron los sucesos delictivos, pues tales sucesos sucedieron durante los meses de enero, febrero, marzo, julio, septiembre y octubre de 2013, pero fue condenado mediante la Ley 30096, que ingresó en vigencia el 23 de octubre de 2013, por lo que la norma aplicable era el Art. 185 del CP, que en su modo agravado era el Art. 186, numeral 3 del referido código. Este Tribunal aprecia que durante la vigencia del primer párrafo del Art. 8 de la Ley 30096, con el agravante comprendido en el inciso 2 del artículo 11, se sancionaba la infracción de fraude informático. Conforme la Resolución del 26 de diciembre de 2017, al actor se le imputó en total ocho años de pena privativa de la libertad efectiva por las infracciones de fraude informático y falsificación de firma en documento privado, vigente al momento de los hechos y que se encontraba dentro del marco normativo del primer párrafo del Art. 8 de la Ley 30096 y del primer párrafo del Art. 427 del CP.

Concluyendo el TC donde declara infundada la demanda.

1.4. Formulación del problema.

¿La normativa penal actual sobre delitos informáticos, protege el patrimonio de las personas naturales y jurídicas en la Corte Superior de Justicia del Santa, Chimbote?

1.5. Justificación e importancia del estudio.

Este trabajo investigativo se explica, en la medida que el desarrollo del tratamiento penal en las infracciones informáticas hacia el patrimonio de las personas naturales y jurídicas, como es la estafa, el hurto, el fraude y el sabotaje informático, así mismo, se trata sobre el desarrolla de la ciberdelincuencia como producto del adelanto de las TIC y de los delitos informáticos, que se facilitan en los datos y sistemas informáticos, hacia la persona o hacia la empresa.

Según Trujillo en línea del 18 de octubre del 2022, señala que en nuestro país el fraude informático y la suplantación de identidad son las infracciones informáticas que más atentan con el patrimonio jurídico y natural y son los más denunciados. Hasta abril del año 2022 se reportaron más de 7,00 denuncias ingresadas en el Ministerio Público en todo el país. De este total, 5,356 son infracciones informáticas tipificadas.

En la División de Investigación de Delitos de Alta Tecnología (Divindat) de la Policía, se registran aproximadamente 300 denuncias de infracciones informáticas cada mes, lo que conlleva a que surja una mayor demanda de soluciones en el servicio de seguridad y vigilancia en el país.

El Grupo Eulen Perú, compañía especializada en soluciones integrales y servicios auxiliares, reveló que la industria de seguridad electrónica es uno de los que más crecimiento ha reportado desde el 2018, teniendo en el 2020 y 2021 (con la pandemia) sus mayores picos de ascendencia, superando la valla del 40%.

Se observa actualmente que existen distintos cambios de la forma penal concerniente a las infracciones informáticas, en esta dirección, lo que anteriormente se sistematizaba de manera rápida en el código Penal, hasta ahora es regulado mediante la Ley Nº 30096 y su respectiva reforma. Por dicho motivo, se considera que hay una inseguridad legal para la penalidad de las infracciones informáticas, debido a que la normatividad efectiva no consigue alcanzar y no concuerda con los sucesos que deberían ser castigados, es, además, un sinnúmero de infracciones informáticas que no son descubiertos por el alto sofisticación de los procedimientos que se hace en la red sucia o negra.

La actual ley especial N° 30096 de los delitos informáticos y su rectificatoria ley N° 30171 en el Perú, permite normar estas renovadas maneras de transgredir. Por lo tanto, el parlamentario ha incumplido en ligerezas normativas e imprecisiones, ya que algunas formas penales ya son reguladas por el CP, sobreponiéndose las formas penales.

Este trabajo de investigación es importante porque recoge notabilidad jurídica y académica, toda vez que trata de un tema actual que viven las personas naturales y jurídicas, son tal vez escasas los trabajos de investigación ejecutadas en relación a las infracciones informáticas hacia el patrimonio. En este orden de opiniones, así mismo hay un nuevo escenario primordial de preferencia de la investigación es las formas de las infracciones informáticas hacia el patrimonio como es la estafa, fraude, sabotaje y hurto, por lo tanto, se propone la modificación del Art. 8 de la actual Ley Nº 30096 con el propósito de proteger el patrimonio de las personas naturales y jurídicas.

1.6. Hipótesis.

Si se modifica y aplica adecuadamente la normativa penal sobre delitos entonces se protegerá el patrimonio de las personas naturales y jurídicas.

1.7. Objetivos

Objetivo General

Determinar los efectos jurídicos de la modificatoria de la ley de delitos informáticos para proteger el patrimonio de las personas naturales y jurídicas en la Corte Superior de Justicia del Santa, Chimbote.

Objetivos Específicos

1. Conocer los fundamentos teóricos del tipo penal de los delitos informáticos en la doctrina nacional y comparada.
2. Analizar jurisprudencialmente los elementos del tipo penal de los delitos informáticos.
3. Plantear la modificación del Art. 8 de la Ley Nº 30096 con el fin proteger el patrimonio de las personas naturales y jurídicas.

II. Material y método

2.1. Tipo y diseño de investigación

Tipo de investigación mixto, en el nivel propositivo

Tipo mixto porque conjuga las dos formas de investigación cualitativa y cuantitativa, que al ser conjugadas se genera un nuevo tipo de investigación como el que se presenta en nuestro estudio. Asimismo, Hernández (2018) refiere que la Investigación entrelaza a la cualitativa y cuantitativa, la mezcla, pero es más que la adición de las dos anteriores e involucra su interacción y potenciación. Los métodos híbridos o mixtos simbolizan un conjunto de procesos críticos, sistemáticos y empíricos de investigación e involucran el recojo y la interpretación de datos tanto cualitativos como cuantitativos, así como su combinación y discusión conjunta. (p.10).

Nivel propositivo porque se cimenta en la necesidad o vacío adentro de la ley, una forma que se tome la información relatada, se realizará una propuesta para plantear la modificación del Art. 8 de la actual Ley Nº 30096 con el propósito de resguardar el patrimonio de las personas naturales y jurídicas.

Diseño no experimental

Esta clase de diseño busca que la investigación se realice sin maniobrar intencionadamente las variables. Tal como Hernández (2018) afirma que el diseño se hace sin maniobrar intencionadamente las variables. Es decir, se refiere de estudios en los que no haces alterar en forma intencional las variables independientes para notar su resultado sobre otras variables. Lo que verificas en la investigación no experimental es ver o medir fenómenos y variables tal como se dan en su situación natural, para examinarlas. (p. 174).

Se fundamenta en la percepción de situaciones tales y como se dan en su contexto real para después examinarlos. En este diseño se busca presentar los resultados en tablas y describir y revisar la jurisprudencia respectiva.

2.2. Población y muestra

Población

El tratadista Hernández y otros (2018, p.199) afirma que el universo o población, es el conjunto de todos los casos que conciertan con determinadas especificaciones. El trabajo presente investigativo, la población su es escenario es la Corte Superior de Justicia del Santa de Chimbote, estando compuesta por, los especialistas del derecho, jueces de primera y segunda instancia penal, fiscales, personal especialista en derecho informático y abogados litigantes de la región de Ancash.

Muestra

La muestra en este caso no probabilística, el nombramiento de los componentes no obedece de la probabilidad, sino de causas conexas con las peculiaridades de la indagación o las intenciones del investigador. El proceso no es mecánico ni es basado en fórmulas de probabilidad, sino que obedece del proceso de toma de decisiones de un investigador o de un equipo de investigadores y, desde pronto, las muestras selectas dependen a otros criterios de investigación. (Hernández y otros, 2018, p. 215).

La muestra de la investigación está constituida por 50 informantes, conforme se detalla a continuación:

Participantes	Cantidad
Jueces	05
Fiscales	05
Abogados litigantes	30
Personal Especializado	10
TOTAL	**50**

Elaboración: Propia

2.3 Variables, operacionalización

Variable Independiente:

Para Sánchez y Reyes (1998). Denominada experimental o causal. Variable que se presume es el componente que causa, condiciona o afecta de manera precisa a la variable dependiente. (p.50)

La investigación presente, la variable independiente es: Artículo 8 de la ley 30096.

En lo referido a esta variable, el actual Art. 8 de la Ley Nº 30096, tipifica el fraude informático, en lo que se propone a través de un proyecto de ley la modificatoria de dicho artículo contra el patrimonio para proteger a las personas naturales y jurídicas, con el fin, de hacer efectiva y con el mejor tratamiento penal.

Variable dependiente:

Para Sánchez y Reyes (1998). Denominada condicionada o efecto. Variable que deriva presumida por la disposición de la variable independiente. (p. 50)

En la presente investigación la variable dependiente es: Tratamiento penal de delitos informáticos contra el patrimonio.

Lo referido a esta variable el tratamiento penal es doctrinario, jurisprudencial y normativo, fundamentalmente en el objeto de estudio de las infracciones informáticas hacia el patrimonio en las personas naturales y jurídicas en la Corte Superior de Justicia del Santa, Chimbote.

Operacionalización de Variables:

Variables	Dimensiones	Indicadores	Ítem	Técnica e Instrumento de recolección de datos
V.I Artículo 8 de la ley 30096	Tecnologías de la información y comunicación	Medir el mal uso de las tecnologías de la información y comunicación y el provecho ilícito que se comete fraude informático	Escala de Likert	Técnica: *Encuesta.* Instrumento: *Cuestionario*
V.D Tratamiento penal de delitos	Personal especializado	Ingenieros y licenciados informáticos		

informáticos contra el patrimonio	Manipulación de sistemas informáticos	Introducción, alteración, borrado, supresión, clonación de datos informáticos que se produce en prejuicio de terceros mediante el uso de la tecnología.		

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

Técnicas:

Observación: Permite instruir la muestra en sus oportunas actividades de grupo y personal. Conociendo: Qué, quién, cómo, cuánto, cuándo, porqué, etc.

Encuesta: Técnica personalizada que accedió adquirir información a través de interrogaciones en forma directa, personal y verbal; se formuló diez preguntas, en base a la escala de Likert a especialistas jurídicos e informáticos.

Fichaje: Técnica que se utiliza especialmente para recolectar y almacenar información, lo cual le confiere unidad y valor propio.

Técnica de gabinete: Cuyo propósito es conocer un argumento de trascendencia, entre un grupo con definitivos compromisos y con la finalidad inmediata de tomar decisiones.

Técnica de análisis documentario: Son operaciones orientadas a personalizar un escrito y su contenido bajo un tipo disímil de su modo original, con el objetivo de facilitar su recuperación ulterior e identificarlo.

Instrumentos:

Cuestionario: Se fundamenta en preguntas y otras indicaciones con la finalidad de conseguir respuesta de los entendidos. A modo están planteados para poder efectuar un análisis estadístico de las contestaciones. El cuestionario de la investigación consta de diez preguntas con cinco ítems en escala de Likert.

Fichas:

Textuales son las que se copian literalmente un fragmento de un libro, revista o folleto.

Bibliográficas son las que tienen la información de tipificación de un libro, artículo escrito sobre el ente de averiguación.

Para acopiar la indagación suficiente y precisa para conseguir los propósitos del estudio, se hizo uso del procedimiento de análisis documental, cuyos instrumentales fueron las fichas de resumen, de comentario, de parafraseo y bibliográficas. Lo preliminar admite formalizar un proyecto de proceso, textuales y examinación de la información, establecidos en los propósitos investigativos. Así poder vincular la información en un cualquier análogo y lógico; pensando una distribución razonable, un esquema o una teoría que complete esa pesquisa se utilizó el procedimiento de argumento jurídico.

2.5. Procedimiento de análisis de datos

Recolección de datos: Fundamenta en conseguir los datos e información, antecedentes del fenómeno de estudio, a través de los métodos de la observación, el examen documental y la encuesta.

Revisión de los datos: Hace una diagnostico extenso de la información alcanzada a fin de confirmar de modo general los datos conseguidos

Organizar los datos e información: Organizó la información obtenida en tablas y gráficos estadísticos (columna, barras, circular, ojivas, etc.) haciendo uso de Excel, Power Point, con el fin de organizar adecuadamente los efectos de la indagación.

Codificación de datos: Enfoca en niveles: Genera unidades de significado y categoría y, aborda textos y correspondencia entre conceptos, en consecuencia, el fortalecimiento de los dos niveles originó una teoría en base a los datos o información lograda.

Los respectivos datos que se lograron con los procedimientos usados fueron valorados con respecto a la teoría del Argumento Jurídico, toda cuando el Derecho puede entenderse como demonstración de la destreza para lucir sensibles argumentos con el propósito de demostrar una actitud.

2.6. Criterios éticos

En la investigación estarán presentes las consideraciones éticas siguientes: el respeto a la dignidad de cada sujeto de investigación, responsabilidad y libertad para desarrollar la investigación y el principio de doble efecto, garantizando que la investigación no producirá ningún daño.

Honestidad: Es una cualidad propia del investigador que tiene una clara concordancia con los principios de verdad, justicia y con la entereza moral.

Originalidad: Cualidad propia del investigador que se le da a una creación que no fue copiada o imitada, está asociada a algo que es novedoso y que puede ser utilizado para realizar réplicas semejantes.

Justicia: Es una cualidad de obrar y juzgar, teniendo como principio la verdad, de tal modo que el diseño del estudio admita que las obligaciones y los beneficios estén compartidos de manera equitativa entre los grupos de sujetos de investigación.

Libertad: Es un derecho esencial intangible en beneficio del investigador para impedir interferencias o intromisiones en el perfeccionamiento de su labor.

Integridad científica: Manera de la práctica de la investigación, e implica responsabilidad, honestidad, justicia y transparencia. Por lo que comunica las nociones de integridad y solidez moral.

Validez científica: La investigación es elaborada con procedimiento adecuado que atestigüe que los resultados manifestarán a las interrogantes que causaron la investigación.

Finalmente, el investigador hizo uso de la confidencialidad de los datos logrados, la comunicación de los resultados y el manejo de los datos para fines académicos.

2.7. Criterios de Rigor científico

El trabajo investigativo tiene el rigor científico requeridos por la entidad académica, cuando las fuentes que se utilizan en el proceso son honestas, con la correspondida indicación de la fuente de acuerdo a los estándares internacionales bibliográficas, en este estudio, el empleo de las normas APA.

El estudio de investigación se plasma con las razones de fiabilidad, validez, credibilidad y transferibilidad:

Fiabilidad: Es la eventualidad de responder saberes, que un indagador utilice los similares procedimientos de recojo de información que otro, y consiga efectos análogos. Este razonamiento testifica que los efectos personalizan un tanto indiscutible y verídico, y las contestaciones que proveen los participantes son autónomos de los contextos del estudio.

Validez: Es la definición acertada de las consecuencias que se cambie en una columna primordial de las indagaciones. La manera de acopiar los datos, de llegar a seducir los hechos y las prácticas desde diferentes puntos de vista, el poder examinar y comentar la realidad a partir de un equipaje teórico y experiencial, el ser meticuloso en examinar persistentemente los descubrimientos.

Credibilidad: Es el nivel de las consecuencias de la exploración que reflejan una fotografía precisa y típica de un contexto dado. Los resultados del trabajo investigativo son fehacientes a la situación, lográndose garantizar en los fundamentos únicos que se hallan en las referencias e inclusive, confirmando verdaderamente con los informadores.

Transferibilidad: Los resultados del trabajo, se averigua desarrollar las ideas sobre el contenido o finalidad de estudio a otras áreas análogas, es indicar, las consecuencias de la actual indagación son necesarias en demás argumentos afines.

III. RESULTADOS

3.1. Resultados en Tablas y Figuras

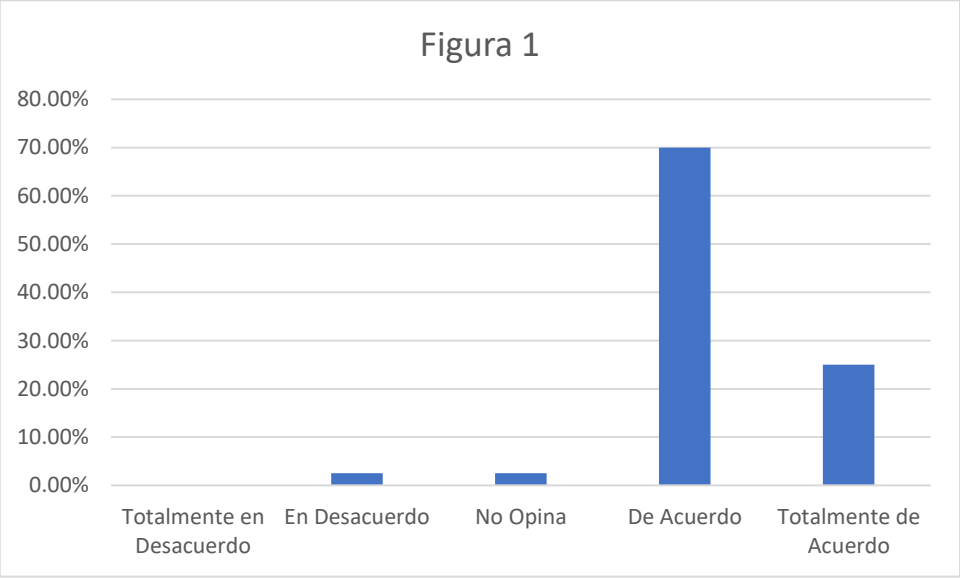
Tabla 1

¿Considera usted que el avance de las TI (tecnologías informáticas) ha acrecentado los delitos informáticos?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0.00%
En Desacuerdo	1	2.50%
No Opina	1	2.50%
De Acuerdo	28	70.00%
Totalmente de Acuerdo	10	25.00%
Total	40	100.00%

Fuente: Elaboración propia

Figura 1



Como se puede evidenciar en este gráfico respecto a que el rápido adelanto de las TIC ha acrecentado los delitos informáticos, se constituye el 70.00% de los jueces, fiscales y abogados se mostraron de acuerdo, el 25.00% está totalmente de acuerdo, y el 2.50% está en desacuerdo y así mismo no opina.

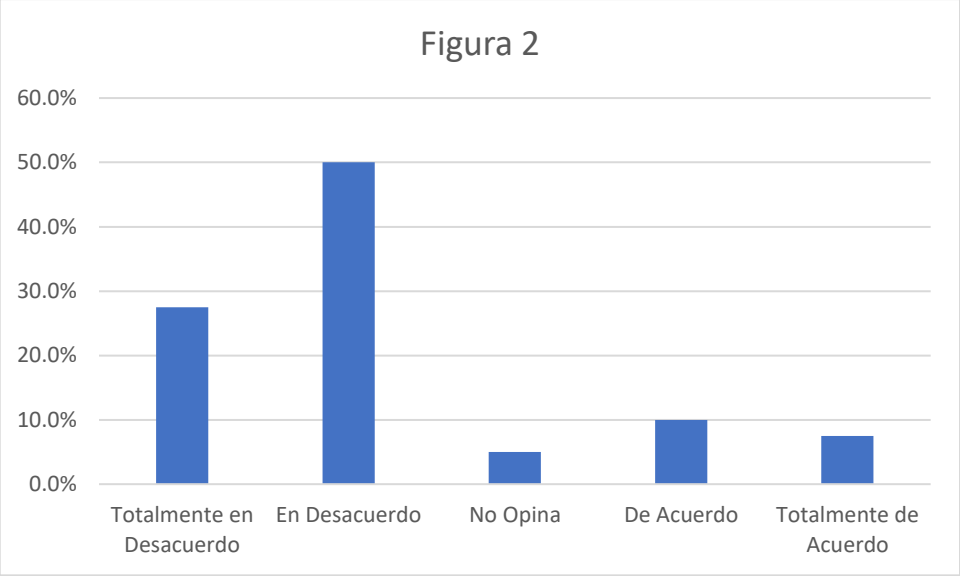
Tabla 2

¿Considera usted que hay eficacia de la legislación para penar las nuevas formas criminales con el empleo de las TIC?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	11	27.5%
En Desacuerdo	20	50.0%
No Opina	2	5.0%
De Acuerdo	4	10.0%
Totalmente de Acuerdo	3	7.5%
Total	40	100.00%

Fuente: Elaboración propia

Figura 2



Como se puede evidenciar en este gráfico, se funda el 50.00% de los jueces, fiscales y abogados se mostraron con el desacuerdo, el 27.50% están totalmente con el desacuerdo, el 10.00% están con el acuerdo, el 7.50% se mostraron en totalmente de acuerdo y el 5.00%, así mismo no opina.

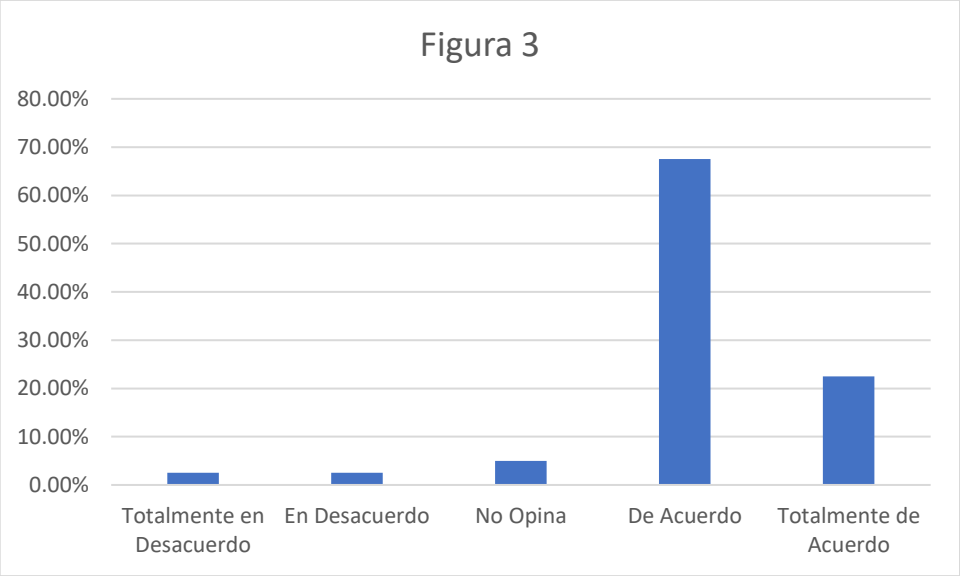
Tabla 3

¿Considera usted que existe prevención de las entidades bancarias para denunciar penalmente delitos de fraude informático de las cuentas bancarias y otros?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	1	2.50%
En Desacuerdo	1	2.50%
No Opina	2	5.00%
De Acuerdo	27	67.50%
Totalmente de Acuerdo	9	22.50%
Total	40	100.00%

Fuente: Elaboración propia

Figura 3



Como se evidencia en este gráfico, se constituye el 67.50% de los jueces, fiscales y abogados se mostraron de acuerdo, el 22.50% está totalmente de acuerdo, el 5.00% no opina, y el 2.50% está en desacuerdo, así mismo totalmente en desacuerdo.

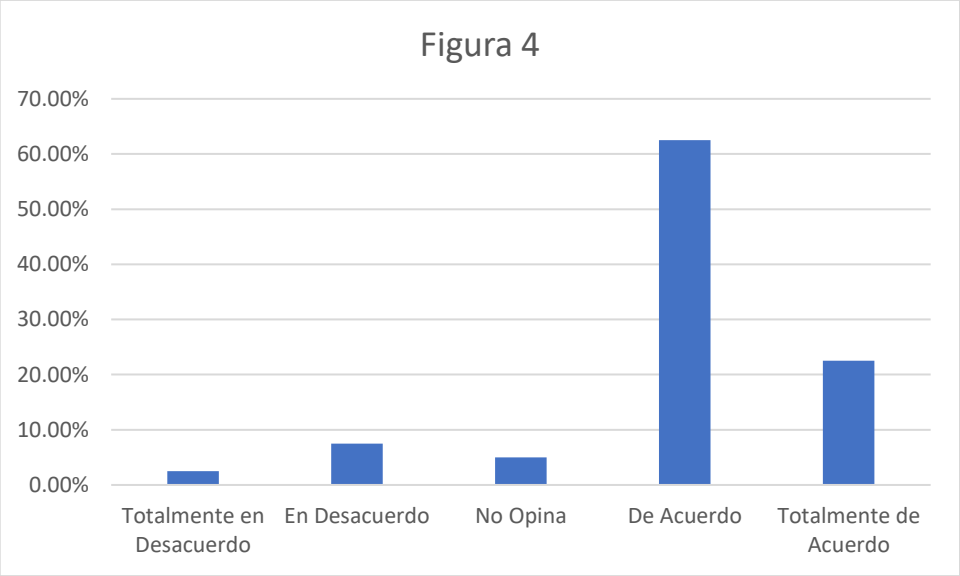
Tabla 4

¿Considera usted que existe procedimientos claros en la prevención y sanción de delitos de fraude informático?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	1	2.50%
En Desacuerdo	3	7.50%
No Opina	2	5.00%
De Acuerdo	25	62.50%
Totalmente de Acuerdo	9	22.50%
Total	40	100.00%

Fuente: Elaboración propia

Figura 4



Como se puede evidenciar en este gráfico, se construye el 62.50% de los jueces, fiscales y abogados se mostraron de acuerdo, el 22.50% está totalmente con el acuerdo, el 7.50% está con el desacuerdo, el 5.00% no da una opinión y el 2.50% está en totalmente en desacuerdo.

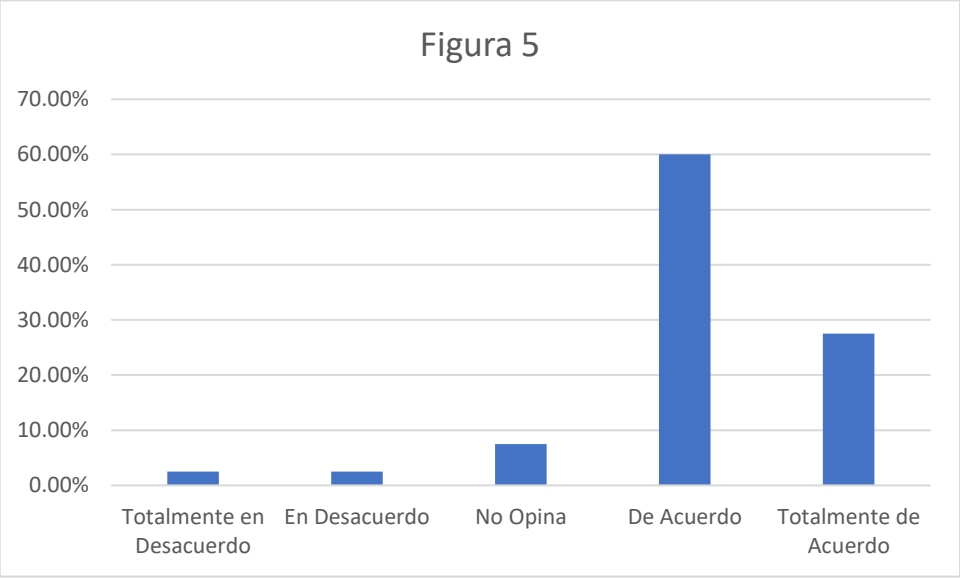
Tabla 5

¿Considera usted que la seguridad de las plataformas digitales para efectuar las compras y contratar servicios por medio del Internet, actualmente no se encuentra tipificado en el código penal?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	1	2.50%
En Desacuerdo	1	2.50%
No Opina	3	7.50%
De Acuerdo	24	60.00%
Totalmente de Acuerdo	11	27.50%
Total	40	100.00%

Fuente: Elaboración propia

Figura 5



Como se demuestra en este gráfico, se forma el 60.00% de los jueces, fiscales y abogados se mostraron de acuerdo, el 27.50% está totalmente de acuerdo, el 7.50% no opina y el 2.50% está en totalmente en desacuerdo, así mismo en desacuerdo.

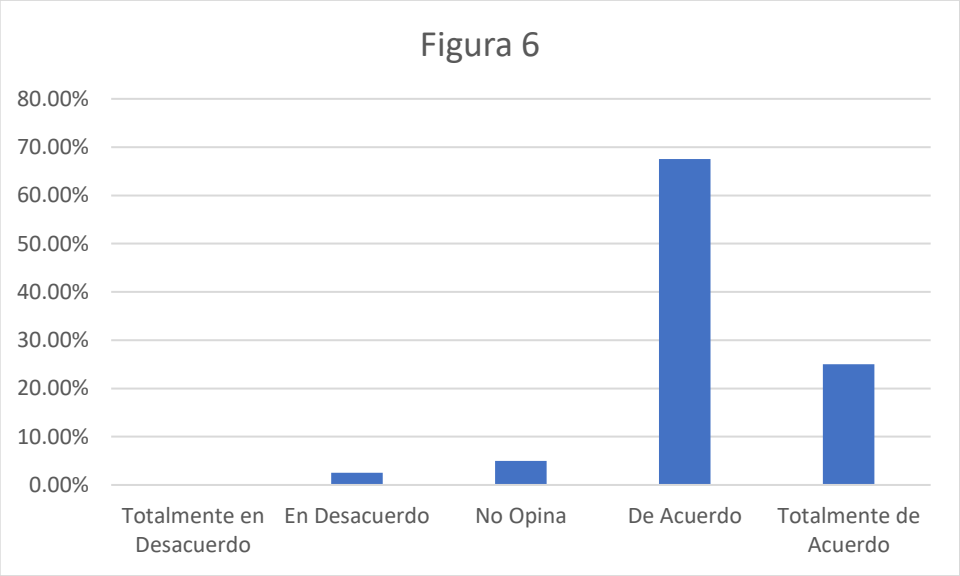
Tabla 6

¿Considera que se produce una afectación al patrimonio del perjudicado con el sabotaje y hurto de la información del software en la red?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0.00%
En Desacuerdo	1	2.50%
No Opina	2	5.00%
De Acuerdo	27	67.50%
Totalmente de Acuerdo	10	25.00%
Total	40	100.00%

Fuente: Elaboración propia

Figura 6



Como se evidencia en este gráfico respecto a que se produce una afectación al patrimonio del perjudicado con el sabotaje y hurto de la información del software en la red, se implanta el 67.50% de los jueces, fiscales y abogados se mostraron de acuerdo, el 25.00% está totalmente de acuerdo, el 5.00% no opina y el 2.50% está en desacuerdo.

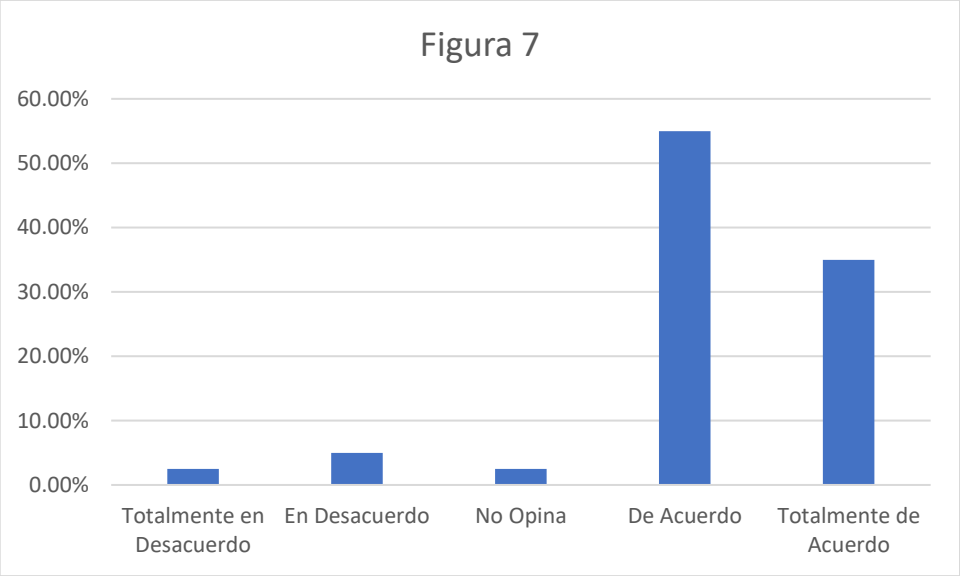
Tabla 7

¿Considera usted que está vigente la norma de los delitos o infracciones informáticas contra el patrimonio y su certeza en prevenir los delitos?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	1	2.50%
En Desacuerdo	2	5.00%
No Opina	1	2.50%
De Acuerdo	22	55.00%
Totalmente de Acuerdo	14	35.00%
Total	40	100.00%

Fuente: Elaboración propia

Figura 7



Como se puede demostrar en este gráfico, se instituye el 55.00% de los jueces, fiscales y abogados se mostraron de acuerdo, el 35.00% está totalmente con el acuerdo, el 5.00% está con el desacuerdo y el 2.50% no brinda opinión, así mismo, totalmente en desacuerdo.

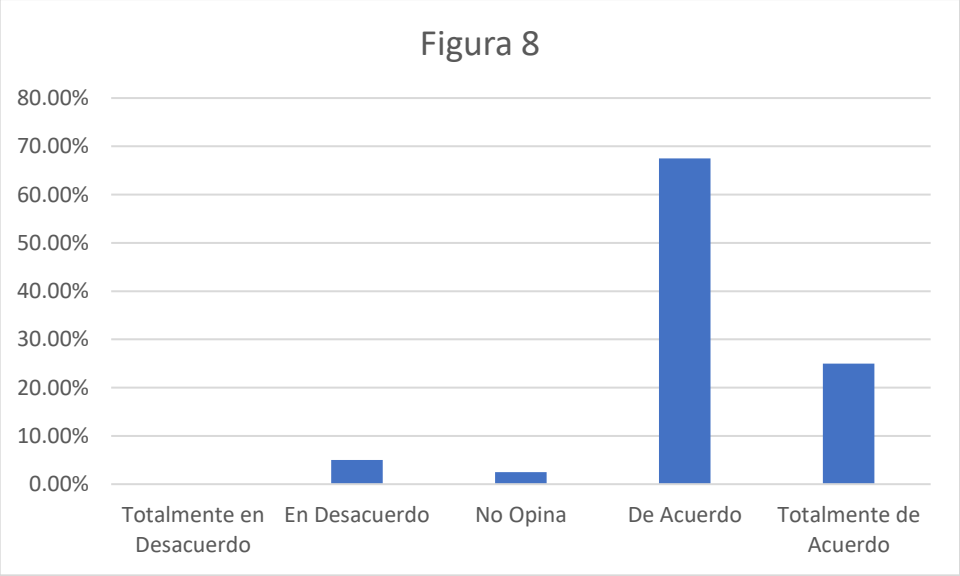
Tabla 8

¿Cree usted que hay el compromiso de reforma legislativa con la prevención y penar los delitos o infracciones informáticas contra el patrimonio?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0.00%
En Desacuerdo	2	5.00%
No Opina	1	2.50%
De Acuerdo	27	67.50%
Totalmente de Acuerdo	10	25.00%
Total	40	100.00%

Fuente: Elaboración propia

Figura 8



Como se evidencia en este gráfico, se funda el 67.50% de los jueces, fiscales y abogados se mostraron de acuerdo, el 25.00% está totalmente con el acuerdo, el 5.00% está con el desacuerdo y el 2.50% no brinda opinión.

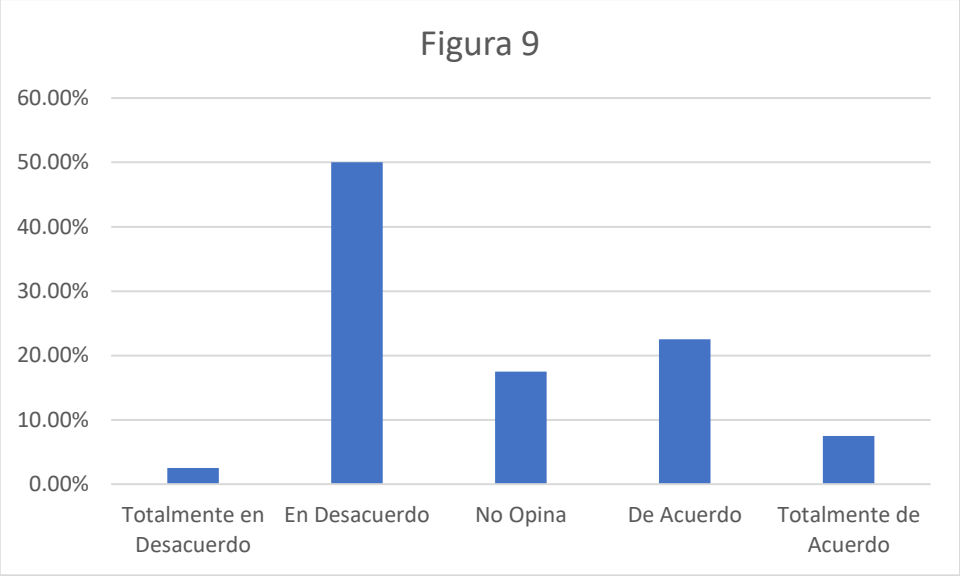
Tabla 9

¿Considera usted que hay norma concreta del delito o infracción de estafa y hurto informático, tipificación y prevención?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	1	2.50%
En Desacuerdo	20	50.00%
No Opina	7	17.50%
De Acuerdo	9	22.50%
Totalmente de Acuerdo	3	7.50%
Total	40	100.00%

Fuente: Elaboración propia

Figura 9



Como se explica en este gráfico, se crea el 50.00% de los jueces, fiscales y abogados se mostraron en desacuerdo, el 22.50% están de acuerdo, el 17.50% no opina, están de acuerdo, el 7.50% están totalmente con el acuerdo y el 2.50% está totalmente con el desacuerdo.

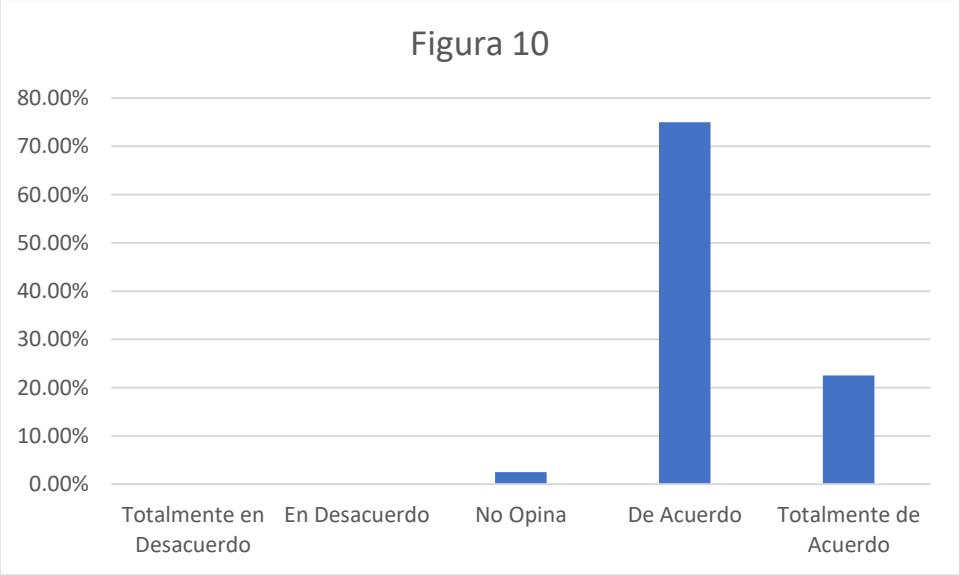
Tabla 10

¿Cree usted que se debe modificar el Art. 8 de la Ley 30096?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0.00%
En Desacuerdo	0	0.00%
No Opina	1	2.50%
De Acuerdo	30	75.00%
Totalmente de Acuerdo	9	22.50%
Total	40	100.00%

Fuente: Elaboración propia

Figura 10



Como se evidencia en el gráfico, se construye el 75.00% de los jueces, fiscales y abogados, se mostraron de acuerdo, el 22.50% está totalmente de acuerdo y el 2.50% no opina.

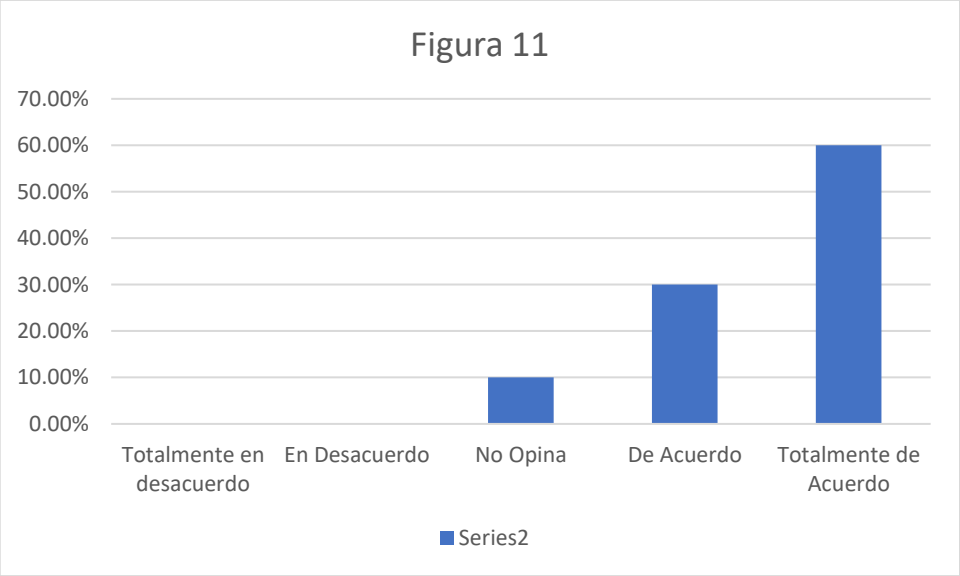
Tabla 11

¿Considera usted que el apresurado avance de las TIC ha acrecentado los delitos informáticos?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0.00%
En Desacuerdo	0	0.00%
No Opina	1	10.00%
De Acuerdo	3	30.00%
Totalmente de Acuerdo	6	60.00%
Total	10	100.00%

Fuente: Elaboración propia

Figura 11



Como se demuestra en el gráfico respecto a que el rápido avance de las TI ha acrecentado los delitos o infracciones informáticas, se establece que el 60.00% de las personas especialistas está totalmente de acuerdo, el 30.00% está en acuerdo y el 10.00% no opina.

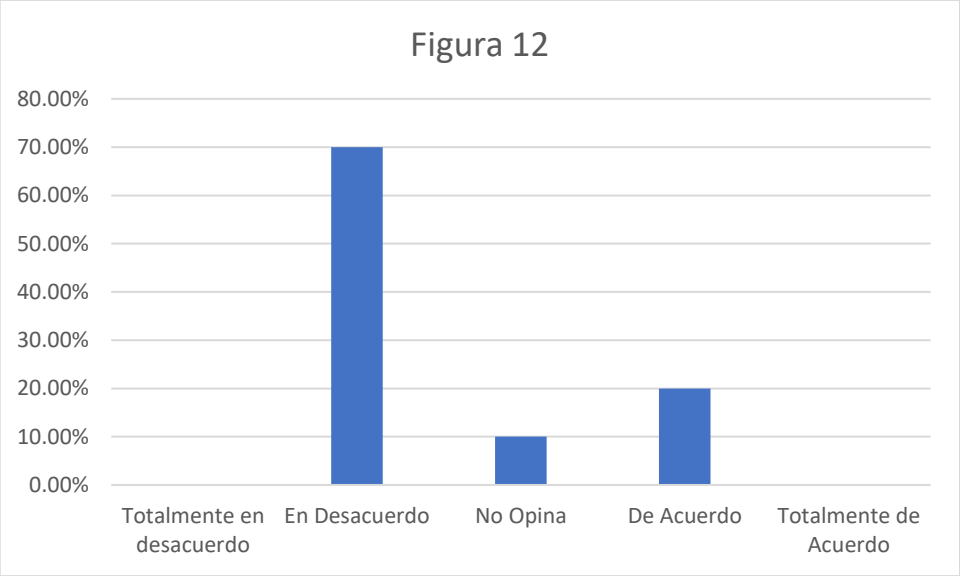
Tabla 12

¿Considera usted que hay eficacia de la legislación para penar las nuevas formas criminales con el empleo de las TIC?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0.0%
En Desacuerdo	7	70.0%
No Opina	1	10.0%
De Acuerdo	2	20.0%
Totalmente de Acuerdo	0	0.0%
Total	10	100.00%

Fuente: Elaboración propia

Figura 12



Como se puede evidenciar en este gráfico, se establece que el 70.00% de las personas especialistas están totalmente en desacuerdo, el 20.00% están en acuerdo y el 10.00% no opina.

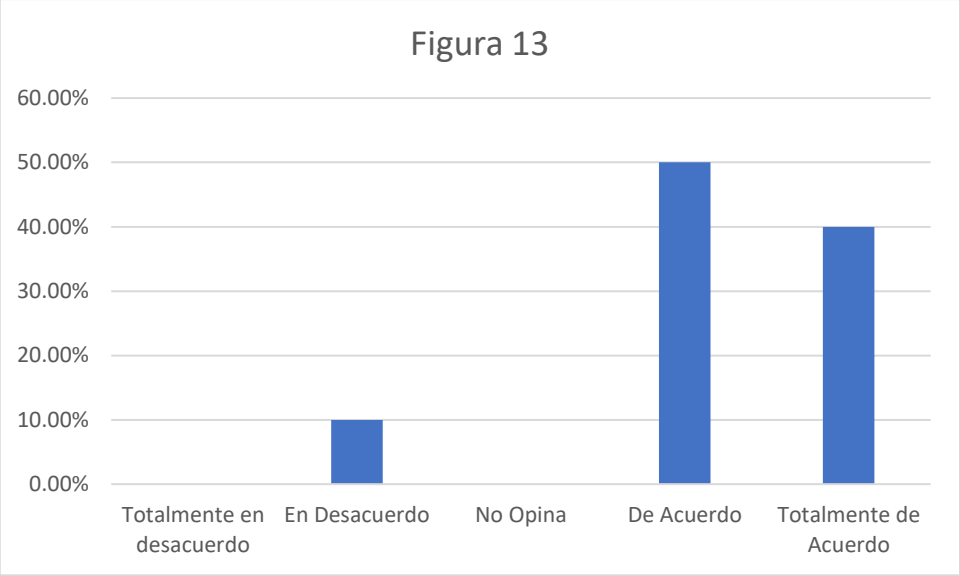
Tabla 13

¿Considera usted que existe prevención de las entidades bancarias para denunciar penalmente delitos o infracciones de fraude informático de cuentas bancarias y otros?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0.00%
En Desacuerdo	1	10.00%
No Opina	0	0.00%
De Acuerdo	5	50.00%
Totalmente de Acuerdo	4	40.00%
Total	10	100.00%

Fuente: Elaboración propia

Figura 13



Como se puede evidenciar en este gráfico, se establece que el 50.00% de las personas especialistas está en acuerdo, el 40.00% está totalmente en acuerdo y el 10.00% está en desacuerdo.

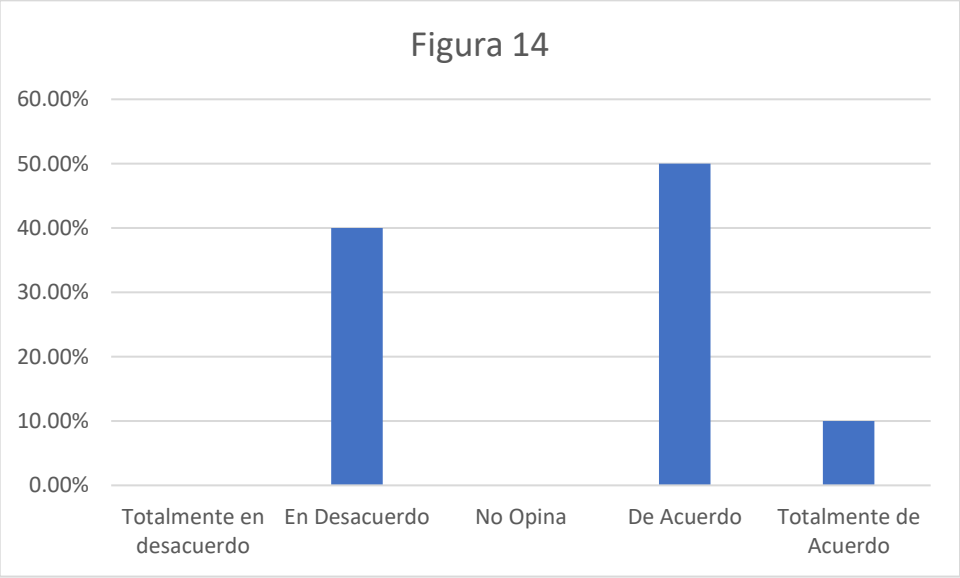
Tabla 14

¿Considera usted que existe procedimientos claros en la prevención y castigo de los delitos o infracciones de fraude informático?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0.00%
En Desacuerdo	4	40.00%
No Opina	0	0.00%
De Acuerdo	5	50.00%
Totalmente de Acuerdo	1	10.00%
Total	10	100.00%

Fuente: Elaboración propia

Figura 14



Como se demuestra en el gráfico, se establece que el 50.00% de las personas especialistas está de acuerdo, el 40.00% está en desacuerdo y el 10.00% está totalmente de acuerdo.

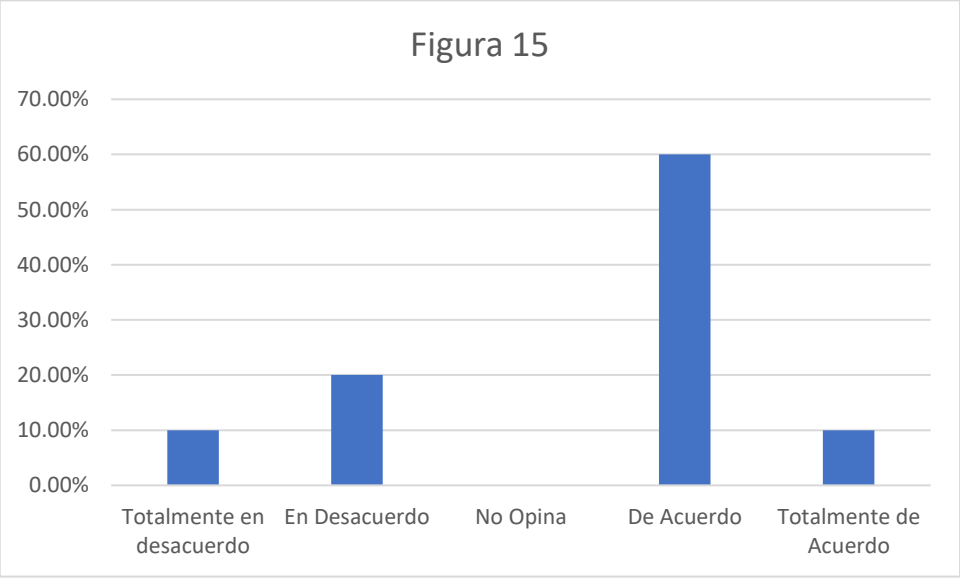
Tabla 15

¿Considera usted que la confianza de las plataformas virtuales para ejecutar compras y acordar servicios a través del Internet son castigados?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	1	10.00%
En Desacuerdo	2	20.00%
No Opina	0	0.00%
De Acuerdo	6	60.00%
Totalmente de Acuerdo	1	10.00%
Total	10	100.00%

Fuente: Elaboración propia

Figura 15



Como se puede evidenciar en este gráfico donde se instituye que el 60.00% de las personas especialistas están de acuerdo, el 20.00% están en desacuerdo, el 10.00% está totalmente con el acuerdo y el 10.00% está totalmente con el desacuerdo.

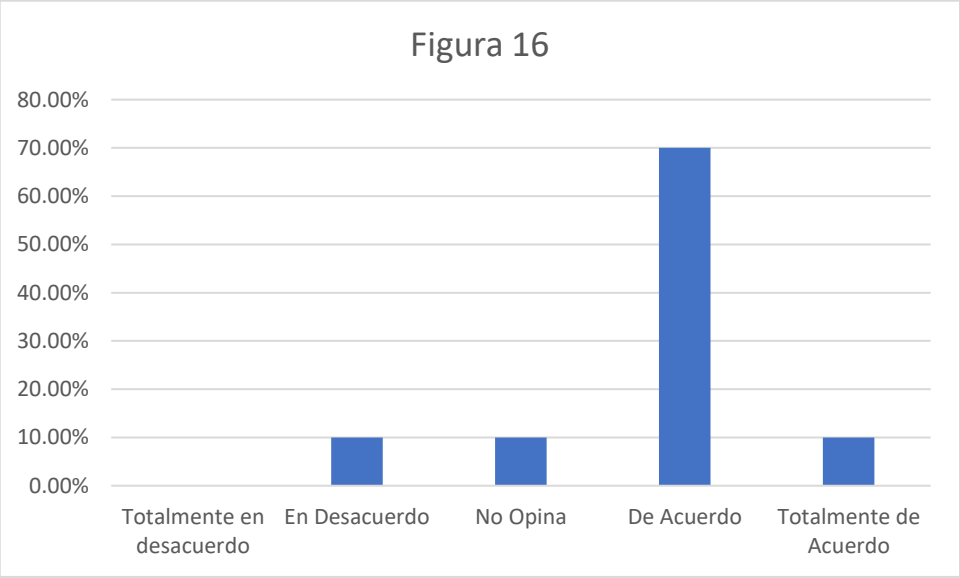
Tabla 16

¿Considera usted que el tratamiento penal del fraude informático crea incertidumbre en su interpretación que no permite una sanción efectiva?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0.00%
En Desacuerdo	1	10.00%
No Opina	1	10.00%
De Acuerdo	7	70.00%
Totalmente de Acuerdo	1	10.00%
Total	10	100.00%

Fuente: Elaboración propia

Figura 16



Como se demuestra en el gráfico respecto a que el tratamiento penal del fraude informático crea incertidumbre en su interpretación que no permite una sanción efectiva se establece que el 70.00% de las personas especialistas está de acuerdo, el 10.00% está totalmente de acuerdo, está en desacuerdo el 10.00% está y el 10.00% no opina.

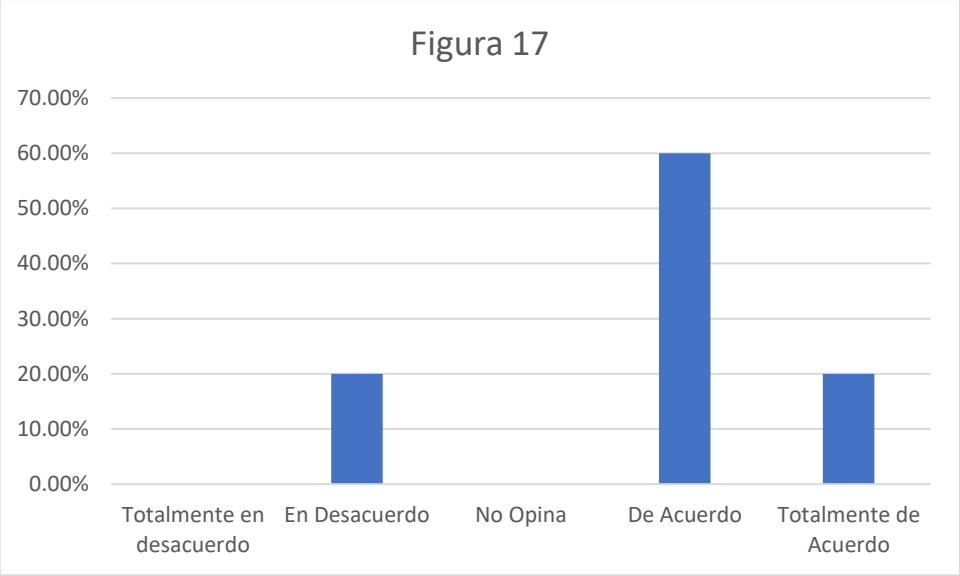
Tabla 17

¿Considera usted que los fiscales que investigan delitos informáticos están realmente capacitados?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0.00%
En Desacuerdo	2	20.00%
No Opina	0	0.00%
De Acuerdo	6	60.00%
Totalmente de Acuerdo	2	20.00%
Total	10	100.00%

Fuente: Elaboración propia

Figura 17



Como se evidencia en el gráfico respecto a que los fiscales que investigan delitos informáticos están realmente capacitados, se establece que el 60.00% de las personas especialistas está de acuerdo, el 20.00% está en desacuerdo y el 20.00% está totalmente de acuerdo.

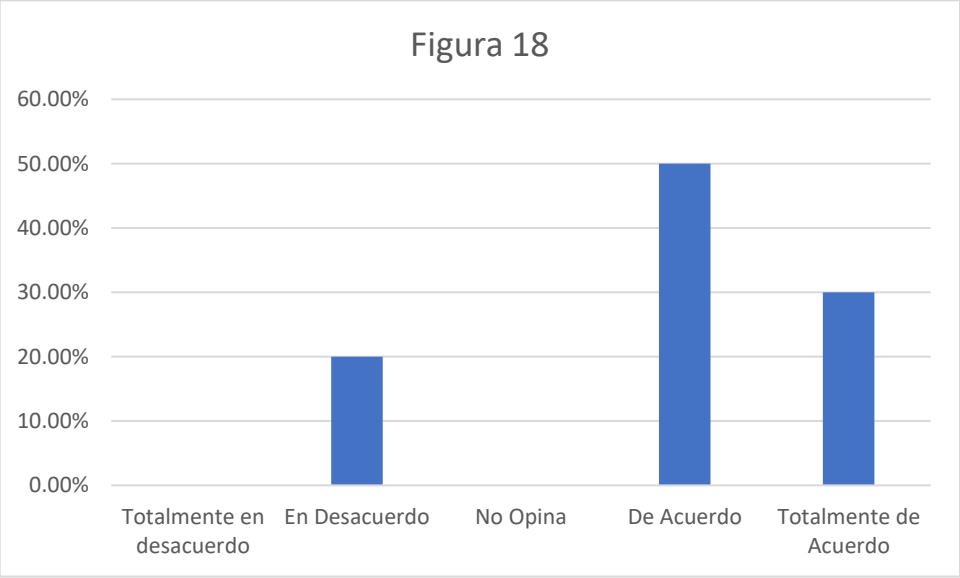
Tabla 18

¿Considera usted que los diferentes operadores del derecho reciben frecuentemente capacitación, sobre el tratamiento penal de los delitos informáticos?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0.00%
En Desacuerdo	2	20.00%
No Opina	0	0.00%
De Acuerdo	5	50.00%
Totalmente de Acuerdo	3	30.00%
Total	10	100.00%

Fuente: Elaboración propia

Figura 18



Como se explica en este gráfico respecto a que los diferentes operadores del derecho reciben frecuentemente capacitación, sobre el tratamiento penal de los delitos o infracciones informáticas, se establece que el 50.00% de las personas especialistas está de acuerdo, el 30.00% está totalmente con el acuerdo y el 20.00% está con el desacuerdo.

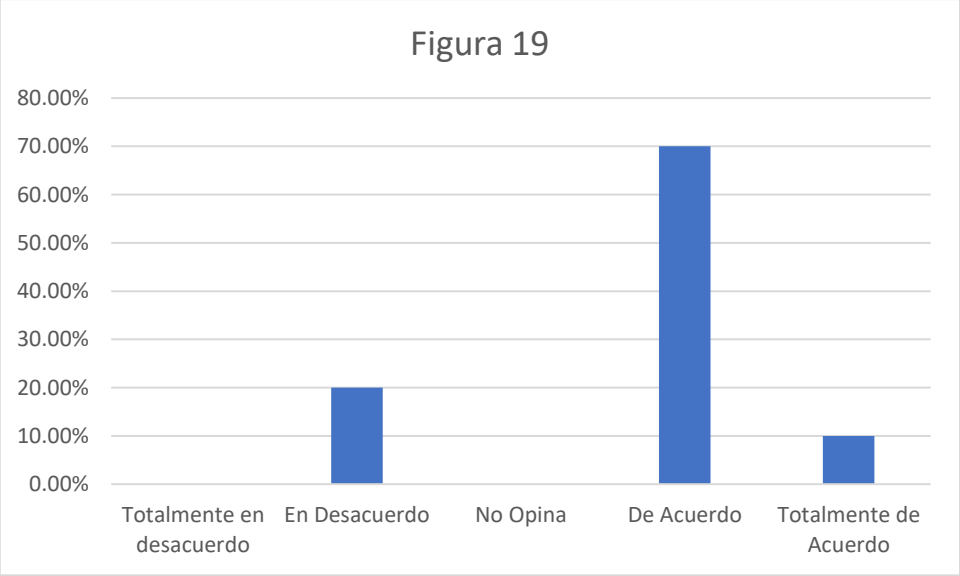
Tabla 19

¿Considera que la ley actual de delitos informáticos no es eficaz para que no se logre muchas sentencias en Chimbote?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0.00%
En Desacuerdo	2	20.00%
No Opina	0	0.00%
De Acuerdo	7	70.00%
Totalmente de Acuerdo	1	10.00%
Total	10	100.00%

Fuente: Elaboración propia

Figura 19



Como se evidencia en el gráfico respecto a la actual ley de delitos informáticos no es eficaz para que no se logre muchas sentencias en Chimbote, se establece que el 70.00% de las personas especialistas se mostraron de acuerdo, el 20.00% está con el desacuerdo y el 10.00% se mostraron totalmente de acuerdo.

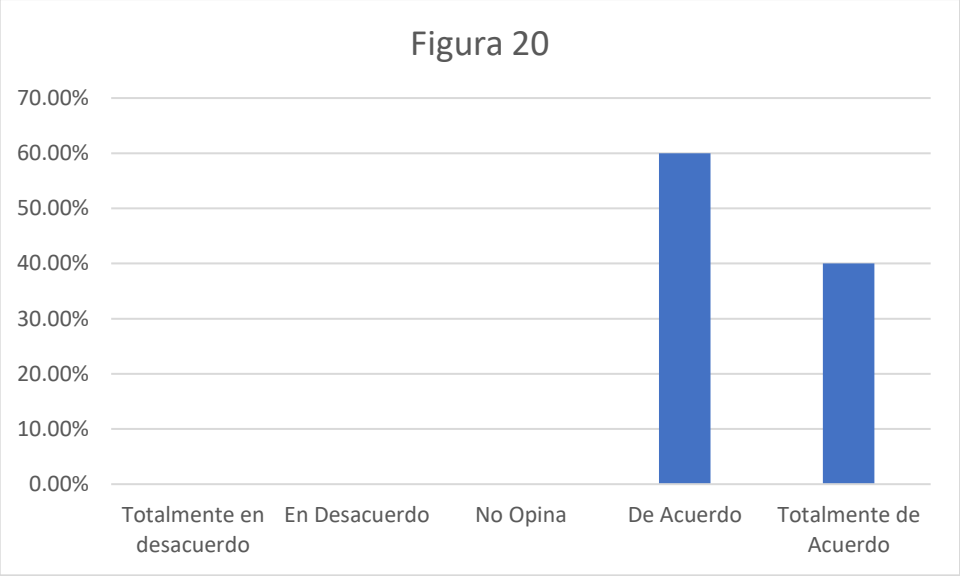
Tabla 20

¿Considera usted que se debe modificar el Art. 8, referente a Fraude informático de la Ley 30096?

Descripción	Frecuencia	Porcentaje
Totalmente en Desacuerdo	0	0.00%
En Desacuerdo	0	0.00%
No Opina	0	0.00%
De Acuerdo	6	60.00%
Totalmente de Acuerdo	4	40.00%
Total	10	100.00%

Fuente: Elaboración propia

Figura 20



Como se demuestra en este gráfico respecto a que se debe modificar el artículo 8 referente a Fraude informático de la Ley 30096, se establece que el 60.00% de las personas especialistas está de acuerdo, y el 40.00% está totalmente de acuerdo.

3.2. Discusión de los resultados

De acuerdo a los resultados conseguidos, según la tabla 01 nos indica que el 70% de los jueces, fiscales y abogados litigantes de la provincia del Santa – Chimbote se mostraron de acuerdo, el 25.00% está totalmente de acuerdo, y el 2.50% está en desacuerdo y así mismo no opina que el acelerado avance de las tecnologías informáticas ha acrecentado los delitos informáticos. Información que al ser confrontados con lo que Bayona (2019), en su estudio investigativo: *El Derecho Informático aplicado al Derecho Penal en el Perú*, dice que el sorprendente e irrefrenable adelanto de las comunicaciones, súplica de la comunidad jurídica el acomodamiento de sus ordenamientos jurídicos para hacer frente a las disímiles expresiones de la informática mencionadas a través de la utilización del Internet, del proceso de datos a través de aplicativos informáticos, el uso de software técnicos, etc., que no son sino equipos necesarios que sin una correcta regulación podrían ser usadas por manos inescrupulosas para realizar hechos ilícitos. (p.10).

Con esos resultados se afirma que el acelerado progreso de las TIC en estos tiempos actuales donde la cibernética, la telemática, la informática y los softwares no son temas ajenos a la ciencia jurisprudencial, para regular los delitos informáticos que se cometen.

Como se puede evidenciar en la tabla 03 detalla que el 67.50% de los jueces, fiscales y abogados litigantes de la provincia del Santa – Chimbote se mostraron de acuerdo, el 22.50% está totalmente de acuerdo, el 5.00% no opina, y el 2.50% está en desacuerdo de la misma manera totalmente en desacuerdo que existe prevención de las entidades bancarias con el fin de enjuiciar penalmente infracciones de fraude informático de cuentas financieras, datos que al ser cotejados con lo hallado por Hancco (2018) en su trabajo de investigación: *La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú - 2017*, dice la evolución de la TIC y su uso prácticamente en los espacios de la acción del ser humano ha traído como efecto que se genere una sumisión en la tecnología y a la vez se dé una coyuntura para la conveniencia por parte de los individuos que operan al margen de la ley y escudriñan el beneficio de estas coyunturas, ello puede

apreciarse en las desfalcos de cuentas por medio de Internet, la clonación de tarjetas, etc. (p. 23).

Con esos resultados se afirma que hay disposición de las personas jurídicas de denunciar penalmente delitos de fraude informático sistemáticos que sufren principalmente los bancos que en estos últimos años se han incrementado según informe de la Oficina de Racionalización y Estadística inscritas en Fiscalías Penales Comunes y Fiscalías Mixtas.

Conforme los efectos alcanzados, según la tabla 06 se evidencia el 67.50% de los jueces, fiscales y abogados de la provincia del Santa – Chimbote se mostraron de acuerdo, el 25.00% está totalmente de acuerdo, el 5.00% no opina y el 2.50% está en desacuerdo que se produce una ficción a la propiedad del perjudicado con la destrucción y hurto del software en la red, fundamentos que al ser cotejados con lo hallado por Romero (2017)) en su investigación titulada: *Delitos informáticos cometidos a través de redes sociales y su tratamiento en el ministerio público en la ciudad de Huánuco, 2016*, indica que debido a la gran sumisión del ciberespacio de la informática y las telecomunicaciones para prácticamente las acciones y servicios, es extremado difícil ignorar el gradual fenómeno de los delitos cibernéticos y el progresivo número de intimidaciones a la vida ciudadana, las acciones ciudadanas y los sistemas gubernamentales. (p. 14).

Con esos resultados se afirma que la afectación al patrimonio del perjudicado con el sabotaje y hurto de la información del software en la red, se concede a los ciberdelincuentes las llaves a las puertas de un grandioso espacio productivo de permisibles afectados de ofensivas contra el patrimonio para que realicen sus acciones ilícitas, sin tener las sanciones necesarias para la regulación y aplicación eficaz de la sanción penal adecuada.

De los encuestados en la tabla 08 se demuestra que el 67.50% de los jueces, fiscales y abogados litigantes de la provincia del Santa – Chimbote se mostraron de acuerdo, el 25.00% está totalmente con el acuerdo, el 5.00% está con el desacuerdo y el 2.50% no da una opinión que hay el compromiso de cambio normativo para advertir y penar las infracciones informáticas hacia el patrimonio, las respuestas al contrastarlo con lo relacionado por Zorrilla

(2018) en su estudio titulado: *Inconsistencias y ambigüedades en la ley de delitos informáticos ley Nº 30096 y su modificatoria ley Nº 30171, que imposibilitan su eficaz cumplimiento*, dice prescindir que el congreso reincida en los equívocos, incertidumbres, al consignar una medida, no compliquemos delitos o infracciones informáticas, en lo que el bien legal preferido es la información presentada por recursos informáticos, con infracciones utilizando como canal la tecnología. (p.99).

Con esos resultados se afirma que hay el compromiso de renovación legal para advertir y penar las infracciones informáticas que en estos tiempos con el adelanto de la tecnología es necesario, la legislación actual no castiga las acciones ilícitas efectuadas por los ciberdelincuentes.

En esta ocasión en la tabla 10 se indica que el 60.00% de los fiscales, jueces, y abogados litigantes de la provincia del Santa – Chimbote se expresaron que están totalmente de acuerdo, el 40.00% se mostraron de acuerdo que se debe existir modificatoria del artículo 8, referente a Fraude informático de la Ley 30096. La modificatoria del artículo 8 plasma la particularidad de infracciones informáticas hacia el patrimonio, información que al ser confrontados con lo descubierto por García (2017) en su estudio investigativo: *Los delitos de estafas y sus consecuencias a través de las redes sociales*, señala que es primordial que conste como una infracción autónoma porque las sanciones determinadas entre confiscación fraudulenta por recursos electrónicos y la estafa posponen en cantidad, y sobre el comportamiento penal notable entre una y otra discrepa, concurriendo una transparente exageración ante una infracción que debe ser calificado del modo incuestionable como estafa. (p.15)

Con esos resultados se afirma que fraude informático contra el patrimonio debe ser modificado abarcado otros tipos de delitos como estafa, sabotaje y hurto contra el patrimonio porque se interpreta intrínsecamente de la modalidad de fraude a todo los posibles indebidos, pues esta forma jurídica no tiene eficacia no permite el castigo efectivo.

De acuerdo a lo que indica la tabla 11 se evidencia que el 60% de las personas especialistas de la provincia del Santa – Chimbote se mostraron en totalmente de acuerdo, 30% en acuerdo y 10% no opina que el rápido progreso de las

tecnologías informáticas ha acrecentado los delitos informáticos. Fundamentos que al ser confrontados con lo encontrado por Hancco (2018) en su trabajo investigativo: *La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú - 2017*, dice que la utilización de computadores y aplicaciones informáticos acceden a la recolección, ordenación, procesamiento y aplicación de la información para diferentes empleos que nos ha concedido un vertiginoso progreso tecnológico, en cambio, estos equipos, sistemas y programas nos ha vuelto más unido de la tecnología, este sometimiento no solo involucra una sumisión de los productores de dispositivos y aplicativos virtuales, sino de aquellos individuos que con un definitivo discernimiento están utilizando el Internet para ingresar a empresas, centros de trabajo, hogares y en toda parte, donde los criminales pueda conseguir alguna clase de utilidad. (p.21).

Con esos resultados se afirma que el acelerado avance de las TIC en estos tiempos, a la vez, suponen la puerta de entrada a la violación de nuestros derechos personales, está claro que el ingreso ilícito a los sistemas informáticos, sin la oportuna autorización, causa una invasión al secreto de las personas naturales y jurídicas, por lo que el acceso ilegal a ellos constituye un delito penal.

De los encuestados en la tabla 16 se demuestra que el 70% de las personas especialistas de la provincia del Santa – Chimbote se mostraron en totalmente con el acuerdo, el 10.00% está totalmente con el acuerdo, está con el desacuerdo el 10.00% y el 10.00% no opina que el tratamiento penal del fraude informático crea incertidumbre en su interpretación que no permite una sanción efectiva, datos que al ser contrastados con lo hallado por Pardo (2018) en su estudio titulado: *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima*, dice que el artículo 8 de la Ley especial de infracciones informáticas plasma un solo modo de infracciones informáticas hacia el patrimonio, siendo titulado con el Nomen Iuris de fraude informático, esta norma general que no admite reconocer y concretar completamente los comportamientos en la forma penal, esto es, la subsunción del comportamiento con la tipificación penal. (p. 74).

Con esos resultados se asevera que el fraude informático contra el patrimonio crea incertidumbre porque es ilimitado debe abarcar otras modalidades de tipificación como sabotaje, estafa y hurto que se da contra el patrimonio de las personas naturales y jurídicas, la norma no permite el castigo efectivo de los quehaceres indebidos.

Como se puede evidenciar en la tabla 20 detalla que el 60.00% de las personas especialistas de la provincia del Santa – Chimbote se mostraron está totalmente de acuerdo, y el 40.00% se expresaron de acuerdo que se debe realizarse la modificatoria del artículo 8, referente a Fraude informático de la Ley 30096. La modificatoria del artículo 8 plasma la peculiaridad de infracciones informáticas hacia el patrimonio, información que al ser confrontados con lo hallado por García (2017) en su estudio investigativo: *Los delitos de estafas y sus consecuencias a través de las redes sociales*, señala es de mucha trascendencia que esta coexista como una infracción autónoma ya que las condenas determinadas en medio de confiscación engañosa por recursos virtuales y la estafa se diferencian en cantidad, y ante todo, el comportamiento penal considerable entre una y otra se diferencian, constando una justa desproporción ante una infracción que debe ser estimado de modo categórico como estafa. (p.15)

Con esos resultados se afirma que fraude informático contra el patrimonio debe ser modificado abarcado otras como estafa, sabotaje y hurto informático contra el patrimonio, puesto que la actual legislación no reconoce el castigo efectivo de las infracciones o delitos realizados contra las personas naturales y jurídicas.

3.3. Aporte práctico

Proyecto de Ley N°…….

PROPUESTA LEGISLATIVA QUE MODIFICA EL ARTÍCULO 8 DE LA LEY 30096 DE DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

FORMULA LEGAL

LEY QUE PROPONE LA MODIFICATORIA DEL ARTÍCULO 8 DE LA LEY 30096 DE DELITOS INFORMÁTICOS.

Artículo 1. Objeto de la Ley

La presente ley tiene por finalidad la modificatoria del artículo 8 de la Ley 30096 de los Delitos Informáticos, que concierne al patrimonio, en los términos siguientes:

Artículo 8: Fraude informático

"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".

MODIFICACIÓN

Artículo 8: Fraude informática

El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el acceso indebido 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.

Artículo 8 – A: Estafa informática

El que hace empleo de medios informáticos para mentir a un tercero con el objetivo de que se deshaga de su patrimonio. La pena será privativa de libertad no menor de cinco ni mayor de diez años y con sesenta a ciento cuarenta días-multa.

Artículo 8 – B: Sabotaje informática

El que hace uso no autorizado de centros de cómputos o instalaciones informáticas donde alteran y destruyen el hardware y software de un sistema informático. La pena será privativa de libertad no menor de cuatro ni mayor de ocho años y con sesenta a ciento veinte días-multa.

Artículo 8 – C: Hurto informático

El que accede y se apropia de hardware y software de terceros, donde retira archivos informáticos, para almacenar su contenido en un soporte propio. La pena será privativa de libertad no menor de cuatro ni mayor de ocho años y con sesenta a ciento veinte días-multa.

EXPOSICIÓN DE MOTIVOS

Antecedentes

En la actualidad, somos sensatos que las TIC son necesarias para la vida diaria, gracias a ellas, podemos acceder rápidamente a más información, nos permite almacenar miles de byte de información, mantenemos contacto en cada momento y reducir distancias con los medios de transporte y comunicación, pero también, nos encontramos con las amenazas de la cibercriminalidad y es necesario afrontarlo, en el Perú contamos con una ley para hacerlo frente.

El procedimiento jurídico penal de los delitos o infracciones informáticas hacia la propiedad es incompleto, toda vez, que inmerecidamente se entiende adentro de fraude informático a todos los modos de delitos o infracciones informáticas que afecta el patrimonio de las instituciones empresariales y las personas, por lo que vienen generando dilema en la interpretación de dicha ley que no reconoce la penalidad requerida de las infracciones informáticas hacia el patrimonio jurídico y personal.

Fundamentos

Desarrollaremos el análisis correspondiente al Art. 8 de la Ley 30096.

El vigente Art. 8 de nuestra legislación peruana es análogo con el Art. 8 del Convenio sobre cibercriminalidad - Budapest (2001), uno y otro artículo condenan la utilización ilícita de la manipulación del funcionamiento datos y sistemas informáticos.

El artículo 8 tipifica un sol modo de delitos o infracciones informáticas hacia la propiedad, que se inscribe el nomen iuris de fraude informático, la ordenación general no admite deslindar y distinguir absolutamente los comportamientos delictivos en la forma penal.

Pero dicho artículo hace referencia tal y conforme manifiesta en su contexto de los delitos informáticos en materia de estudio hacia el patrimonio.

El procedimiento penal de los delitos o infracciones informáticas hacia la propiedad es defectuoso, cada ocasión se entiende adentro de fraude informático a todos los modos de delitos o infracciones informáticas hacia el patrimonio, generando indecisión en la compresión de la ley que no reconoce el castigo real de las infracciones informáticas hacia el patrimonio de las personas tanto jurídicas como naturales.

Este artículo actualmente resulta un injusto penal contra el patrimonio porque no pena los diversos comportamientos delictivos, por la forma como está redactado, trae confusión al momento de interpretarla. Las actitudes impropias de diseñar, introducir, alterar, borrar y suprimir, no enlazan con la infracción de fraude, estos comportamientos son adecuados de la infracción de daño, que viene hacer una infracción de efecto porque no conviene plasmar con la figura penal para que se realice la infracción de fraude virtual, también, es conveniente, que dicha operación parta seguida de una consecuencia separada de la idéntica actitud el que fundamenta en ocasionar un menoscabo a un tercero, de otro manera, la infracción estaría en tentativo.

La finalidad que se pretende poder implementar políticas que ayuden a recoger notabilidad jurídica y académica, toda vez que trata de un tema de la actualidad que viven las todas personas naturales y jurídicas en el país, con relación de las infracciones informáticas hacia el patrimonio, que causa bastante daño.

Se evidencia que la actual Ley N° 30096, presenta desconocimientos en su fundamentación por lo que ocasiona desconcierto en los ejecutores de justicia y los perjudicados, causando bastante periodos que estas peligrosas infracciones no se revelen y no se pueda encontrar a los auténticos criminales.

CONCLUSIONES DE LA PROPUESTA

El procedimiento legislativo surge con la necesidad de salvaguardar el patrimonio de la empresas y las personas, pero penosamente personas malas acceden al mal

uso de las TIC con el fin de causar daño patrimonial, por eso, se determina a través del artículo 8 de la Ley 30096, la actual norma jurídica de las infracciones informáticas hacia la propiedad es ambigua, obligado a que al presentarse de infracciones en el modo de estafa, sabotaje o hurto, la norma no admite la penalidad real de los sucesos ilícitos porque se ha comprendido dentro del modo de fraude todas estas infracciones no teniendo la validez jurídica.

Actualmente se estima que cada vez más, las nuevas y sofisticadas tecnologías informáticas, sistemas de información y en específico las TICs ha ido evolucionado de una manera rápida, donde hay bastante especialistas en el tema, quienes manejan a la perfección diferentes softwares, así mismo realizan acciones indebidas.

ANÁLISIS COSTO BENEFICIO

La propuesta legislativa no creará costo para el estado peruano, porque solo busca la modificatoria del artículo 8 de Ley 30096 con el propósito de salvaguardar el patrimonio de las personas naturales y jurídicas. Se considera que existe una inseguridad normativa para el castigo de las infracciones informáticas, porque la actual ley existente no logra vislumbrar y no se adapta a los sucesos que deberían ser penalizados, es más, un sinfín de delitos o infracciones informáticas que no son descubiertas porque el alto perfeccionamiento de los procedimientos que se comete en la red mundial.

DISPOSICIÓN COMPLEMENTARIA FINAL ÚNICA

El poder ejecutivo adecuará el reglamento de la Ley 30096 según lo actuado en la efectiva ley, en un plazo no mayor de treinta (30) días naturales contados a partir de la vigencia de la presente ley.

Chiclayo, diciembre del 2021

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Las siguientes conclusiones son:

1. La consideración de la Ley N° 30096 referente al artículo 8, se determina que los efectos jurídicos de la modificación serían más eficientes y eficaces para proteger el patrimonio, porque actualmente dicho artículo crea inseguridad en la interpretación del tratamiento penal, donde no admite la penalidad firme de otras modalidades de infracciones informáticas hacia el patrimonio de las personas naturales y jurídicas.
2. El tipo legal de los delitos o infracciones informáticas hacia el patrimonio en su modo de fraude en el Perú es defectuoso, en comparación con otros países donde se incluye todos los modos de infracciones informáticas con respecto a la propiedad. Según Pardo (2018) señala que los delitos o infracciones informáticas hacia el patrimonio (en Perú) es defectuoso, debido a que, al relacionarse de infracciones informáticas en el modo de hurto, sabotaje o estafa, la ley no admite el castigo efectivo de las actividades ilegales, puesto que se ha incluido dentro del modo de fraude todos los posibles indebidos (p. 75).
3. La jurisprudencia penal de los delitos o infracciones informáticas hacia el patrimonio en su modo de estafa, sabotaje, y hurto, no explica la manera precisa y manifiesta la presunción al patrimonio por medio sistemas informáticos, el cual crea impunidad de los sucesos contra las personas jurídicas y naturales.
4. Con la propuesta del presente estudio de investigación, se busca modificar el Art. 8 de la actual Ley 30096, para tratar los delitos o infracciones informáticas en las diversas modalidades, para que permita la sanción efectiva de las acciones ilícitas contra el patrimonio de las personas naturales y jurídicas.

4.2. Recomendaciones

Se tiene las recomendaciones:

1. La sugerencia básica en que se centró el trabajo de investigación es la inmediata modificación del Art. 8 en la Ley N° 30096 contra el patrimonio,

hace falta un debate a conciencia y especializado para poder luego regularla.

2. En todas las instituciones educativas a nivel básico y superior se debe incluir en la asignatura de informática o en el plan de estudio o curricular un curso obligatorio de derecho informático, con hincapié en prever todo tipo de delitos o infracciones informáticas.
3. Este año se han instaurado Fiscalías Especializadas en delitos o infracciones informáticas, se debe contar con personal especializado y equipos tecnológicos modernos para que las investigaciones y sanciones de estos delitos sean eficientes, más cuando el desarrollo de la tecnología informática es mucho más rápido.
4. Debido a que los delitos informáticos son cada vez más perfeccionados y son cometidos desde cualquier parte del mundo, se debe instaurar una Corte internacional con capacidad de estas infracciones donde se pueda realizar la indagación y castigo de sucesos delictivos que se hallan y se ejecutan infracciones con el empleo de los procedimientos informáticos de otros países del mundo.

V. REFERENCIAS

Alarcón Ariza, Diego. A. y Barrera Barón, Javier. A. (2017). *Uso de Internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016*. (Tesis de Maestría, Universidad Privada Norbert Wiener). (Acceso el 26 de setiembre del 2020).

Besares, M. A. (2015). *Tópicos de Derecho Informático*. Texas: UNACH - Instituto de Investigaciones Jurídicas.

Espinoza Coila, Michael. (2017). *Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control*. (Tesis de grado, Universidad Nacional del Altiplano). (Acceso el 25 de setiembre del 2020).

Estrada Garavilla (S/f). Miguel. *Delitos informáticos.*
http://perso.unifr.ch/derechopenal/assets/files/articulos/a_20080526_32.pdf

Flores Vidal (2020). *Los ciberdelitos: la otra pandemia que avanzó en silencio en el Perú*, con fecha 14 de octubre del 2020
https://pagina3.pe/2020/10/14/los-ciberdelitos-la-otra-pandemia-que-avanzo-en-silencio-en-el-peru/

Fuentes, Tomás; Mazún, Rodrigo y Cancino, Gianny (2018). *Perspectiva sobre los delitos informáticos: Un punto de vista de estudiantes del Tecnológico Superior Progreso*. Revista Advance in Engineering and Innovation (AEI), Año 2, No.4, Yucatán, México.

García de la Cruz, J. M. (2009). *Delitos Informáticos.* España: El Cid Editores.

Hernández Sampieri, R. y otros (2018). *Metodología de la Investigación Científica*. 7° Ed. McGraw-Hill, México, D.F.

La República. *Ciberdelitos generarán costos de más de un billón de dólares para economía global,* con fecha el 07 de diciembre 2020.
https://larepublica.pe/economia/2020/12/07/ciberdelitos-generaran-costos-de-mas-de-un-billon-de-dolares-para-economia-global/

Morales Delgado, Deivid Yuly (2016). *La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el perú-2015*, (Tesis de título, Universidad Señor de Sipán). (Acceso el 27 setiembre del 2020).

OCDE - Organización para la Cooperación y el Desarrollo Económico (2015), *Recomendación del Consejo de la OCDE relativa a la Cooperación Internacional en el marco de investigaciones y procedimientos en materia de competencia*. Aprobada por el Consejo el 16 de septiembre de 2014, México.

Pardo Vargas, Alejo (2018). *Tratamiento Jurídico Penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018*, (Tesis de Maestro, Universidad César Vallejo). (Acceso el 01 de abril del 2021).

Piccirilli, Darío. A. (2015). *Protocolos a aplicar en la Forensia Informática en el marco de las nuevas tecnologías (Pericia – Forensia y Cibercrimen).* (Tesis Doctoral, Universidad Nacional de La Plata). (Acceso el 10 de octubre de 2020).

Rincón, L. M., Taborda, D. A., & Roldan, L. M. (2017). *Clonación de tarjetas de crédito*. Medellín: Tecnológico de Antioquia Institución Universitaria.

Rodríguez, F. (2013). *Derecho informático. El derecho en la era digital. La sociedad de información y el sistema jurídico. Contratos informáticos. Protección jurídica de los programas de computación. Delitos informáticos. La tutela jurídica del sistema informático.* UNC y FCEFyN.

Romero Ocampo, Meylin Del Pilar (2017). *Delitos informáticos cometidos a través de redes sociales y su tratamiento en el ministerio público en la ciudad de Huánuco, 2016*. Universidad de Huánuco Facultad de Derecho y Ciencias Políticas

Ruiz Cruz, Carolin Anabel (2016). *Análisis de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos*. (Tesis de Titulo, Universidad Nacional de Loja). (Acceso el 29 de setiembre de 2020).

Rumiche Pazo, José Alfonso (2015). *Sombras de la normatividad que regula el incremento de la ciberdelincuencia en Lima 2015.* (Tesis de título, Universidad Nacional José Faustino Sánchez Carrión de Huacho). (Acceso el 25 de setiembre del 2020).

Sánchez Blas, John. J. (2017). *Adopción de estrategias de Ciberseguridad en la protección de la información en la Oficina de Economía del Ejército, San Borja- 2017*. (Tesis de Maestría, Instituto Científico Tecnológico del Ejército). (Acceso el 26 de setiembre del 2020).

Sánchez Castillo, Zulay N. (2017). *Análisis de la Ley 1273 de 2009 y la evolución de la Ley con relación a los delitos Informáticos en Colombia.* (Tesis de especialista informático, Universidad Nacional Abierta y a Distancia —UNAD).

Tellez Valdez, Julio (2008). *Derecho informático.* 4° Ed. McGraw-Hill/ Interamericana Editores, S.A. DE C.V., México, D.F.

Tenorio Pereyra, Julio E. (2018). *Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia*. (Tesis de grado, Academia Diplomática del Perú "Javier Pérez de Cuéllar). Universidad Nacional del Altiplano el 25 de setiembre del 2020). (Acceso el 27 setiembre del 2020).

Torres, Daniel (2017). *La información y la comunicación del riesgo de origen tecnológico en la empresa Puerto Moa*. Revista Ciencia y Futuro, Año 5, No. 1.

Tundidor, L.; Dianelys, N. y Medina, A. (2018). *Organización de los sistemas informáticos para potenciar en control de la gestión empresarial*. Revista Cofín Habana, Año 13, No. 1, Universidad de Matanzas, Cuba, pp 88-110

Vilca Aira, Gabi L. (2018). *Los hackers: Delito informático frente al código penal peruano*. (Tesis de título, Universidad Nacional Santiago Antúnez de Mayolo de Huaraz) (Acceso el 28 de setiembre del 2020).

Villavicencio T., F. (2014). *Delitos informáticos*. IUS ET VERITAS, *N° 49.*

Zorrilla Tocto, Karina J (2018). *Inconsistencias y ambigüedades en la ley de delitos informáticos ley Nº 30096 y su modificatoria ley Nº 30171, que imposibilitan su eficaz cumplimiento".* (Tesis de título, Universidad Nacional Santiago Antúnez de Mayolo de Huaraz) (Acceso el 25 de setiembre del 2020).

Diccionario de la Real Academia Española

https://dle.rae.es/contenido/actualizaci%C3%B3n-2019 (visto 11 de octubre del 2020)

Cibercrimen tratamiento de los delitos informáticos, Lunes 11 de noviembre del 2019. https://angelderechoinformatico.blogspot.com/2019/11/

Recurso de casación de España

https://supremo.vlex.es/vid/708911241?_ga=2.122428811.1091237250.1618504592-2121396731.1618504592

Trujillo en Línea del 18 de octubre del 2022. *Conoce los casos de ciberdelincuencia más comunes en el Perú*
http://www.trujilloenlinea.pe/noticias/tecnologia/18/10/2022/conoce-los-casos-de-ciberdelincuencia-mas-comunes-en-el-per
El Peruano. Lima 09 de setiembre del 2022. *Denuncias por delitos informáticos se incrementaron en más del 90% en el Perú.*
https://www.elperuano.pe/noticia/188048-denuncias-por-delitos-informaticos-se-incrementaron-en-mas-del-90-en-el-peru#:~:text=Cada%20vez%20se%20registran%20m%C3%A1s,en%20comparaci%C3%B3n%20con%20el%202020.

VI. ANEXOS

6.1. Matriz de Consistencia

TÍTULO: EL TRATAMIENTO PENAL DE LOS DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO DE LAS PERSONAS NATURALES Y JURÍDICAS EN LA CORTE SUPERIOR DE JUSTICIA DEL SANTA - CHIMBOTE.

<table>
<tr><th>VARIABLES</th><th>PROBLEMA</th><th>HIPÓTESIS</th><th>OBJETIVOS</th></tr>
<tr><td>INDEPENDIENTE:

Artículo 8 de la ley 30096</td><td rowspan="2">¿La normativa penal actual sobre delitos informáticos, protege el patrimonio de las personas naturales y jurídicas en la Corte Superior de Justicia del Santa, Chimbote?</td><td rowspan="2">Si se modifica y aplica adecuadamente la normativa penal sobre delitos entonces se protegerá el patrimonio de las personas naturales y jurídicas.
.</td><td rowspan="2">GENERAL:

Determinar los efectos jurídicos de la modificatoria de la ley de delitos informáticos para proteger el patrimonio de las personas naturales y jurídicas en la Corte Superior de Justicia del Santa, Chimbote.

ESPECÍFICOS:

1. Conocer los fundamentos teóricos del tipo penal de los delitos informáticos en la doctrina nacional y comparada.
2. Analizar jurisprudencialmente los elementos del tipo penal de los delitos informáticos.
3. Plantear la modificación del Art. 8 de la Ley Nº 30096 con el fin proteger el patrimonio de las personas naturales y jurídicas.</td></tr>
<tr><td>DEPENDIENTE:

Tratamiento penal de delitos informáticos contra el patrimonio</td></tr>
</table>

6.2. Cuestionario

UNIVERSIDAD SEÑOR DE SIPÁN

CUESTIONARIO APLICADO A LOS JUECES, FISCALES Y ABOGADOS DE LA CORTE SUPERIOR DE JUSTICIA DEL SANTA - CHIMBOTE.

EL TRATAMIENTO PENAL DE LOS DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO DE LAS PERSONAS NATURALES Y JURÍDICAS

Estimado(a): Se le solicita su valiosa colaboración para que marque con un aspa el casillero que crea conveniente de acuerdo a su criterio y experiencia laboral, puesto que, mediante esta técnica de recolección de datos, se podrá obtener la información que posteriormente será analizado e incorporada al trabajo de investigación con el título descrito líneas arriba.

NOTA: para cada pregunta se considera la escala de 1 a 5 donde:

1	2	3	4	5
Totalmente en Desacuerdo	En Desacuerdo	No Opina	De Acuerdo	Totalmente de Acuerdo

ÍTEM	TD	D	NO	A	TA
1. ¿Considera usted que el acelerado avance de las tecnologías informáticas ha acrecentado los delitos informáticos?					
2. ¿Considera usted que hay eficacia de la legislación para penar las nuevas formas criminales con el uso de las tecnologías informáticas?					
3. ¿Considera usted que existe prevención de los bancos para denunciar penalmente delitos de fraude informático de cuentas bancarias y otros?					
4. ¿Considera usted que existe procedimientos claros para la prevención y sanción de delitos de fraude informático?					
5. ¿Considera usted que la seguridad de las plataformas informáticas para efectuar compras y contratar servicios a través de Internet actualmente no se encuentra tipificado en el código penal?					
6. ¿Considera que se produce una afectación al patrimonio del perjudicado con el sabotaje y hurto de la información del software en la red?					
7. ¿Considera usted que está vigente la norma de los delitos informáticos contra el patrimonio y su certeza en la prevención de delitos?					
8. ¿Considera usted que hay el compromiso de reforma legislativa para prevenir y penar los delitos informáticos contra el patrimonio?					
9. ¿Considera usted que hay norma concreta del delito de estafa y hurto informático, tipicidad y prevención?					
10. ¿Considera usted que se debe modificar el artículo 8 de la ley 30096?					

CUESTIONARIO APLICADO A LOS ESPECIALISTAS INFORMÁTICOS DE LA PROVINCIA DEL SANTA - CHIMBOTE.

EL TRATAMIENTO PENAL DE LOS DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO DE LAS PERSONAS NATURALES Y JURÍDICAS

Estimado(a): Se le solicita su valiosa colaboración para que marque con un aspa el casillero que crea conveniente de acuerdo a su criterio y experiencia laboral, puesto que, mediante esta técnica de recolección de datos, se podrá obtener la información que posteriormente será analizado e incorporada al trabajo de investigación con el título descrito líneas arriba.

NOTA: para cada pregunta se considera la escala de 1 a 5 donde:

1	2	3	4	5
Totalmente en Desacuerdo	En Desacuerdo	No Opina	De Acuerdo	Totalmente de Acuerdo

	TD	D	NO	A	TA
	1	2	3	4	5
1. ¿Considera usted que el acelerado avance de las tecnologías informáticas ha acrecentado los delitos informáticos?					
2. ¿Considera usted que hay eficacia de la legislación para penar las nuevas formas criminales con el uso de las tecnologías informáticas?					
3. ¿Considera usted que existe prevención de los bancos para denunciar penalmente delitos de fraude informático de cuentas bancarias y otros?					
4. ¿Considera usted que existe estrategias claras para la prevención y sanción de los delitos de fraude informático?					
5. ¿Considera usted que la confiabilidad de las plataformas informáticas para realizar compras y contratar servicios a través de Internet son castigados?					
6. ¿Considera usted que el tratamiento penal del fraude informático crea incertidumbre en su interpretación que no permite una sanción efectiva?					
7. ¿Considera usted que los fiscales que investigan delitos informáticos están realmente capacitados?					
8. ¿Considera usted que los diferentes operadores del derecho reciben frecuentemente capacitación, sobre el tratamiento penal de los delitos informáticos?					
9. ¿Considera usted que la ley de delitos informáticos no es eficaz para que no se logre muchas sentencias en Chimbote?					
10. ¿Considera usted que se debe modificar el artículo 8 referente a Fraude informático de la Ley 30096?					

6.3. Ficha de validación del cuestionario

UNIVERSIDAD SEÑOR DE SIPÁN

FICHA DE VALIDACIÓN DE INSTRUMENTO POR JUICIO DE EXPERTOS

1. NOMBRE DEL JUEZ		Melissa Fiorella Alarcón Olivos
2.	**PROFESIÓN**	Abogada
	ESPECIALIDAD	Penal
	GRADO ACADÉMICO	Magister en Derecho Penal
	EXPERIENCIA PROFESIONAL (AÑOS)	07
	CARGO	Asistente Registral en SUNARP
TÍTULO DE LA INVESTIGACIÓN: **EL TRATAMIENTO PENAL DE LOS DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO DE LAS PERSONAS NATURALES Y JURÍDICAS EN LA CORTE SUPERIOR DE JUSTICIA DEL SANTA - CHIMBOTE**		
3. DATOS DEL TESISTA		
3.1	NOMBRES Y APELLIDOS	FRANCISCO JAVIER DELGADO BENITES
3.2	ESCUELA PROFESIONAL	DERECHO
4. INSTRUMENTO EVALUADO		1. Entrevista ( ) 2. Cuestionario (X) 3. Lista de Cotejo ( ) 4. Diario de campo ( )
5. OBJETIVOS DEL INSTRUMENTO		GENERAL: Validar el cuestionario referido al tratamiento penal de los delitos informáticos de las personas naturales y jurídicas.
		ESPECÍFICOS: 4. Conocer los fundamentos teóricos del tipo penal de los delitos informáticos en la doctrina nacional y comparada. 5. Analizar jurisprudencialmente los elementos del tipo penal de los delitos informáticos.

	6. Proponer la modificatoria del artículo 8 de la Ley Nº 30096 para proteger el patrimonio de las personas naturales y jurídicas.

A continuación se le presentan los indicadores en forma de preguntas o propuestas para que usted los evalúe marcando con un aspa (x) en "A" si está de ACUERDO o en "D" si está en DESACUERDO, SI ESTÁ EN DESACUERDO POR FAVOR ESPECIFIQUE SUS SUGERENCIAS

N°	**6. DETALLE DE LOS ITEMS DEL INSTRUMENTO**	**ALTERNATIVAS**
01	Considera usted que el acelerado avance de las tecnologías informáticas ha acrecentado los delitos informáticos 1- En desacuerdo 2- Ni de acuerdo, ni en desacuerdo 3- De acuerdo 4- Totalmente de acuerdo	A (x) D ( ) SUGERENCIAS: …… ……..
02	Considera usted que hay eficacia de la legislación para sancionar las nuevas formas criminales con el uso de las tecnologías informáticas 1- En desacuerdo 2- Ni de acuerdo, ni en desacuerdo 3- De acuerdo 4- Totalmente de acuerdo	A (x) D ( ) SUGERENCIAS: …… ……..
03	Considera usted que existe prevención de los bancos para denunciar penalmente delitos de fraude informático de cuentas bancarias y otros. 1- En desacuerdo 2- Ni de acuerdo, ni en desacuerdo 3- De acuerdo 4- Totalmente de acuerdo.	A (x) D ( ) SUGERENCIAS: …… ……..
04	Considera usted que existe procedimientos claros para la prevención y sanción de delitos de fraude informático. 1. En desacuerdo 2. Ni de acuerdo, ni en desacuerdo	A (x) D ( ) SUGERENCIAS:

	3. De acuerdo 4. Totalmente de acuerdo	……..… ……..
05	Considera que la confiabilidad de las plataformas informáticas para realizar compras y contratar servicios a través de Internet actualmente no se encuentra tipificado en el código penal. 1. En desacuerdo 2. Ni de acuerdo, ni en desacuerdo 3. De acuerdo 4. Totalmente de acuerdo	A (x) D ( ) SUGERENCIAS: ……..… ……..
06	Considera que se produce una afectación al patrimonio de la víctima con la destrucción de la información y software en la red. 1- En desacuerdo 2- Ni de acuerdo, ni en desacuerdo 3- De acuerdo 4- Totalmente de acuerdo	A (x) D ( ) SUGERENCIAS: ……..… ……..
07	Considera usted que está vigente la regulación de los delitos informáticos contra el patrimonio y su efectividad en la prevención de delitos. 1- En desacuerdo 2- Ni de acuerdo, ni en desacuerdo 3- De acuerdo 4- Totalmente de acuerdo	A (x) D ( ) SUGERENCIAS: ……..… ……..
08	Considera que hay la necesidad de reforma legislativa para prevenir y sancionar los delitos informáticos contra el patrimonio. 1- En desacuerdo 2- Ni de acuerdo, ni en desacuerdo 3- De acuerdo 4- Totalmente de acuerdo	A (x) D ( ) SUGERENCIAS: ……..… ……..

09	Considera que hay regulación específica del delito de estafa y hurto informático, tipicidad y prevención. 1- En desacuerdo 2- Ni de acuerdo, ni en desacuerdo 3- De acuerdo 4- Totalmente de acuerdo	A (x) D ( ) SUGERENCIAS: …… ……..
10	Considera usted que se debe modificar el Artículo 8 de la Ley Nº 30096. 1- En desacuerdo 2- Ni de acuerdo, ni en desacuerdo 3- De acuerdo 4- Totalmente de acuerdo	A (x) D ( ) SUGERENCIAS: …… ……..

PROMEDIO OBTENIDO:	A (x) D ( )
7.COMENTARIOS GENERALES **Ninguna** ----------	
8. OBSERVACIONES: **Ninguna** ----------	

6.4. Carta de autorización para aplicar instrumentos

COLEGIO DE ABOGADOS DEL SANTA

"Año del Bicentenario del Perú: 200 años de la Independencia"

AUTORIZACIÓN DE RECOJO DE INFORMACIÓN

El que suscribe **Dr. CHRISTIAM ERNESTO ESTRADA VELARDE** Decano del Colegio de Abogados del Santa:

Por el presente. Autorizo para aplicar cuestionario y recojo de datos, al alumno: **DELGADO BENITES, FRANCISCO JAVIER**, identificado con **DNI Nº 19669351** y código de estudiante **Nº 2161802791**, estudiante de la Facultad de Derecho y Humanidades, y autor del trabajo de investigación denominado: **EL TRATAMIENTO PENAL DE LOS DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO DE LAS PERSONAS NATURALES Y JURÍDICAS EN LA CORTE SUPERIOR DE JUSTICIA DEL SANTA – CHIMBOTE**, al uso de dicha información que conforman el expediente técnico, para efectos exclusivamente académicos de la elaboración de la tesis de PRE GRADO, enunciada líneas arriba de quien solicita se garantice la absoluta confiabilidad de la información solicitada.

Atentamente.

Chimbote 23 de junio de 2021.

COLEGIO DE ABOGADOS DEL SANTA
Abog. Christiam Ernesto Estrada Velarde
DECANO

Jr. Elías Aguirre 151 - 153
Chimbote - Perú
Telf: (051) 043-324459
(051) 043-320927
E-mail: colegioabogadossanta@yahoo.es
facebook: Casantachimbote

6.5. Jurisprudencia

Jurisprudencia internacional

T R I B U N A L S U P R E M O
Sala de lo Penal
Sentencia núm. 159/2018
Fecha de sentencia: 05/04/2018
Tipo de procedimiento: RECURSO CASACION
Número del procedimiento: 1061/2017
Fallo/Acuerdo:
Fecha de Votación y Fallo: 14/03/2018
Ponente: Excmo. Sr. D. Andrés Martínez Arrieta
Procedencia: Audiencia Nacional. Sección Primera de la Sala de lo Penal.
Letrada de la Administración de Justicia: Ilma. Sra. Dña. Sonsoles de la Cuesta y de Quero
Transcrito por: AMV
Nota:
RECURSO CASACION núm.: 1061/2017
Ponente: Excmo. Sr. D. Andrés Martínez Arrieta
Letrada de la Administración de Justicia: Ilma. Sra. Dña. Sonsoles de la Cuesta y de Quero
TRIBUNAL SUPREMO
Sala de lo Penal
Sentencia núm. 159/2018
Excmos. Sres.
D. Andrés Martínez Arrieta
D. Miguel Colmenero Menéndez de Luarca
D. Juan Ramón Berdugo Gómez de la Torre
D. Alberto Jorge Barreiro
D. Andrés Palomo Del Arco
En Madrid, a 5 de abril de 2018.
Esta sala ha visto el recurso de casación por infracción de ley, quebrantamiento de forma e infracción de precepto constitucional, interpuesto por Dña. Raquel y Don Blas , ambos representados por el procurador D. Argimiro Vázquez Guillén y defendidos por la letrada Dña. Sylvia Córdoba Moreno, contra la sentencia dictada por la Audiencia Nacional Sección Primera de la Sala de lo Penal, de fecha 10 de marzo de 2017 , que les condenó por delito continuado de estafa y de un delito de participación activa en asociación ilícita, siendo también parte el Ministerio Fiscal; y como partes recurridas ACCUVEN BUSINESS & FINANCIAL SERVICES INC representada por la procurador Dña. Rebeca Fernández Osuna y defendida por el letrado D. José Luis Parra Gómez; D. Indalecio representado por la procuradora Dña. María Isabel Torres Ruíz y defendido por el letrado D. Manuel Santiago Chicote Martín: INVERSIONES FOREX CANARIAS. S.L. representada por la procuradora Dña. María Eugenia Pato Sanz y defendida por la letrada Dña. Alicia María Armas Navarro; D. Rafael representado por la procuradora Dña. María del Ángel Sanz Amaro y defendido por la letrada Dña. Almudena Solana López.
Ha sido ponente el Excmo. Sr. D. Andrés Martínez Arrieta.

ANTECEDENTES DE HECHO
PRIMERO
El Juzgado Central de Instrucción nº 2, instruyó Procedimiento Abreviado 301/2010 contra Raquel y Blas y otros por delitos de estafa, falsificación en documento mercantil, blanqueo de capitales y asociación ilícita, y una vez concluso lo remitió a la Audiencia Nacional, Sección Primera, que con fecha 10 de marzo de 2017 dictó sentencia que contiene los siguientes HECHOS PROBADOS: "El acusado Blas , con la colaboración de la también acusada Raquel , en compañía de otros sujetos a los que no afecta la presente resolución decidieron crear una estructura de carácter permanente con la que enriquecerse ilícitamente y ocultar las ganancias así obtenidas, mediante fa puesta en funcionamiento de un sistema defraudatorio capaz de afectar a un elevadísimo número de víctimas a lo largo de todo el mundo, al operar a través de internet. Dicha trama, que perduró desde los primeros meses del año 2007, hasta principios del año 2011 cuando se desarrolló la operación policial, y en la que cada uno de ellos asumió un papel diferente. Así, Blas , en cuanto promotor y máximo responsable de dicha estructura, se valió de la mercantil "Evolution Market Group, Inc", sociedad constituida en la República de Panamá mediante escritura pública del dia 8 de marzo de 2007, siendo "Finanzas Forex" la marca comercial utilizada para operar en el mercado de divisas, conocido a nivel mundial corno Mercado Forex, y de la que aquél era el único socio, con poderes de la entidad para operar a cualquier nivel, teniendo su sede en el edificio Torre Global Bank, calle 50. Bella Vista. Ciudad de Panamá. Mientras que, la acusada, Raquel, se encargaba de reinvertir las ganancias así obtenidas, ocultando su ilícita procedencia y la titularidad real de los activos, con la única finalidad de enriquecerse ilícitamente, aprovechando para ello sus contactos en su país de origen, Colombia.
Así, la citada mercantil de la que el acusado Blas, era el máximo responsable de su gestión, carecía de cualquier tipo de estructura sobietaria legal, más allá de la existencia de un departamento de contabilidad en Panamá y una persona encargada de los servicios informáticos Conrado que operaba desde Argentina, cuya

principal misión era dar soporte técnico a la página web de la empresa. "Finanzas Forex", contaba con tres vicepresidentes ficticios Bruno, Felicisimo , y Manuel , y un Departamento de Marketing dei que figuraba como responsable el acusado Severino , aunque no lo ejercía efectivamente, al igual que los demás cargos societarios, quienes sin embargo si llevaban a cabo labores de promoción de laempresa en los distintos países. Este acusado participó en diversas conferencias y reuniones promocionando la empresa, en concreto en la celebrada en Cartagena de Indias (Colombia) los días 28 y 29 de febrero de 2008, hasta que se produjo la advertencia de la CNMV (7 de abril de 2008) acerca de, que "EMG"/TFX" no estaba autorizada en España, para llevar a cabo labores de captación de inversores, cesando en su actividad, y permaneciendo en la empresa como mero inversor-promotor. Carecía de cualquier tipo de poderes, o autorizaciones para actuar como Director de Marketing, y no figuraba como tal en ningún registro público, ni consta haber tenido intervención alguna en fa constitución de ningún tipo de sociedad mercantil, ni en la apertura de cuentas bancarias.
De cara a los organismos públicos, figuraba como Presidenta y Representante Legal de "ErvIG"/"FFX" Doña Rosana, miembro de un despacho de abogados de Panamá, habiendo otorgado amplio apoderamiento a Blas, para llevar a cabo todo tipo de intervención, en especial, los relacionados con la apertura de cuentas en las diversas entidades bancarias y de negocio.
Desde la fecha de su constitución, hasta el mes mayo de 2009, centró su actividad en el citado mercado de divisas "Forex", captando a clientes e inversores bajo la promesa de altísimos réditos, a quienes se abonaban unos supuestos rendimientos con las aportaciones de los nuevos inversores, sin que en realidad existiera ninguna actividad comercial o financiepá que produjera rentabilidad alguna, desviando además; la inversión.a otros mercado, como el inmobiliario, el mercado del oro, los "commodities", todo ello en contra lo prevenido en las cláusulas contractuales que aquellos se veían obligados a firmar.

SEGUNDO.- A los posibles inversores, se les informaba falsamente que con el dinero depositado se operaría el mercado de divisas (Forex), y de esta forma se obtendrían los supuestos rendimientos que, en cada momento podrían consultarse en la website de la empresa www.finanzasforex.com., página que resultaba fundamental .a fin de llevar a cabo la estrategia de expansión del engaño, y que tras la iniciación de los procesos en los EE.UU., pasó a ser sustituida por la red "PF Place", en cuya página web se publicitaban otras empresas también constituidas por Blas , con sus respectivas páginas web, como PF Place.com ; Merbabid.com ; Forcebusiness,com; Comer FX.com ; algunos de cuyos dominios se encontraban registrados en la empresa española "Merkaweb Servicios de Internet". El propio contrato de inversión entre "EMG"P'FFX" y los inversores, decía expresamente que la empresa depositaba los fondos de los inversores en las casas broker mediante las cuales operaba en el mercado Forex. Estos, una vez captados, transferían sus aportaciones directamente a "EMG"/"FFX", a través primero de unas cuentas bancarias abiertas en la entidad Multicaja de "Zaragoza" a nombre de Blas y de un broker denominado "lnterbank", y después a través de otro broker suizo "Dukascopy Bank S,A." y de las cuentas que la entidad "Crowne Gold Inc" tenía abiertas en el "Wells Fargo Bank" de EE.UU., creada específicamente para ello en dicho pais, o en otros países, principalmente Panamá, tales como "HSBC Bank USA", "Wells Fargo Bank", "BB&T Bank", 'Washington Mutual Bank" o "Wachovia Bank". Desde estas cuentas, supuestamente se realizaban las inversiones en el mercado de divisas (Forex), a través del broker suizo "Dukascopy Bank S.A.". Por su parte "Crowne. Gold, Inc", entidad con presencia online, actuaba corno un banco intermediario qué aceptaba fondos de inversores en nombre de los clientes de "EMG"/"FFX"; sin embargo, en lugar de invertir el dinero de estos en el mercado Forex, la mayor parte de Jos fondos se desviaban aotro tipo de inversiones, fundamentalmente inversiones inmobiliarias en Panamá, que en definitiva iban a engrosar el patrimonio personal de los acusados Blas y Raquel.
Posteriormente, tras concluir "EMG"/"FFX" sus relaciones comerciales con "Dukascopy Bank" y con "Crown,v Gold Inc" respectivamente, los sitios web de aquella indicaron a los inversores que debían enviar su dinero a otras cuentas, a nombre de otras entidades, incluyendo en ellas a "DWB Holding Company" (DWB, establecida en Oliendo. Florida), "Superior International Investment Corporation" (SlIC, establecida también en Orlando) y "Obbalube Investment Corporation" (010, de Miami), las cuales figuraban a nombre de un tal Emilio , con el que el acusado Blas habría suscrito con anterioridad determinados contratos, y que actuaban de manera muy parecida a "Crowne Gold, 'no", es decir, como bancos intermediarios al aceptar fondos por cuenta de inversores de "EMG"/"FFX", y que ofertaban corno uno de los productos estrella, la inversión en "commodities", con muy altas y rápidas rentabilidades garantizadas de hasta el 100%. No existen contratos que justifiquen estas inversiones, ni la relación comercial de la mercantil "EMG"/"FFX" con el Sr. Emilio o sus empresas, tratándose de meras inversiones llevadas a cabo por el acusado Sr. Blas, siendo a posteriori, cuando informa a los clientes de que esas inversiones eran suyas, lo que forma parte, una vez más del engaño, ya que las mismas en ningún caso se destinaban al mercado de divisas "Forex".
Salvo una pequeña cantidad, que fue destinada al mercado Forex, el resto de los capitales transferidos por los inversores fueron a parar a los propios gastos de funcionamiento de "EMG"f'FFX", a la preparación de convenciones internacionales destinadas a captar nuevos clientes o, en su mayor parte, a adquisiciones patrimoniales realizadas por el acusado Blas y Raquel, en su propio beneficio.
Por este motivo, los inversores cuando intentaron recuperar los fondos y las ganancias acumuladas, que según los estados financieros a los que accedían a través de Internet, se iban produciendo, no percibieron cantidad alguna, siendo invitados a cobrar las cantidades que les correspondían mediante la incorporación de nuevas personas a las que traspasarían sus saldos acreedores, o través de unas tarjetas prepago que debían adquirirse a la mercantil registrada en Nueva Zelanda, "Pacific Mutual Saving & Loan Limitad", previo pago de 150 dólares USA cada una de ellas.

TERCERO.- Como parte de la puesta en escena para dotar de credibilidad a la estructura defraudatoria, Blas llegó a establecer una relación comercial con el broker suizo "Dukascopy Bank S.A." en julio de 2007, si bien la misma finalizó en mayo de 2008 cuando "Dukascopy" cerró todas las cuentas de Blas y sus representados, por acuerdo de su Consejo de Dirección, tras recibir informes de los encargados de prevención del blanqueo de capitales de la citada entidad. Durante el período de vigencia de dicha relación comercial, Blas abrió catorce cuentas personales conjuntas en "Dukascopy" y una a nombre de "Evolution Iviarket Group", teniendo en todas ellas poderes para su gestión.
Sólo en las cuentas de "Crowne Gold inc", se recibieron más de 189.000.000 dólares USA de inversores de "EMG"/"FFX", pero sólo se enviaron a "Dukascopy" y a otras sociedades de inversión unos 9.110.000 dólares, es decir, menos del 5% del dinero transferido por los inversores a través de "Crowne Goid, Inc". Además, las operaciones llevadas a cabo en el mercado de divisas no devengaron ganancia alguna, por lo que nunca hubo altas rentabilidades (tal y como se anunciaban) o de otro tipo, para poder repartir entre los clientes, ya que nunca se distribuyó de manera efectiva el beneficio obtenido por aquellos, o lo fue, en cantidades ridículas.
En definitiva, las supuestas ganancias de los inversores se sufragaban con las cantidades aportadas por los nuevos clientes, de forma que mientras la base de inversores de "Finanzas Forex" siguiera aumentando, los acusados disponían de fondos para mantener y acrecentar la ficción del negocio, y por ende la trama concebida.

CUARTO.- La necesidad de ampliar permanentemente la base de los inversores, determinaba a los acusados a desarrollar una agresiva y engañosa publicidad, tanto a través de Internet, como en convenciones y reuniones presenciales, en los que se ofrecían al público la posibilidad de obtener rendimientos de hasta el 20% mensual en el Plan de inversión más conservador, y que podrían llegar hasta el 40% en el llamado Plan variable, todo ello en el mercado de divisas "Forex".
Además, se propiciaba que los inversores se convirtieran a su vez en promotores, ofreciéndoles lo que denominaban 'Plan de Carrera", para lo que debían captar a su vez a otros inversionistas, que a su vez obtendrían nuevos clientes, sirviéndose para ello de su propio círculo familiar o social, hasta alcanzar así, el séptimo nivel. En tales supuestos, con independencia de la retribución de su propia inversión, al inversor convertido en promotor, se le ofrecía un 0,50% de comisión de las cantidades invertidas por los clientes así captados. Dependiendo de los niveles y del número de promotores que habían conseguido, se les asignaba una categoria diferente, como Ejecutivo, Líder de Organización, Director Internacional, ofreciendo en los niveles más altos premios como viajes, cruceros, coches de lujo o bonos para la adquisición de viviendas. La CNMV advirtió al público, en fecha 7 de abril de 2008, que "EMG"rFFX" no estaba autorizada en España, para llevar a cabo labores de captación de inversores.

QUINTO.- Aunque las cantidades aportadas por los inversores, no se destinaban al mercado Forex y por tanto no generaban rendimiento alguno, el acusado Blas , con la finalidad de mantener el engaño al que hablan sido sometidos los clientes en 'Finanzas Forex', a través de la página web y en formato electrónico, facilitó a aquellos extractos de movimientos ficticios y "certificados de inversión", con los que les hacían creer que hablan obtenido ganancias en poco tiempo, y que mantenían saldos positivos, si bien unas y otros eran irreales. Estos documentos electrónicos podían ser descargados de la web por los inversores, como justificantes que reflejaban una posición financiera que no se ajustaban a la realidad, ya que entre otras condtíctas ilícitas, se incluían en los estados financieros activos que no les correspondían, y que en realidad se encontraban a nombre de alguna de las Sociedades instrumentales que los acusados Blas , principalmente, y Raquel , hablan creado, ayudados por otros sujetos ajenos a la presente causa, y cuya única finalidad era la de ocultar el verdadero origen del dinero, y por ende, su destino final.
Gracias a dicha actividad promocional, el número de clientes captados por la compañia aumentó de forma exponencial, de forma tal que, en fecha del 5 de Marzo de 2008 (a un año escaso de su puesta en marcha) el número de los mismos ascendía a 18.720, y el importe gestionado a 121.154.519 dólares USA, produciéndose un crecimiento diario de 600 clientes y 2 millones de dólares de inversión. El progresivo aumento de la base de la pirámide, hizo que en marzo de 2011, una vez ya cerrada la actividad comercial de "Finanzas Forex", el número de afectados por el fraude ascendiera a más de 186.000 personas, distribuidas por todo el mundo, con un saldo de inversión total en marzo de 2011, de 390.698.233,77 dólares USA.

SEXTO.- Blas, además de las cuentas de "Crawne Gold, Inc", utilizó también sus propias cuentas personales, y las de su entorno, para recibir o canalizar fondos provenientes de inversores de "EMG"/"FFX". Ya en el año 2009 y debido a la liquidación de las relaciones con "Crowne Gold Inc", le ordenarte pasó a ser la entidad "Ava Financial Ltd" con sede en las Islas Vírgenes Británicas, emitiendo un total de doce transferencias por valor de 1.222.107'99 euros.
Así, durante el año 2007, el acusado Blas habría recibido en una cuenta cotitulada por éste y la también acusada Eloisa , en la Caja Rural Aragonesa y de los Pirineos (Multicaja), un total de 129 ingresos por un montante global de 115.402'93 euros abonados por personas físicas, y muchos de ellos bajo el concepto de "Depósito Forex". También emplearon una cuenta abierta a nombre de la mercantil "Planetcom Systems & Trade Sl"; `asimismo, en fecha 9 de julio de 2009 la cuenta de "Pianetcom Systems & Trade, S.L.", registró el ingreso de un' cheque nominativo a favor de "Coloraba Assests Inc", emitido desde el banco panameño "Banvivienda" en concepto de "cancelación de cuenta de cliente de banca privada" por importe de 18.377,77 euros, pagadero en Panamá, y endosado a favor de "Planetcom Systems & Trade S.L." El endosante del cheque era Blas, en virtud de los poderes generales que, a su favor le había conferido, el 26 de febrero de

2008, la sociedad "Calambo Assets lnc". Parte de los fondos recibidos en esta cuenta, serían utilizados en la adquisición por parte de "Planetcom Systems & Trade S.L." de una serie de propiedades inmobiliarias.
Esta mercantil fue constituida por los acusados Blas y Eloisa , en fecha 20 de agosto de 2004, y tenía como objeto social la comercialización de productos de telefonía móvil, ampliando su objeto en agosto de 2006 a la compraventa de inmuebles. Al principio se dedicaron a la telefonia, luego eran comisionistas de empresas inmobiliarias como "Ivietrovacesa" y otras inmobiliarias, vendían sus productos. En escritura pública de fecha 26 de abril de 2006 (protocolo n° 957 del Notario de Valencia D. Santiago Mompó Gimeno) cesa en el cargo de administrador único Blas y se nombra para el mismo a Eloisa , y posteriormente, en escritura pública de 26 de diciembre de 2006 (protocolo n° 2527 del Notario de Zaragoza D. Juan Pardo Defez) se produce el cese de aquella como administradora única y se nombra para el mismo a Blas . Eloisa vendió a la mercantil "News Edition, S.L.", representada para ese acto por Blas dos mil doscientas cincuenta y dos participaciones sociales de la entidad "Planetoom Systems & Trade, S.L." (números 1 a 2252) de un valor nominal de un euro cada una (escritura de compraventa de participaciones sociales de fecha 22 de octubre de 2009 (protocolo n° 2099 del Notario de Zaragoza D. Juan Pardo Defez).

SÉPTIMO.- Coincidiendo con la advertencia de la Comisión Nacional del Mercado de Valores española ya reseñada, y otras similares como L' Autorite des Marches Financiers de Francia, de la Oficina de Decisión y Revisión de Valores de la provincia de Québec (Canadá), la Comisión Nacional de Valores de Panamá, o la Superintendecia Finariciera de Colombia, "Crovvne Gold, Inc" decidió cerrar las cuentas de "EMG"PF.›`," a partir-del 31 de julio de 2008, llegando a un acuerdo con esta entidad, según el cual los depósitos de "EMG" en "Crowne Goid, Inc" se convertirían en oro. Dichos depósitos de oro, así como las cuentas, vehículos y otros activos, han sido objeto de embargo por las autoridades de los Estados Unidos de América, a efectos de su decomiso.

OCTAVO.- Una vez obtenidos los fondos de los clientes, mediante las conductas antes descritas, el acusado Blas puso en marcha una actividad destinada a su reinversión en diferentes modalidades y bajo un complejo entramado de "sociedades pantalla" creadas, cotituladas, gerenciadas o participadas de alguna manera por aquél, y de las que se sirvió para sus ilícitos fines, tales como "Planetcom Systern & Trade S.L.", "Zentrurn Biz, Inc", "Contocommerce Corp", "Grand Palm Investment Corp", "Pacific Mutual Saving & Loan Limited", "News Edition, S.L.", "Colombo Assets, Inc", "Pacific Mutual Group, Inc", "Oceanía, S.A.", "International Trading lnvestment, S,A.", 'Astana Enterprises Corp", "Logikim, S.L.", "Pacific Atlantic Investment, Inc", "Regency Suites LLC", "Limited Liability Company", "Ibertrom Trade Corporation S.A.", "Partania Comerce Inc", "Bentley Finance Co, Inc", "Gates Trading Ltd. Corp", "Collin Trading inc", "Mann -trading !no", "Novasis International LLC", "ColomIDo Assets, S.A", "Force Business, S.L.", "Cerner FX Financial Ltd", "Varsovia Finance Ltd", "Grandex Corp", "Forexone AG Corp", "Danex Capital, Inc", "Epic Capital, Inc", "Fondos de Garantías, S,A.", entre las más destacadas, destinadas todas ellas a gestionar y a ocultar el verdadero origen de los bienes y fondos así obtenidos, para dificultar en definitiva su recuperación. A tal fin el acusado Blas ya a título individual, ya junto con su pareja sentimental la también acusada Raquel, y través del mencionado entramado societario, llevó a cabo numerosas operaciones inmobiliarias. Entre otras, el 11 de julio de 2007, Blas adquirió de la mercantil "Proyectos, Inversión y Desarrollo, S,A." el 100% de una vivienda situada en la localidad de Cuarte de Huerva (Zaragoza), así como la plaza de aparcamiento y trastero anejos, por un importe glObai de 203.000 euros más IVA (217.210 euros), subrogándose frente a la "Caja Laboral PoPdlar" en un crédito hipotecari9 por valor de 215.000 euros. En noviembre de 2007, Blas , en nombre y representación de la mercantil panameña "Zentrum Biz Inc", adquirió a la mercantil "FBEX Promo Inmobiliaria, S.L" una serie de inmuebles, por los que realizó pagos en efectivo por importe de 141.212'45 euros, además de un cheque por importe de 20.766 euros, También en noviembre de 2007, Blas , en nombre y representación de la mercantil panameña "Evolution Market Group Inc", compró a "FBEX Promo Inmobiliarias, S.L." inmuebles por los que realizó pagos en efectivo por importe de 310.893 euros, En septiembre de 2008, Blas , en nombre y representación de la mercantil "Contocomrnerce Corp", compró a "FBEX "Promo Inmobiliaria, S.L." inmuebles por los que realizó pagos en efectivo por importe de 300.000 euros. El 8 de octubre de 2008, Blas, en nombre y representación de la mercantil "Planetcom Systems & Trade, S.L." adquirió a "Construcciones Sarvise, S,A." el 100% de una vivienda sita en Cuarte de Huerva (Zaragoza), junto a su garaje y trastero, por un importe global considerado de 135,248 euros más IVA (144.715'36 euros).
El 24 de octubre de 2008, Blas, en nombre y representación de la mercantil panameña "Contocommerce Corp", de la que Raquel figuraba como apoderada, adquirió a "Viviendas Jardín S.A." el 100% de un total de nueve inmuebles, tres viviendas con sus respectivos garajes y trasteros, en AVENIDA000 número NUM000 , de Valencia, por un importe global de 931.517,41 euros más IVA (996.723'63 euros). El precio fue satisfecho mediante dos transferencias internacionales realizadas por el colombiano Luis Pedro (el 10 de septiembre de 2008, 35.434'37 euros) y por la mercantil estadounidense "Superior International Investment Corporation" (el 23 de octubre de 2008, 965.221'74 euros). En concreto ésta última, fue efectuada desde una cuenta del "Old Southern Bank" en Florida (EE.UU.), receptora directa de transferencias electrónicas de inversores de "EMG", por un montante global de 17.698.33325 dólares USA. El 28 de octubre de 2008, Blas, en nombre y representación de la mercantil "Planetcom Systems & Trade, S.L." adquirió a "Promociones F20, S,A," dos viviendas, con sus dos garajes anejos, situadas en la localidad de Pinseque (Zaragoza), por un importe global de 383.205,30 euros más IVA (410.029'68 euros), subrogándose frente a la "Caja Inmaculada de Aragón" en un préstamo hipotecario de 191.600 euros.

También en octubre de 2008, Blas, en nombre y representación de la mercantil panameña "Zentrum Biz lnc", adquiere a "FBEX Prorro Inmobiliaria, S.L." inmuebles por los que realiza dos pagos, mediante transferencia, por importe de 1.011.522'08 euros (506.271'63 euros y 505.250'45 euros). Las cantidades satisfechas a "FBEX Promo Inmobiliaria, S.L.", se refieren a inmuebles sitos principalmente en Valencia y Villarreal (Castellón), y las cantidades abonadas, que alcanzan los 1.843.687'22 euros, lo fueron en concepto de reserva, siendo el valor total de los inmuebles señalados de 24.000.000 euros.
Este acusado, efectuó asimismo adquisiciones inmobiliarias, con la también coacusada Eloisa . Así, el 26 de julio de 2007, adquirieron proindiviso de "Proyectos Inversión y Desarrollo" una vivienda sita en la CALLE000 con DIRECCION000 , manzana NUM001 , zona NUM002 de la localidad de Cuarte de Huerva (Zaragoza), por un importe global de 301.740 euros incluido el IVA, constituyendo un préstamo hipotecario en garantía de la misma por importe de 315. 650 euros, en favor de la entidad Caja Laboral". El 27 de junio de 2008, ambos, proindiviso, adquirieron de la mercantil "Metrovacesa S.A." una vivienda junto con su trastero y garaje, sita en la manzana NUM003 de la localidad de Playa de Almenara (Castellón) por un importe global de 130.300 euros, para cuya financiación suscribieron un préstamo hipotecario (escritura pública de 26 de junio de 2008) con la entidad bancaria "Multicaja" (anteriormente "Caja Rural Aragonesa y de los Pirineos Sociedad Cooperativa de Crédito") por importe de 85.000 euros.
Asimismo, aparecen en Panamá, titularidades inmobiliarias= a nombre de las mercantiles relacionadas con la estructura defraudatoria investigada, como las siguientes:
- "Zentrum Biz Inc.", en la cual tiene otorgado un poder especial Blas , que es propietaria de un apartamento en el EDIFICIO000 , Corregimiento de Bella Vista, Ciudad de Panamá escriturado el 16 de octubre de 2007.
- Igualmente, la sociedad panameña "Grand Palm Investment Corp.", en la cual tiene otorgado un poder especial la también acusada Raquel, es titular de un apartamento en el EDIFICIO000 , Corregimiento de Bella Vista, Ciudad de Panamá cuya propiedad también fue escriturada el 16 de octubre de 2007.
- Con fecha de 2 de abril de 20Ó8 Raquel adquirió én su propio nombre un Apartamento de 113,34 metros en DIRECCION001 NUM004 - NUM005 - NUM006 en la Zona Centro de Bogotá D.C. (Colombia). Raquel, pareja sentimental de Blas desde finales del año 2007, llevó a cabo diversas operaciones financieras e inmobiliarias, aprovechando sus distintos apoderamientos en las entidades reseñadas, con pleno conocimiento de que los fondos procedian de la ilícita actividad desarrollada por éste en la mercantil "EMG"/TFX". Tenía poderes de las mercantiles panameñas "Contocommerce Corp" y "Colombo Assests Inc", pertenecientes a "EMG", que se utilizaron para la compra de inmuebles en Colombia, donde se adquirieron hasta un total de treinta y un inmuebles por un valor aproximado de entre dos y cuatro millones de dólares. Tenía además una cuenta a su nombre en el broker "Lada' Securitys", y otras cuentas en "Crovvne Godl, Inc" también a su nombre, además de poderes en "Etv1G". Se desconoce dónde fueron a parar el dinero de la venta de los inmuebles, pero al igual que sucede con el resto de los fondos, en ningún caso a los inversores.
La totalidad de las inversiones inmobiliarias llevadas a cabo por el acusado Blas, formaban parte del entramado defraudatorio, ya que .aquél no invertía en nombre de la mercantil "EMGIFFX", ni de los clientes, sino de las sociedades opacas de su propiedad, creadas con tal finalidad, como así hizo, entre otras, con la mercantil "Fondos de Garantías, S.A." administrada por un despacho de abogados de Panamá. En la citada actividad, y formando parte: del entramado delictivo, participaba activamente la acusada Raquel, llevando a cabo continuas operaciones inmobiliarias, a nombre de las sociedades por aquel creadas, y de las que ésta participaba directamente; por medio de su gestión o dirección, o a través de sucesivos apoderamientos, que le autorizaban a efectuar diversas operaciones financieras e inmobiliarias con pleno conocimiento de que los fondos procedían de la ilícita actividad. Conductas ilícitas en las que asimismo, tuvieron participación otros sujetos no acusados, que sin embargo, aparecen en la investigación llevada a cabo con una destacada participación dentro del entramado creado, y que por las razones que fueren, no han sido traídos a esta causa.
Tal modo de proceder, ha causado numerosos perjuicios tanto de un punto de vista cuantitativo, ya que constan en las actuaciones 174.860 inversionistas perjudicados por la citada trama, en todo el mundo, y un perjuicio global, cuantificado, de 390.698.234 dólares USA, algunos de los cuales ciertamente considerables, si se tienen en cuenta las cantidades invertidas, y cuya relación nominal, con indicación del saldo pendiente, se encuentra en el Anexo de la presente resolución. Perjuicios además continuados en el tiempo, pues hasta fechas anteriores a la celebración del presente enjuiciamiento, se ha estado intentando llegar a acuerdos con los mismos, a cambio de la renuncia a las acciones y civiles y penales en la misma, para así poder acudir a la justicia norteamericana donde supuestamente se encontrarían retenidos parte de los bienes de los inversores de "EMG"flFFX".

SEGUNDO
La Audiencia de instancia dictó el siguiente pronunciamiento: FALLO:
1) Debemos absolver y absolvemos, con todos los pronunciamientos favorables, a los acusados Severino , y Eloisa , del delito de asociación ilícita del que venían acusados por el Ministerio Fiscal y la acusación particular de Remedios , con declaración de oficio de las costas procesales causadas.
2) Debemos absolver y absolvernos, con todos los pronunciamientos favorables al acusado Severino, del delito de estafa agravado y continuado, del que venía siendo actiSadopot el. Ministerio Fiscal, y por las diversas acusaciones particulares, con declaración de oficio de las costas procesales:"catisadas.
3) Debemos absolver y absolvemos, con todos los pronunciamientos favorables a la acusada Eloisa de los delitos de estafa agravada continuada, y del delito de blanqueo de capitales de los que venía siendo acusada por el Ministerio Fiscal y por las acusaciones particulares de "Inverscres Forex Canarias, S.L.", D. Rafael,

"Asociación Drustvo Mednarodnih Vlagateljen", y Doña Remedios, con declaración de oficio de las costas procesales causadas.
4) Debemos absolver y absolvemos, con todos les pronunciamientos favorables a la acusada Raquel del delito de estafa agravada continuada, del que venía siendo acusada por las acusaciones particulares de Inversores Forex Canarias, S.L.". y D. Rafael , con declaración de oficio de las costas procesales causadas.
5) Debemos condenar y condenamos a Blas , como autor criminalmente responsable, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal de un delito continuado de estafa agravado por el valor de la defraudación, en concurso ideal con un delito continuado de falsificación en documento mercantil, a la pena global de ocho años de prisión, y multa de dieciséis meses a razón de 50 euros diarios, así como a las penas accesorias de inhabilitación especial para el ejercicio del derecho de sufragio pasivo durante el tiempo de la condena, y la de quince años inhabilitación especial para profesión, oficio, industria o comercio relacionados con la intermediación financiera o el comercio por internet: así como al pago de las costas procesales causadas, en su parte proporcional, incluidas las de las distintas acusaciones particulares.
6) Asimismo, debemos condenar y condenamos a Blas , como autor criminalmente responsable, sin la concurrencia de circunstancias modificativas de la responsabilidad, criminal de un delito de blanqueo de capitales, a la pena de tres años y tres meses de prisión y multa de 300.000.000 euros, con la accesoria de inhabilitación especial para el derecho de sufragio pasivo durante el tiempo de la condena, así como y al pago de las costas procesales causadas, en su par-te proporcional, incluidas las de las distintas acusaciones particulares.
7) Por último, debemos condenar y condenamos al acusado Blas , como autor criminalmente responsable, sin la concurrencia de circunstancias modificativas de fa responsabilidad criminal, de un delito de asociación ilícita, en calidad de director de la misma, a la pena de dos años de prisión, multa de doce meses a razón de 50 de euros diarios, e inhabilitación especial para el ejercicio del derecho de sufragio pasivo durante el tiempo de la condena, así como y al pago de las costas procesales causadas, en su parte proporcional, incluidas las de las distintas acusaciones particulares.
8) Debemos condenar y condenamos a la acusada Raquel , como autora criminalmente responsable, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, de un delito de blanqueo de capitales, a la pena de dos años de prisión, y multa de 900.000 euros con fa accesoria de inhabilitación especial para el derecho de sufragio pasivo durante el tiempo de la condena, así como y al pago de las costas procesales causadas, en su parte proporcional, incluidas las de las distintas acusaciones particulares.
9) Asimismo, debemos condenar y condenamos a la acusada Raquel , como autora criminalmente responsable, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, de un delito de participación activa en asociación ilícita, a la pena de un año de prisión, y multa de doce meses a razón de 30 diarios euros, e inhabilitación especial para el ejercicio del derecho de sufragio pasivo durante el tiempo de la condena, así como al pago de las costas procesales causadas, en su parte proporcional, incluidas las de las distintas acusaciones particulares.
Se acuerda el decomiso de la totalidad de los bienes muebles e inmuebles, fondos; activos, dinero y demás reseñados en el relato de hechos probados, incluidos los depósitos de oro intervenidos en los EE.UU de América.
Se decreta la disolución de la mercantil de nacionalidad panameña "Evolution Market Group Inc", como consecuencia accesoria de la comisión de un delito de asociación ilícita.
Se decreta la clausura de la página web empleada por la entidad "EMG"/"FFX" www.finanzasforex. com, así como de cualesquiera otra por aquellos empleadas para llevar a cabo la publicidad de los productos, la captación de los inversores, y la contratación de los mismos.
En concepto de responsabilidad civil,el acusado Blas , deberá indemnizar a los perjudicados que figuran en Anexo de la presente
resolución como parte de la misma, por los daños y perjuicios causados y en las cantidades allí recogidas, todo ello, sin perjuicio de que en sede de ejecución de sentencia, se concreten o modifiquen aquellas en los términos expuestos en e] Razonamiento Jurídico octavo de la presente resolución, con la responsabilidad civil subsidiaria y con carácter solidario de la mercantil "Etv1G"/TFX", y con aplicación de los intereses de mora prevenidos en el artículo 576 de la Ley de Enjuiciamiento Civil .
Para el cumplimiento de las penas privativas de libertad, se fes computará el tiempo de prisión provisional padecido en esta causa.
Una vez firme la presente, se acordará lo procedente respecto de su ejecución para lo cual deberán desplegarse las acciones necesarias dirigidas a la recuperación de los activos, acudiendo para ello a los mecanismos de auxilio y cooperación jurisdiccional y policial internacional, necesarios a tal fin.
Notifíquese esta resolución a todas las partes y a los interesados, haciéndoles saber que la misma no es firme, y cabe interponer contra aquella recurso de casación ante la Sala de lo Penal del Tribunal Supremo, que deberá prepararse ante esta Sala en plazo de los cinco días siguientes al de la última notificación.
Así por esta nuestra sentencia, la pronunciamos, mandamos y firmamos".

TERCERO
Notificada la sentencia a las partes, se preparó recurso de casación por la representación de Raquel y las representaciones de las acusaciones particulares de ACCUVEN BUSINESS & FINANCIAL SERVICES INC D. Indalecio, INVERSIONES FOREX CANARIAS. S.L.D., y Rafael, que se tuvo por anunciado remitiéndose a esta Sala Segunda del Tribunal Supremo las certificaciones necesarias para su sustanciación y resolución, formándose el correspondiente rollo y formalizándose los recursos.

CUARTO
Formado en este Tribunal el correspondiente rollo, la representación del recurrente, formalizó el recurso, alegando los siguientes MOTIVOS DE CASACIÓN:
La representación de Raquel y Blas:

PRIMERO.- Por infracción de ley e infracción de precepto constitucional artículo 24.2, por vulneración del derecho a la presunción de inocencia y del derecho a la tutela judicial efectiva, al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial , y al amparo dispuesto en los artículos 849.1 y 852 Ley de Enjuiciamiento Criminal , artículo 5.4 Ley Orgánica del Poder Judicial .

SEGUNDO.-Por infracción de ley e infracción de precepto constitucional, artículos 18.3 , 18.1 y 24.2 por vulneración del derecho al secreto de las comunicaciones, al derecho a la intimidad y al derecho un proceso con las debidas garantías al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial , y al amparo de lo dispuesto en los artículos 849.1 y 852 de la Ley de Enjuiciamiento Criminal , artículo 5.4 LOPJ .

TERCERO.- Por infracción de ley por aplicación indebida de los artículos del Código Penal 248,200 49,250.1.6 390.1.2º, 392.1, 301.1 (según redacción vigente en el momento de los hechos) 515.1 y 517.1, al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial , y de lo dispuesto en los artículos 849.1 y 852 de la Ley de Enjuiciamiento Criminal .

CUARTO.- Con carácter subsidiario a los precedente motivos de recurso, se invoca infracción de precepto constitucional al amparo del artículo 852 Ley de Enjuiciamiento Criminal , por vulneración del derecho a la tutela judicial efectiva y del derecho un proceso con las debidas garantías reconocidos en el artículo 24 1 Y 2 de la Constitución Española respectivamente, por entender la sentencia de instancia que la asociación "Accuven Bussiness Financial Services INC. estaba legitimada para ejercer la acusación particular.

QUINTO
Instruido el Ministerio Fiscal del recurso interpuesto, la Sala admitió el mismo, quedando conclusos los autos para señalamiento de fallo cuando por turno correspondiera.

SEXTO
Por Providencia de esta Sala de fecha 20 de febrero de 2018 se señala el presente recurso para fallo para el día 14 de marzo del presente año, prolongándose la deliberación del mismo hasta el día de la fecha.

FUNDAMENTOS DE DERECHO
PRIMERO
La sentencia objeto de nuestra revisión transaccional condena a los dos recurrentes como autores responsables de un delito continuado de estafa, agravado por el valor de la defraudación, en concurso ideal con un delito de falsedad en documento oficial. Igualmente condena a los recurrentes como autores responsables de un delito de blanqueo de capitales y otro de asociación ilícita.
Los dos recurrentes formalizan una impugnación conjunta en la que cuestionan en los dos primeros motivos, la correcta enervación de su derecho fundamental a la presunción de inocencia, desde la perspectiva de la ilegalidad en la producción de la prueba, y consecuentemente, desde la insuficiencia de la precisa actividad probatoria. En el motivo tercero, el error de derecho por la indebida aplicación de los tipos penales objeto de la condena. En el cuarto cuestiona la vulneración del derecho tutela judicial efectiva -con las garantías debidas-, que concreta en el hecho de haber sido admitida la personación de una acusación particular a pesar de la falta de legitimación que fue denunciada como cuestión previa.
En síntesis, el relato fáctico, extenso en su redacción declara probado que los acusados, en compañía de otras personas a las que no afecta esta resolución crearon una estructura de carácter permanente con la que enriquecerse ilícitamente, mediante la puesta en funcionamiento de un sistema defraudatorio capaz de afectar a un elevadísimo número de víctimas se refiere la utilización de sociedades y empresas, entre las que destaca finanzas Forex, con la que se captan clientes y a los que prometen elevadas retribuciones por su inversión en el sector inmobiliario, el mercado del oro, etc.. En apartado quinto del hecho probado se añade que "aunque las cantidades aportadas por los inversores no se destinaban al mercado y por lo tanto no generaban rendimiento alguno, el acusado, con la finalidad de mantener el engaño al que habían sido sometidos los clientes a través de la página web y en formato electrónico... facilito extractos de movimientos ficticios y "certificados de inversión" con los que les hacían creer que habían obtenido ganancias en poco tiempos y que mantenían saldos positivos..." En otros apartados de la relación fáctica se indica las sanciones y advertencias de la Comisión nacional del mercado de valores y otros similares de países de la Unión Europea, así como del mercado financiero de Estados Unidos, no obstante lo cual los acusados pusieron en marcha inversiones en diferentes modalidades y bajo un complejo entramado de "sociedades pantallas" a través de las cuales se realizaron numerosas operaciones inmobiliarias.
Analizamos en primer término el motivo opuesto en cuarto lugar en el que cuestiona la vulneración de su derecho fundamental al proceso debido, al entender que la asociación "Accuven Bussinessand Financial Services inc" no debió ser admitida como acusación particular porque "no concurrirían los requisitos procesales para la admisión de la persuasión como acusación al no costar esa entidad ni con la presentación de poderes necesarios para ser parte del procedimiento." La cuestión deducida en el recurso ha sido objeto de análisis en

la sentencia impugnada. En el fundamento primero, apartado d), el tribunal de instancia rechaza la queja planteada al inicio del enjuiciamiento y declara la correcta personación de la entidad "Accuven" señalando la sentencia la representación de la misma, identificando los perjudicados a quienes representaban y señalando que la responsabilidad civil se determinará en ejecución de sentencia en función del anexo que se adjunta a la sentencia y la documentación de sus correspondientes créditos en virtud de los contratos cuya nulidad se ha declarado. El contenido de la impugnación se refiere a lo que el tribunal y el juzgado de instrucción debió realizar para constatar la efectiva representación de perjudicados, los estatutos de la persona jurídica y la forma de designación y apoderamiento de sus representantes en el pleito, alegaciones que pudieron, y le debieron, ser objeto de análisis y cuestionamiento en el juicio oral a través de las personas que eran sus representantes y actuaron en su representación. En este sentido el tribunal ha dispuesto que los elementos y documentos son suficientes para tener por formulada la representación y la tiene por personada. Ratifican en el fundamento primero, apartado D, de la sentencia, para denegar la pretensión de nulidad que con invocación del derecho al proceso debido se alega en este motivo de casación.

SEGUNDO

Analizamos conjuntamente el primero y el segundo los motivos de casación en los que el recurrente denuncia, respectivamente la vulneración del derecho fundamental a la presunción de inocencia por inexistencia actividad probatoria para conformar el hecho probado, en tanto que en el segundo motivo denuncia la vulneración del derecho al secreto de las comunicaciones, a la intimidad y al derecho a un proceso con las garantías debidas que entiende se han producido en la diligencia de volcado de los ordenadores realizado en el juzgado, entendiendo que tales diligencias supusieron una ilícita injerencia en los derechos fundamentales afectados y expone que, aunque en la diligencia de volcado estuvo presente el Letrado de la administración de justicia, no estuvo presente el recurrente, que se encontraba preso a disposición del juzgado. Consciente de que la principal actividad probatoria resulta del mencionado registro policial y de los correos electrónicos intervenidos, cuestiona la legalidad de ese proceso intervención y, consecuentemente, la vulneración del derecho fundamental a la presunción de inocencia.

En reiterada jurisprudencia de esta sala hemos señalado que el contenido esencial del derecho fundamental a la presunción de inocencia, cuando es invocada ante esta sala de casación en un proceso de revisión que afecta a dicho derecho fundamental, exigir que esta sala examine y compruebe que la actividad probatoria desarrollada ante el tribunal de instancia desde la perspectiva de la legalidad, de la licitud de la actividad probatoria, y desde la perspectiva de su estructura racional en virtud de la cual se declara un hecho probado que incrimina a la persona acusada. Es por ello que ambos motivos deben ser analizados conjuntamente pues el derecho fundamental a la presunción de inocencia parte de comprobar la legalidad y la regularidad de la prueba y el examen de su carácter de cargo. El recurrente cuestiona dos apartados bajo la rúbrica de vulneración del derecho fundamental a la presunción de inocencia: de una parte, la regularidad de la diligencia consistente del volcado de los ordenadores. De otra, la estructura racional de la prueba que permite la incriminación contenida en el hecho declarado probado.

Con relación al primer apartado el apartado E) del fundamento de derecho primero de la sentencia analiza la corrección legal y constitucional de la diligencia del registro en el domicilio de los acusados y de la diligencia del volcado de ordenadores. A su contenido nos remitimos por la corrección expresada respecto a la observancia de los hechos y garantías de las diligencias de entrada y registro y del volcado y copia de los ordenadores que estuvieron amparados en la autorización judicial. El registro domiciliario se realizó bajo autorización judicial, con asistencia del fedatario público y de la presencia del propio acusado, detenido, trasladándose el contenido de lo referenciado en el acta de registro al juzgado, donde, a presencia del Letrado de la administración de justicia, y del letrado del recurrente se procedió a su volcado en los términos autorizados por el registro acordado judicialmente. El recurrente cuestiona que no estuvo presente en dicha diligencia que afecta a su derecho a la intimidad, protegida constitucionalmente, pero esa exigencia no aparece en la ley cuando regula esa diligencia a partir de la ley 13/2015, de 5 octubre, ni con anterioridad, tampoco se exigiría esa presencia, y la situación procesal del investigado aparecía suficientemente cubierta con la actuación de la Comisión judicial en cumplimiento de la orden judicial, y con la asistencia del letrado defensor del recurrente. Como dice la sentencia de 2 marzo de 2016, el nuevo artículo 588 sexies c) ni siquiera requiere la presencia de secretario judicial en el momento de abrir el ordenador. El juzgado proporcionó las garantías previstas en la ley a la diligencia de volcado de la información, por lo que la misma es regular y lícita, pudiendo conformar la prueba susceptible de ser valorada por el tribunal de instancia los términos que veremos a continuación.

En el siguiente apartado de oposición a la sentencia denuncia la vulneración del derecho fundamental a la presunción de inocencia, cuestionando la existencia de prueba que acredite la participación de los acusados en los hechos. En el desarrollo argumental del motivo funda la queja casacional en la nulidad de la diligencia anterior, y respecto a la restante prueba arguye que las declaraciones de los funcionarios policiales solamente afirman el contenido de las comisiones rogatorias, y niegan extremos fácticos, como la promesa de elevados rendimientos a las inversiones y que los perjudicados no fuesen advertidos del riesgo que asumían. En definitiva, que no existía engaño que determine la existencia de la estafa piramidal que se describe en el hecho.

El motivo carece de base atendible y debe ser desestimado. La realidad de los hechos aparece determinada por las propias declaraciones de los acusados en orden a la referencia que el hecho probado contiene sobre adquisición de inmuebles. Además, los propios recurrentes admiten la existencia de la actividad probatoria precisa cuando refieren que el núcleo esencial de la prueba de cargo que justifica la condena se deriva del registro policial de los correos electrónicos de los acusados, lo cual supone un reconocimiento de la precisa

actividad probatoria, por más que en este motivo niegue su capacidad convictiva en base a la nulidad de dicha diligencia por motivos aducidos en el motivo segundo que ha sido analizado con anterioridad. Si, como hemos dicho, la actividad probatoria de volcado de los ordenadores e intervención de los correos electrónicos es regular en su obtención, y lícita, el tribunal puede, como lo ha hecho, obtener su convicción a partir del contenido de esa actividad probatoria. El tribunal de instancia valora la actividad probatoria en el fundamento de derecho segundo donde recoge con detalle el entramado personal y societario, las ofertas de negociación realizadas, las promesas y la actividad que se relata el hecho probado que resulta de la abundante prueba documental intervenida. El tribunal analiza y valora las declaraciones de los acusados destacando sus contradicciones internas derivadas de otra prueba presentada por ellos, prueba pericial, de la que resulta la realidad de los hechos, explicados por informes periciales, comisiones rogatorias, documentación bancaria que ha sido intervenida. Igualmente el fundamento tercero de la sentencia realiza la valoración de la prueba con un contenido argumentativo amplio que de forma racional y lógica desarrolla la función judicial al realizada por el de una distancia. El análisis de los informes policiales confeccionados sobre la documentación intervenida permite la afirmación del relato fáctico con un análisis de los denominados contratos de inversión que cada uno de los perjudicados realizaba exponiendo las inversiones en distintos países con un entramado de empresas. Las argumentaciones del recurrente, cuestionando la veracidad de los testigos al tiempo que realiza una valoración de sus declaraciones, son ajenas al contenido esencial del derecho que invoca. Desde la función de revisión que nos corresponde comprobamos la regularidad de la prueba y la estructura racional de la motivación a partir de la prueba personal valorada por el tribunal que directamente la ha percibido, por lo que nos remitimos a la explicación y motivación de la sentencia realizada en explicación de la convicción obtenida por el tribunal de estancia.
Constatada la existencia de la precisa actividad probatoria el motivo se desestima.

TERCERO
En el tercer motivo de la oposición denuncia el error de derecho por la indebida aplicación al relato fáctico dos artículos 248 , 249 , 250 , 390 , 392 , y 515 y 517 del Código penal , es decir los tipos penales objeto de la condena. Sin embargo en la exposición argumental del motivo el recurrente se aparta de la vía de impugnación elegida para cuestionar la actividad probatoria. Así señala que, con relación al delito de estafa, no concurrió en los elementos porque "no estarían acreditados los elementos del tipo de la estafa, especialmente el dolo por parte del autor", lo que supone una reiteración del contenido del motivo anterior referido a la vulneración del principio de presunción de inocencia.
Con relación al delito de falsedad refiere que los apuntes contables acreditan la realidad de las inversiones, no eran falsos, lo que incidiría del derecho fundamental a la presunción de inocencia ya analizado, y, en todo caso, no serían documentos mercantiles, sino privados. El motivo se desestima. Frente a la argumentación de recurrente sobre la inocuidad del documento y los apuntes contables contenidos en el mismo, su examen permite comprobar que se trata de anotaciones contables que cumplen con las exigencias documentales de garantía y de acreditación de la realidad de una operación mercantil y, por lo tanto, serían documentos mercantiles. El Código penal no contiene una definición de lo que debe entenderse por documento mercantil. Su concreción ha sido realizada por la Jurisprudencia de esta Sala y las posiciones de la doctrina científica que durante mucho tiempo la censuraron abiertamente. La jurisprudencia de esta Sala hasta 1991 mantuvo un concepto amplio de lo que debió entenderse por documento mercantil compresivo de los documentos regulados en el Código de Comercio y leyes especiales mercantiles, también aquellos documentos que recogen una operación de comercio o que tengan validez o eficacia para hacer constar derechos u obligaciones de tal carácter o sirvan para demostrarlos (STS 22.2.1985 ; 3.2.1989). A partir del año 1990 está jurisprudencia varía para delimitar el concepto de documento mercantil a los documentos explícitamente contemplados en la legislación mercantil que tengan una eficacia jurídica superior a la de simple documento privado que justifique la agravación de su falsedad respecto a la de aquél (SSTS 31.5.91 ; 1.4.91 y su antecedente de 17.5.89). Justifica ese cambio jurisprudencial la mayor punición de este tipo de documento frente a los privados y su equiparación más los documentos públicos y oficiales que sí tienen en nuestro ordenamiento una definición (art. 1216 Código civil y 596 de la derogada Ley de Enjuiciamiento Civil). También la constatación del hecho de que la falsificación de documentos mercantiles normalmente acompaña a otros delitos normalmente patrimoniales. La STS 1387/2015, de 17 de febrero , nos dice que consolidada jurisprudencia, al analizar el concepto jurídico-penal de documento mercantil, ha manifestado que se trata de un concepto amplio, equivalente a todo documento que sea expresión de una operación comercial, plasmado en la creación, alteración o extinción de obligaciones de naturaleza mercantil, ya sirva para cancelarlas, ya para acreditar derechos u obligaciones de tal carácter, siendo tales "no solo los expresamente regulados en el Código de Comercio o en las Leyes mercantiles, sino también todos aquellos que recojan una operación de comercio o tengan validez o eficacia para hacer constar derechos u obligaciones de tal carácter o sirvan para demostrarlas, criterio éste acompañado, además por un concepto extensivo de lo que sea aquella particular actividad. Como documentos expresamente citados en estas leyes figuran las letras de cambio, pagarés, cheques, órdenes de crédito, cartas de porte, conocimientos de embarque, resguardos de depósito y otros muchos: también son documentos mercantiles todas aquellas representaciones gráficas del pensamiento creadas con fines de preconstitución probatoria, destinadas a surtir efectos en el tráfico jurídico y que se refieran a contratos u obligaciones de naturaleza comercial. Finalmente, se incluyen otro tipo de representaciones gráficas del pensamiento, las destinadas a acreditar la ejecución de dichos contratos tales como facturas, albaranes de entrega u otros semejantes.

Desde lo expuesto es claro que la documentación de operaciones de inversión en las que se captaban capitales ofreciendo una rentabilidad, reflejan operaciones mercantiles y por lo tanto cumple con las exigencias expuestas para su consideración de documento mercantil. En este sentido, los denominados "certificados de inversión" cumplen las exigencias de garantía, constitución y prueba que caracterizan el documento mercantil.
Con relación al delito de asociación ilícita, el recurrente cuestiona su aplicación no por la concurrencia de los elementos de los artículos 515 y 517 el Código penal sino, sobre todo, por el incumplimiento de las convención de Palermo en cuanto refieren la necesidad de tres personas, como mínimo para su declaración. El motivo se desestima. Basta con la referencia contenida en el fundamento de derecho cuarto en el que aborda la tipicidad de los hechos declarados probados y, concretamente, en los distintos delitos objeto de la condena señalando que los dos condenados, junto a otros acusados contra los que no se sigue el juicio oral formaban una estructura material permanente para llevar a cabo una serie de actividades ilícitas, como lo es el complejo entramado formado a través de numerosas personas jurídicas, muchas de ellas, en paraísos fiscales, destinadas a continuar la actividad delictiva y a ocultar, a través de diversas operaciones mercantiles que el dinero de los inversores que había empecinado su inversión al mercado de divisas. Desde el inicio de las operaciones, desde la propia creación de las empresas, se organiza una trama para captar un dinero que revierta en el beneficio particular de los acusados. La sentencia explica, y el recurrente no discute, la exigencia de la estructura organizativa, la finalidad delictiva de la pluralidad de personas que la permanencia de la asociación dentro de una organización jerarquizada.
Ningún error cabe declarar por lo que el motivo se desestima.

F A L L O
Por todo lo expuesto, en nombre del Rey y por la autoridad que le confiere la Constitución, esta sala ha decidido Desestimar el recurso de Casación interpuesto por la representación procesal de Dña. Raquel y Don Blas , contra sentencia dictada el día 10 de marzo de 2017 en causa seguida contra ellos mismos y otros, por delitos de estafa, falsificación en documento mercantil, blanqueo de capitales y asociación ilícita.
Imponer a dichos recurrentes el pago por mitad de las costas ocasionadas en el presente recurso.
Comuníquese esta resolución a la mencionada Audiencia a los efectos legales oportunos, con devolución de la causa.
Notifíquese esta resolución a las partes e insértese en la colección legislativa.
Así se acuerda y firma.

Andrés Martínez Arrieta
Miguel Colmenero Menéndez de Luarca
Juan Ramón Berdugo Gómez de la Torre
Alberto Jorge Barreiro
Andrés Palomo Del Arco

Jurisprudencia nacional

CORTE SUPREMA DE JUSTICIA DE LA REPÚBLICA
SALA PENAL PERMANENTE
R. N. N.° 2041-2018
LIMA

Objeto civil y titularidad
La titularidad del objeto civil descansa en el perjudicado por el delito. Pero cuando este no se apersona o no formula pretensión el Ministerio Público debe peticionar un monto indemnizatorio como consecuencia jurídica del hecho delictivo. Por el contrario, si el afectado ejerce su derecho a una reparación civil, ya no le corresponde al fiscal formular la pretensión resarcitoria.
Lima, diecinueve de noviembre de dos mil diecinueve

VISTOS: los recursos de nulidad interpuestos por los encausados Luis Miguel Salinas Torrez y Jesús Alberto Horna Salazar y por la Procuraduría Pública de Orden Público del Ministerio del Interior contra la sentencia del dieciocho de septiembre de dos mil dieciocho (foja 647), en el extremo en el que fijó la reparación civil solidaria en S/ 30 000 (treinta mil soles) a favor del Estado y en S/ 16 000 (dieciséis mil soles) a favor de la empresa Selme S. A. C., sin perjuicio de devolver el monto indebidamente transferido a la empresa agraviada. De conformidad en parte con lo opinado por el señor fiscal supremo en lo penal.
Intervino como ponente el señor juez supremo Príncipe Trujillo.

CONSIDERANDO
I. De las pretensiones impugnativas
Primero. El encausado Salinas Torrez, al formalizar su recurso (foja 669), señaló expresamente que su impugnación estaba dirigida al monto fijado como reparación civil. Argumentó que no le es posible pagarlo, pues carece de patrimonio y solo gana el sueldo mínimo. Aunque, por otro lado, refirió que no se acreditó el dolo en su actuación, que aceptó los cargos con la finalidad de dar por concluido rápidamente el proceso y no

someterse a una condena efectiva, y que debió aplicarse el error de tipo, ya que equivocadamente hizo entrega de su tarjeta de débito y su clave del BBVA, sin saber cuál era el propósito del solicitante.

Segundo. El imputado Horna Salazar, en la fundamentación de su recurso (foja 673), denunció la vulneración de la garantía de la motivación de las resoluciones judiciales, pues refirió que no se especificó qué tipo de daño se ocasionó a los agraviados y que el monto de la reparación civil resulta desproporcional a los ingresos que percibe. Solicitó que se disminuya la reparación civil a S/ 20 000 (veinte mil soles).

Tercero. La representante de la Procuraduría, en su recurso formalizado (foja 660), instó el incremento de la reparación civil, en virtud de la magnitud del daño ocasionado y el perjuicio producido al Estado.
Sostuvo que para la determinación del quantum patrimonial del daño se debió considerar el gasto que irroga la lucha contra el crimen organizado, tanto para la prevención como la protección de la adquisición de nueva tecnología, además del sueldo de los operadores de justicia (daño emergente). Argumentó que tal gasto perjudica el monto que se destinaría a la construcción de hospitales, centros educativos y otras inversiones sociales (lucro cesante) y que existe un daño moral, ya que el crimen organizado pone en zozobra a la sociedad representada por el Estado. Indicó que a ello debió sumarse el detrimento que se genera a la imagen del Estado, por los índices de confianza en el sector público. En suma, solicitó que se incremente el monto fijado a S/ 50 000 (cincuenta mil soles).

II. De los hechos objeto del proceso penal
Cuarto. El Tribunal Superior declaró probado que Jesús Alberto Horna Salazar, Luis Miguel Salinas Torrez y Ángel Stiven Orozco Ramos conformaron una asociación dedicada a cometer fraudes informáticos mediante el uso de aparatos tecnológicos de última generación y herramientas virtuales o software especiales que les permitían obtener información reservada de los números de cuentas y claves secretas de sus víctimas. Así, el catorce de enero de dos mil catorce ingresaron a las cuentas bancarias que en moneda nacional y extranjera tenía la empresa Selme S. A. C. en el Banco Continental y realizaron tres trasferencias electrónicas de S/ 4800 (cuatro mil ochocientos soles) cada una, por medio del servicio Banca por Internet, a las cuentas de los referidos imputados.

III. De la absolución del grado
Quinto. La fiscal superior de Lima, mediante el dictamen del veintitrés de noviembre de dos mil diecisiete, formuló acusación contra los recurrentes Jesús Alberto Horna Salazar y Luis Miguel Salinas Torrez por el delito de asociación ilícita para delinquir y fraude informático, previstos, respectivamente, por el artículo 317 del Código Penal y el artículo 8 de la Ley número 30096 (Ley de Delitos Informáticos).
Su pretensión incluyó la pena y la reparación civil. Sobre esta última, solicitó que se imponga la suma de S/ 4000 (cuatro mil soles) a favor de cada agraviado (empresa Selme S. A. C. y el Estado).

Sexto. Puesta en conocimiento de los sujetos procesales la acusación fiscal, solo la representante de la Procuraduría Especializada en Delitos contra el Orden Público formuló oposición. En lo central, peticionó una reparación civil ascendente a S/ 50 000 (cincuenta mil soles). Argumentó que se trató de un caso de delincuencia económica que incrementó la inseguridad ciudadana y que genera gastos destinados a la lucha contra la criminalidad, en desmedro de una inversión en educación, salud o modernización del país.

Séptimo. Los hechos declarados probados se dedujeron de la conformidad de los acusados con ellos, la cual se alcanzó previo acuerdo con su representación letrada y con el cumplimiento del procedimiento establecido en la Ley número 28122, apartado 5, esto es, el conocimiento previo de los hechos imputados y sus consecuencias jurídicas y la observancia de la doble garantía que representa, de un lado, la personalísima anuencia del imputado y, de otra parte, el asesoramiento de su abogado defensor (véanse las actas del cinco y el catorce de septiembre de dos mil dieciocho, a fojas 642 y 645, respectivamente).
Los procesados, asistidos por sus respectivos abogados, se limitaron a señalar que no estaban de acuerdo con la reparación civil solicitada, pues estaban colaborando con la justicia al someterse a la conclusión anticipada.

Octavo. La reparación civil es una institución de naturaleza jurídico-civil, que descansa en el daño ocasionado, no en el delito cometido, y se proyecta, en cuanto a su contenido, a lo establecido en el artículo 93 del Código Penal, y procesalmente está informada por los principios dispositivo y de congruencia. La titularidad del objeto civil descansa en el perjudicado por el delito, pero cuando este no se apersona o no formula pretensión el Ministerio Público debe peticionar un monto indemnizatorio como consecuencia jurídica del hecho delictivo. Por el contrario, si el afectado ejerce su derecho a una reparación civil, ya no le corresponde al fiscal formular la pretensión resarcitoria.
Luego, dentro de los marcos de la pretensión civil y de la resistencia, corresponderá al órgano jurisdiccional fijar motivadamente la cuantía de la reparación civil.

Noveno. En el presente caso, la reparación civil de S/ 4000 (cuatro mil soles) solicitada a favor de la empresa Selme S. A. C. no fue objetada por aquella y, por ende, el Tribunal Superior no podía alterarla sorpresivamente en perjuicio de los imputados. Aquel monto peticionado por el fiscal superior en su acusación incluyó los conceptos de daño patrimonial y extrapatrimonial por el delito de fraude informático y, si bien se aprecia que

no cubre el monto indebidamente apropiado por los acusados, no corresponde al órgano jurisdiccional modificarlo, pues el titular del objeto civil se ha conformado.

Décimo. Caso distinto ocurrió con el delito de asociación ilícita, pues la Procuraduría Pública Especializada en Delitos contra el Orden Público, en representación del Estado, objetó el monto solicitado por el fiscal.
Su petición, acogida parcialmente, incluyó una reparación por los gastos que irroga el Estado para luchar contra el crimen organizado y, evidentemente, también la gravedad del ilícito y la modalidad de su realización, con especial consideración de que los delitos informáticos se han acrecentado y están generando un grave perjuicio en la seguridad económica de los ciudadanos. Sin embargo, los S/ 30 000 (treinta mil soles) fijados por el Tribunal Superior son suficientes para cumplir con los objetivos indemnizatorios y no se han formulado nuevos criterios que permitan incrementar dicho monto.

DECISIÓN
Por estos fundamentos, los jueces integrantes de la Sala Penal Permanente de la Corte Suprema de Justicia de la República **DECLARARON:**

I. HABER NULIDAD en la sentencia del dieciocho de septiembre de dos mil dieciocho (foja 647), en el extremo en el que fijó en S/ 16 000 (dieciséis mil soles) el monto de la reparación civil que deberán abonar solidariamente Luis Miguel Salinas Torrez y Jesús Alberto Horna Salazar, con el condenado Ángel Stiven Orozco Ramos, a favor de la empresa Selme S. A. C.; REFORMÁNDOLA, fijaron en S/ 4000 (cuatro mil soles) la reparación civil solidaria a favor de la empresa Selme S. A. C., sin perjuicio de devolver el monto indebidamente transferido a la citada empresa.

II. NO HABER NULIDAD en la acotada sentencia, en cuanto a que fijó la reparación civil solidaria en S/ 30 000 (treinta mil soles) a favor del Estado; con lo demás que al respecto contiene y es materia del recurso. Hágase saber a las partes procesales apersonadas en esta Sede Suprema. Y los devolvieron.
Intervino el señor juez supremo Castañeda Espinoza por periodo vacacional de la señora jueza suprema Chávez Mella.