FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

TESIS

“Análisis de la ley 30096 de delitos informáticos en su aplicación a los delitos de fraude informático en el Perú, 2022”

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

Autor

Bach. Alcantara Diaz Fabian Eduardo

https://orcid.org/0000-0002-2386-4077

Asesora

Dra. Delgado Fernandez Rosa Elizabeth

https://orcid.org/0000-0001-6995-3609

Línea de Investigación

Desarrollo Humano, Comunicación y Ciencias Jurídicas para enfrentar los Desafíos Globales

Sublínea de Investigación

Poblaciones vulnerables y brechas sociales

Pimentel – Perú

2024

DECLARACIÓN JURADA DE ORIGINALIDAD

Quien suscribe la DECLARACIÓN JURADA, soy Fabian Eduardo Alcantara Diaz, egresado del Programa de Estudios de la Escuela Profesional de Derecho y Humanidades de la Universidad Señor de Sipán S.A.C, declaro bajo juramento que soy autor del trabajo titulado:

"Análisis de la ley 30096 de delitos informáticos en su aplicación a los delitos de fraude informático en el Perú, 2022"

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación de la Universidad Señor de Sipán, conforme a los principios y lineamientos detallados en dicho documento, en relación con las citas y referencias bibliográficas, respetando el derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y autentico.

En virtud de lo antes mencionado, firma:

Alcantara Diaz Fabian Eduardo	DNI: 75556039	

Pimentel, 27 de Marzo de 2024.

REPORTE DE SIMILITUD TURNITING

Reporte de similitud

NOMBRE DEL TRABAJO

"Análisis de la ley 30096 de delitos infor máticos en su aplicación a los delitos de fraude informáti

AUTOR

Fabian Eduardo Alcantara Diaz

RECUENTO DE PALABRAS

20673 Words

RECUENTO DE CARACTERES

109270 Characters

RECUENTO DE PÁGINAS

52 Pages

TAMAÑO DEL ARCHIVO

147.6KB

FECHA DE ENTREGA

Apr 4, 2024 8:52 AM GMT-5

FECHA DEL INFORME

Apr 4, 2024 8:53 AM GMT-5

15% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 14% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 8% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 8 palabras)

“ANÁLISIS DE LA LEY 30096 DE DELITOS INFORMÁTICOS EN SU APLICACIÓN A LOS DELITOS DE FRAUDE INFORMÁTICO EN EL PERÚ, 2022”

Aprobación del jurado

DR. GONZALES HERRERA JESUS MANUEL

Presidente del Jurado de Tesis

MG. HANANEL CASSARO CECILIA ELIZABETH

Secretario del Jurado de Tesis

MG. DELGADO FERNANDEZ ROSA ELIZABETH

Vocal del Jurado de Tesis

“ANÁLISIS DE LA LEY 30096 DE DELITOS INFORMÁTICOS EN SU APLICACIÓN A LOS DELITOS DE FRAUDE INFORMÁTICO EN EL PERÚ, 2022”

Resumen

En el proyecto de investigación se estableció como problemática el delito de fraude cibernético dentro de nuestra legislación, es por este motivo que se estableció como objetivo general el poder analizar la ley 30096 de delitos informáticos en su aplicación a los delitos de fraude informático en el Perú, esto con el fin de poder determinar si existen vacíos u omisiones legales dentro de la presente ley de la cual los ciberdelincuentes puedan sacar provecho, es por ello que en el primer capítulo se dará a conocer cuál es la realidad problemática en el presente tema tanto a nivel internacional, nivel nacional y nivel local, los antecedentes de estudio tanto a nivel internacional, nivel nacional y nivel local, las teorías relacionadas al tema, la formulación del problema en donde se evidencia cual es el problema general y los problemas específicos dentro de la investigación, también la justificación e importancia del estudio tanto justificación teórica, justificación social, justificación practica y metodológica, además también de los objetivos tanto general como específicos, en el capítulo segundo se podrá visualizar el material y método y dentro de él se podrá constatar el tipo y diseño de la investigación, el escenario de estudio, categorización de sujetos participantes, las categorías, subcategorías y matriz de categorización, las técnicas e instrumentos de recolección de datos, validez y confiabilidad, procedimientos de análisis de datos, criterios éticos, criterios de rigor científico, en el tercer capítulo podremos ver cuáles son los . resultados de la investigación tanto en tablas y figuras, discusión de resultados y el aporte practico, por último, en el cuarto y último capítulo podremos conocer cuáles fueron las conclusiones y recomendaciones, además de las referencias bibliográficas y los anexos correspondientes.

Palabras Clave: Delitos Informáticos, Fraude Cibernético, Ciberdelincuentes

Abstract

In the present research project, the crime of cyber fraud was established as a problem within our legislation, it is for this reason that the general objective was established to be able to analyze the law 30096 of computer crimes in its application to the crimes of computer fraud in the Peru, this in order to determine if there are legal gaps or omissions within this law from which cybercriminals can take advantage, which is why in the first chapter it will be announced what is the problematic reality in this topic both internationally, nationally and locally, the background of the study both internationally, nationally and locally, theories related to the subject, the formulation of the problem where the general problem and the specific problems within are evident, of the investigation, also the justification and importance of the study both theoretical justification, social justification, just Practical and methodological ification, in addition to the general and specific objectives, in the second chapter you can see the material and method and within it you can see the type and design of the research, the study scenario, categorization of participating subjects. , the categories, subcategories and categorization matrix, the data collection techniques and instruments, validity and reliability, data analysis procedures, ethical criteria, scientific rigor criteria, in the third chapter we will be able to see what the . research results both in tables and figures, discussion of results and practical contribution, finally, in the fourth and last chapter we will be able to know what the conclusions and recommendations were, in addition to the bibliographic references and the corresponding annexes.

Keywords: Computer Elites, Cyber Fraud, Cybercriminals

I. INTRODUCCIÓN

A lo largo de los años, en la mayoría de lugares del mundo como en nuestro país, la tecnología se ha estado desarrollando rápidamente y nos ha brindado muchas ventajas, como la tecnología, dispositivos móviles, ordenadores, esto nos trajo una nueva era de comunicación e información gracias al internet, este tipo de prácticas, conocimientos y herramientas relacionadas con el consumo de la información a través de la red hasta el día de hoy sigue avanzando gracias a las constantes investigaciones y avances tecnológicos, ya sea mejora de dispositivos móviles u ordenadores, nuevas tecnologías de comunicación como las antenas 5G lo cual potencia el uso de la red y la comunicación y nos permite que comunicarnos con personas en cualquier parte del mundo sea algo mucho más fácil, gracias a todo lo mencionado ha cambiado nuestro estilo de vida, facilitándonos la vida en muchos aspectos, pero no todo son ventajas, con la llegada de esta era tecnológica también llegaron personas a aprovecharse de ellas para empezar a cometer nuevos tipos de delitos pero no comunes , a estos delitos se les llamo delitos informáticos que en primera instancia no estaban dentro del control legal o social o debidamente reglamentados en nuestra legislación peruana, es por ello que con esta nueva era muchas personas utilizan esto a su favor para poder proporcionar información falsa y creíble, cambiar datos y hacerse pasar por Internet por otras personas esto con el único motivo de cometer fraude, lo que se denomina fraude informático o cibernético.

Es así que el fraude cibernético o informático y la estafa en modalidad de spoofing son dos de los delitos informáticos más comunes en nuestro ordenamiento peruano, por lo que la presente ley tienen como objetivo general cumplir con su rol preventivo y sancionador de toda aquella actividad ilegal en las que se utiliza el Internet para destruir datos y sistemas informáticos y atacar activos legales protegidos de importancia delictiva sustancial, es por ello que esta ley fue emitida para combatir de manera efectiva los delitos informáticos. En resumen, a finales de 2020, un año afectado por las pandemias y la cuarentena obligatoria, los delitos de estafa o fraude informática aumentaron exponencialmente, llegando a más de 9.000 casos, por lo tanto, ante el auge del ciberdelito en nuestro país, nuestro gobierno peruano se comprometió a firmar el Tratado de Budapest, y como resultado, el sector público se vio obligado a crear un departamento fiscal dedicado al ciberdelito porque antes de la creación de estas unidades fiscales especializados los fiscales penales ordinarios recibían todas las denuncias relacionadas con cibernéticos y muchas veces hacían mal sus funciones 1 por no haber recibido la formación adecuada para este delito en particular ni contar con capacitaciones adecuadas.

El presente proyecto de investigación ayudará a fiscales, ciudadanos en general y especialistas en ciberdelincuencia a poder reconocer e interpretar correctamente la presente ley en el manejo de casos de fraude informático, así como la comprensión de lo que es un sistema informático y las sanciones correspondientes para que puedan proporcionar la mejor función de prevención y sanción que otorga la ley.

Dentro de la realidad problemática a nivel internacional Bequai (2020) en su estudio "Delitos informáticos en Europa" expresa que, si se continúa el caos político a escala global, veremos cómo los sistemas de información y comunicación atraen la ira de los ciberdelincuentes, se librarán estas nuevas guerras y surgirá en forma computarizada o también denominada cibernética y aparecerá en computadoras y redes como lo hemos estado experimentado todo el tiempo hasta el día de hoy".

Si bien esto es cierto en el mundo actual que hemos experimentado en el siglo XXI, podemos mirar a nuestro alrededor y darnos cuenta de que estamos rodeados de sistemas informáticos en todas partes, pero otros países desarrollados, como los países del Este, difieren en sus políticas ya sea democrático y firme mediante la introducción de nuevas leyes que protejan los derechos de las personas y haga cumplir leyes civiles efectivas contra el robo o el fraude.

Herrera (2016) nos hace entender que, en Ecuador, la rebelión de los sistemas electrónicos y cibernéticos ha marcado un enorme monopolio entre los grupos tecnocráticos sobre el flujo de información procesada a nivel mundial, pues ya vivimos en una sociedad informatizada, el poder y la ambición son cada vez más sinónimos del control de todas las bases de datos cibernéticas existentes.

La OCDE (2020) publicó un informe titulado Delitos informáticos: un análisis de las leyes y reglamentos, dónde establecieron: qué reglamentos siguen vigentes hoy, y además de la reforma legislativa propuesta por muchos Estados miembros, también recomiendan qué a una lista de ejemplos del uso del período, que los estados o países pueden prohibir y sancionar de acuerdo con sus leyes adoptadas, como en el caso del fraude informático y la falsificación, y otras actividades delictivas que suelen ser sancionadas de esta manera, como la modificación de programas y datos informáticos, como la apropiación indebida y la interceptación de datos.

Forbes. (2021) señala que en México: Existe un gran número de integrantes de la CPICC que recomiendan que se instituyan aquella seguridad penal en contra de cualquier uso indebido ya sea se trate de espionaje cibernético o también de la no autorización del manejo de programas informáticos encriptados, estando incluido el hurto de secretos confidenciales o que afecten a todo un sector en el mercado o la industria.

Para completar la preparación del informe de la OCDE, el Consejo de Europa ha llevado a cabo un análisis exhaustivo del tema, cuyo único objetivo es proporcionar recomendaciones que ayuden al legislador a determinar qué tipo de comportamiento debe prevenirse. e identificado en la ley penal en la forma en que puede lograrse, teniendo siempre en cuenta cuál es el conflicto de interés y la necesidad de asegurar la protección en los Estados miembros.

En cuanto al nivel nacional de acuerdo con nuestra legislación, en el año 2013 se aprobó la Ley de Delitos Cibernéticos, Ley 30096, con el objeto de establecer las penas y penas correspondientes para todos los diversos delitos que pueden ser objeto de esta disposición.

Espinoza (2017), nos da a conocer que: “Ante el actual boom de la delincuencia informática en nuestra legislación peruana, se delimitar cual es el bien jurídico que está siendo lesionado por la ciberdelincuencia y poder examinar cuál es su debida evolución legislativa en el ordenamiento jurídico actual, además es preciso aclarar que ninguno de ciberdelitos no puede ser considerado una actividad la cual se pueda someter al deseo temporal que viven las personas día a día en la sociedad que se encuentra creciendo, es por ello que se aspira a la consolidación de leyes más eficaces y amplias para nuestra legislación.

García (2018) afirma: “No se puede dejar al Perú en una situación en la que tenga que sufrir consecuencias para lograr resultados, y la jurisprudencia debe promover una legislación que aborde mejor los vacíos legales”.

Como hemos aprendido recientemente, la tecnología es demasiado efectiva para facilitar la comisión de una variedad de delitos típicos. En algunos casos, las adaptaciones tradicionales no son imprescindibles, pero en otros es necesario adaptarse a los tipos de delitos para entender el comportamiento que utiliza la tecnología.

El efecto principal del uso de la información o la tecnología para lesionar los intereses legítimos de otros es el surgimiento de un nuevo bien jurídico que es necesario y confiable para la protección, por lo que la respuesta penal debe ser correcta en relación con todas las consecuencias probadas.

Blossiers (2018) afirma que: “A pesar de los esfuerzos de las organizaciones públicas y privadas, el uso de las tecnologías de la información ha tenido un impacto negativo en la sociedad en la que nos desenvolvemos, donde algunos ciudadanos utilizan sus conocimientos tecnológicos y se involucran en las redes informáticas utilizando Internet Las nuevas formas de cometer delitos contra la propiedad, como el fraude de computadoras en transacciones ilegales en beneficio de los ciberdelincuentes, afecta los derechos de propiedad de las personas debido a la falta de conocimiento sobre el uso de programas y tecnologías de rendimiento informático por parte de la mayoría de los usuarios”.

Entonces, el problema de nuestra legislación actual en materia de fraude en línea es que nuestra legislación no cubre ampliamente dónde se producen este tipo de delitos, teniendo en cuenta que la Comisión de Delitos se basa en hechos, normas y fuentes de evidencia.

En este caso, Akamai (2020) dice que, en la situación actual de nuestro país, nos enfrentamos a la delincuencia tanto a nivel nacional como internacional, y cabe recalcar que, aunque hoy en día se introduzcan leyes contra los ciberdelitos, aún existe una regulación en forma de ciberdelincuencia. Vulnerabilidad al fraude.

A nivel local según Custodio (2021), nuestro noticiero local anunció recientemente un escenario de alerta para los habitantes de la región, debido a que los usuarios del sector financiero están suspendiendo sus cuentas bancarias luego de registrar sus datos o datos.

Cuando se recibe códigos de información de su banco que redirige a una página falsa donde se insertan datos como nombre, número de cédula, número de cuenta y contraseña, recurso que los delincuentes utilizan para obtener beneficios económicos porque es la información básica de una persona. "

Fernández (2021) afirma que los ciberdelitos más comunes en la actualidad son el fraude informático, la usurpación de identidad, la extorsión y los ataques a la propiedad, por lo que existen muchos otros como el phishing. La legislación peruana, que por lo general solo regula los delitos de fraude cibernetico, en el artículo 8 del Capítulo V de la Ley de Delitos Informáticos en la Ley núm. 30096, incluso ahora hay varias omisiones como la fabricación de abuso. programa malicioso o portal web de malware.

Por otra parte, Ruiz (2020), nos da a conocer que tras los intentos de nuestra legislación peruana como también de la empresa privada aún sigue existiendo cada día mayor número de delitos cibernéticos como en este caso el fraude informático ha tenido graves daños en la comunidad, sobre todo en el departamento de Lambayeque, en el cual se han aprovechado de sus técnicas y conocimientos sobre ciberseguridad e informática para poder cometer delitos y atentar contra los ciudadanos y el derecho a su privacidad cometiendo actos ilegales en contra el patrimonio privado, esto afectando gravemente los derechos de los ciudadanos, sacando provecho de la falta de conocimiento de los ciudadanos y el desconocimiento de estos programas y software maliciosos que pueden inyectar fácilmente cualquier dispositivo electrónico.

En consecuencia, la problemática que existen en la región de que ya no pueden confiar en ningún anuncio, mensaje ni en sus propias cuentas bancarias se da porque en nuestra legislación no se cubre de forma vasta los entornos en los cuales se comete esta clase de delitos teniendo presente que la comisión delictiva se basa sobre la base los recursos fácticos, normativos y probatorios.

Dentro de los antecedentes de estudio a nivel internacional Ruiz (2020), en su investigación denominada “Estudio de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos” presentado en la Universidad Nacional de Loja - Ecuador, manifiesta que, actualmente la sociedad hace uso de diversos recursos cibernéticos para comunicarse, dando paso al aumento de delitos informáticos. Su principal objetivo es dar a conocer como estos delitos informáticos han incrementado y quedan impunes debido a que no logran identificar al culpable, provocando esto una violación a los derechos de los ciudadanos ecuatorianos. Los resultados muestran que existe un limbo jurídico en la elaboración o tipificación de los delitos cibernéticos como la incautación o usurpación de datos en las redes sociales, por los cuales deben sancionar para así proteger los derechos y dignidad de los ecuatorianos. Finalmente concluye que la carencia de conocimiento sobre el manejo de las TIC es una razón por la cual los ejecutores de justicia no han podido sancionar a los criminales.

Montañéz (2018), en su investigación “Análisis de los Delitos Cibernéticos en la actual legislación colombiana” presentado en la Universidad de Bogotá en Colombia expresa que Colombia crea la ley N° 1273 de 2019, la que refuerza el tratamiento jurídico digital de la información, causando vacíos que generan contradicciones

y errores al interpretar la ley. El objetivo principal es implantar si la ley 1273 en Colombia del 2009 es eficiente para penar las conductas cometidas por ciberdelitos. Los resultados señalan que esta ley presenta confusión al momento de ser interpretada causando errores en su ejecución. Finalmente concluye que hay cierto desinterés por conocer y dominar más el uso de esta ley por parte de los letrados, los cuales deberían ser los más interesados, ya que día a día se originan nuevos cambios y es necesario ir a la par para así poder afrontar nuevos retos. Así mismo definir mejor la ley en cuanto a ciberdelitos.

Chavarría (2019), en investigación denominada "La ciberdelincuencia y su regulación jurídica en Centroamérica con hincapié en Costa Rica, El Salvador y Nicaragua" presentada por la Universidad Nacional Autónoma de Nicaragua, manifiesta que a medida que se ha incrementado el uso de las plataformas virtuales tanto en el ambiente social y económico, se ha visto afectada tras la vulneración de su información personal; causando problemas económicos como la lesión a los derechos. El objetivo general es realizar una investigación sobre los delitos informáticos en los países centroamericanos. Los resultados señalan que hay una escasa información, seguimiento, recursos para identificar a los hackers. Se concluye finalmente que se debe crear nuevas normas en dónde la persona vulnerada pueda acudir a denunciar tales delitos, asimismo cooperar entre estados para hacer frente a la ciberdelincuencia.

En nuestra legislación a nivel nacional Cárdenas (2019), en su tesis denominada: "Delitos Informáticos y el rol de La División de Investigación de Delitos de Alta Tecnología PNP" manifiesta que se ha definido por medio de esta averiguación que, en los delitos informáticos, el papel de la DIVINDAT - PNP es positivo, habiéndose probado nuestras propias premisas. El objetivo general es establecer que todos aquellos delitos cibernéticos que más grande incidencia se denuncian a la DIVINDAT – PNP, es en relación a operaciones fraudulentas bancarias con trasgresión de accesos de Password secretos y confidenciales por medio de la "banca en línea" o "banca por internet" y clonaciones de esas tarjetas de créditos y tarjetas de débitos. Los resultados señalan que, respecto al impresionante desarrollo de las TIC's, abren mayores posibilidades de delincuencia, como son los delitos informáticos, constituyendo la red de internet como nueva vía de comunicación, el instrumento o herramienta tecnológica más utilizada en la comisión de estos delitos, en razón que los delincuentes piensan su simple ingreso, mínimo peligro y lo anónimo que se da. Se concluye en que la DIVINDAT – PNP, en la actualidad tiene déficit en sus trabajadores, empezando por el número de todo el personal especializado, no poseen las herramientas tecnológicas suficientes, que les permitan estar a la par de las Unidades que son semejantes de afuera del país y que estos mismos ponen en grave peligro el desempeño y eficacia de la tarea asignada.

Pereyra (2018), en su proyecto de investigación titulado: "Los Retos y oportunidades de la deferencia del Perú al Convenio de Budapest sobre el Cibercrimen", tiene como principal objetivo que los ciberdelitos y las posibilidades como se hacen dichos tipos de delitos informáticos se hallan en constante evolución a partir de la masificación del Internet a principios de la década de los 90, generando pérdidas económicas y perjuicios sociales cada vez más grandes gracias al uso de novedosas tecnologías y programa para la comisión del delito

a partir de cualquier y en cualquier instante. Los resultados señalan que para protegerse de los ciberdelitos, instituciones y organizaciones permanecen llevando a cabo inversiones en ciberseguridad, generando más pérdidas económicas reflejadas en menores ingresos y probables déficits proyectados, y no realizando frente al primordial problema, el cual abandonó de ser un único de un territorio, para ser un problema que debería ser combatido por todos los Estados por medio de la cooperación universal en materia jurídica, de conocimientos, vivencias e información importante para implantar responsabilidad penal a los relacionados. Se concluye dando a conocer que el Pacto de Budapest sobre la Ciberdelincuencia es un instrumento de enorme utilidad en temas de derecho penal sustantivo y procesal para todos los Estados Parte al buscar la una política penal común frente a los ciberdelitos, y el aumentar las habilidades y eficiencia en la averiguación, seguimiento y el debido proceso penal.

Quiroz (2019) en su disertación titulada "Ciberdelitos y la Justificante Protección Penal de la Privacidad en el Distrito Judicial de Lima, 2008-2012", "Universidad Nacional Federico Villarreal" Lima, Perú Gran Misión de Mediación Judicial Permite Ausencia y Desconocimiento Tecnologías de la Información en el Investigación y Persecución de Delitos Cibernéticos por Inviolabilidad de la Privacidad, empero son indiferentes para los fiscales y al costado de los policías mencionan estar en desacuerdo. Los resultados señalan que los jueces y fiscales permiten que coexistan infracciones de nuestras legislaciones actuales, los magistrados permanecen conforme con la decisión del tipo penal, en lo que los policías y los fiscales permanecen en desacuerdo. Se concluye dando a conocer que los jueces permanecen según la inadecuada decisión del mal, con el insuficiente cálculo del costo indemnizatorio, en lo que los policías y fiscales, son indiferentes y permanecen en desacuerdo.

En el nivel local Leon (2018) en su proyecto de investigación "Bloqueo Dinámico de IP en el Comercio Electrónico como Medida de Prevención de Cibercrimen en la Ley N° 30096", cuyo principal objetivo es detectar, a partir de los resultados obtenidos mediante el cálculo de los umbrales, y los ciberdelitos pueden ser advirtió porque es una medida de seguridad frente a la estabilidad, por lo que la muestra de investigación menciona que la iniciativa indicada es factible." Finalmente, se señala que existen diversas formas de eludir los consejos de ciberdelincuencia con el único fin de reducir significativamente la delincuencia, por lo que el bloqueo de IPs en todos los soportes informáticos redundará en la estabilidad informática, cuyo objetivo es poder prevenir los delitos informáticos.

Carrillo (2018) en su trabajo "Delitos informáticos o tecnológicos y su falla legislativa en los delitos de ataque a cualquier sistema informático" tiene como principal objetivo que broten novedosas y diferentes posibilidades delictivas, las que no se hallan especialmente regularizadas en la legislación penal, frente a este contexto es que se proclamó la Ley Particular de Delitos Informáticos en el año 2013. Como resultados se señaló que no se regula de forma determinada el delito que atenta en contra la integridad de sistemas informáticos, es por ello que es necesario que se modifique el artículo 4 de la presente ley, es por esto que se incorporaría los medios tecnológicos de comunicación e información, así como los medios comisivos de

este delito, fin de que se proteja los intereses de cada persona y de sus sistemas informáticos". como conclusión se sustenta que, por el progreso de las nuevas tecnologías, brotaron nuevas y novedosas posibilidades de delitos cibernéticos aquellos que en nuestro estado se hallan regulados a partir del año 2013, año desde el cual los cibercrímenes han evolucionado y se han adaptado a las situaciones actuales en que se está enfrentando como sociedad.

Delgado (2016), en su tesis titulada "La inseguridad al usar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú, 2015", tiene como principal objetivo que en el mundo actual pleno siglo 21 el que vivimos, cual nace novedosas técnicas cibernéticos las cuales muestran constantes y nuevos beneficios para el individuo humano, sin embargo, además implica desventajas pues han surgido novedosas posibilidades delictivas. Como resultado se dio que se necesita que en la legislación se prevea de dichos aspectos para que así ante los problemas desconocidos que se presentan, son capaces de luchar de manera razonable según el desarrollo de las nuevas tecnologías, lo que obliga a las autoridades a tomar precauciones ante dicho desarrollo. En conclusión, a veces es difícil saber de dónde vienen estos delitos y actividades delictivas, por lo que es necesaria una nueva clasificación de los avances tecnológicos.

En cuanto a la Justificación e importancia del estudio tenemos que como justificación teórica se menciona que según Correa (2018) aporta que: "Teniendo conocimiento que el Perú continúa afrontando ciberextorsiones desarrollados, sofisticados, especializados, de manera progresiva y proveniente de cualquier parte del mundo por grupos organizados y que tienden a evolucionar está siendo una realidad problemática que no solo afecta a determinadas personas sino también a nivel social o a nivel territorial peruano.

Es por ello que tenemos a la Ley Nº 30171 la cual modifica a la ley Nº 30096, con el objetivo de adecuarla al convenio de Budapest, para que en materia penal se homologuen normas de derecho penal de manera estandarizada internacionalmente para poder llegar a combatir los ciberdelitos en el Perú.

Como justificación social se pretende precisar cuáles son los factores que determinan que la ley 30096 de Delitos Informáticos tenga poca eficacia en su aplicación en el delito de fraude informático en el Perú, esto porque al determinar la baja eficiencia además de buscar vacíos legales podremos reforzar la ley a ayudar a la DIVINDAD combatir los fraudes cibernéticos que se dan día a día en nuestro país, lo cual contribuirá a disminuir el índice de este tipo de delitos en nuestra legislación.

Como justificación práctica nos damos cuenta que teniendo en claro que cada vez más se agrava la situación cuando, a pesar de haberse inspirado en las convenciones de delitos informáticos de Budapest, en nuestra legislación no se regula esto, asimismo como se instituye, debido a que el modo en que operan es perjudicar, es por eso que se sanciona esta conducta delictiva que se encuentra tipificada dentro de nuestra legislación penal.

Es por esto que se pretende encontrar estos vacíos legales y deficiencias ya que cabe recalcar que la ciberdelincuencia en nuestra legislación actual no se encuentra debidamente regulada del todo y sabiendo muy bien que la Ley 30096 no es rigurosa en funcionalidad a la vulneración de sistemas informáticos y bases de datos, no regulando los próximos bienes jurídicos, como por ejemplo: la estabilidad e intangibilidad del flujo de información en la red y estabilidad de las comunicaciones e información informática, delincuencia solamente salvaguarda la funcionalidad del sistema informático más no la información que está en este.

Como justificación metodológica Cervo (2017), afirma que es un a una acción enfocada en la resolución de las problemáticas existentes, ya que su objetivo se basa en encontrar respuestas a cuestiones por medio del trabajo de procesos científicos, y si bien es cierto que, a partir desde un punto de vista científico, la investigación es la formulación de un proceso metódico y sistemático que permitirá dar una respuesta a un problema y al mismo tiempo generar conocimientos diferentes e innovadores que conducirán a una posible solución a lo anterior al problema planteado.

Como justificación metodológica damos a conocer que es una investigación es básica descriptiva de enfoque cualitativo con un diseño no experimental, en el cual mi población serán los jueces, fiscales y abogados especialistas en el derecho penal del distrito de Chiclayo, con respecto a las técnicas e instrumentos utilizadas se usará la entrevista.

De acuerdo con lo descrito se plantea como problema general de la investigación:

- ¿Es posible la aplicación de la ley 30096 para prevenir los delitos de fraude informático en el Perú, 2022?

A su vez, se plantean los siguientes problemas específicos:

- ¿Existen vacíos legales y omisiones que posee la ley 30096 de delitos informáticos en función al delito de fraude cibernético?
- ¿La ley 30096 cumple adecuadamente con su rol preventivo y sancionador en relación al delito de fraude informático?
- ¿Se deberían implementar más unidades fiscales especializadas en ciberdelincuencia en todas las regiones del país para garantizar la eficacia de la ley 30096?

Como objetivo general se planteo:

- Analizar la aplicación de la ley 30096 de delitos informáticos para prevenir los delitos de fraude informático en el Perú, 2022.

Como objetivos específicos se tomo en cuenta

- Identificar los vacíos legales y omisiones que posee la ley 30096 de delitos informáticos

en función al delito de fraude cibernético.

- Definir si la ley 30096 cumple adecuadamente con su rol preventivo y sancionador en relación al delito de fraude informático.
- Determinar si se deberían implementar más unidades fiscales especializadas en ciberdelincuencia en todas las regiones del país para garantizar la eficacia de la ley 30096.

Dentro de las teorías relacionadas al tema se tomó en cuenta determinar cuál es la definición del sistema informático dentro de nuestra legislación peruana a lo cual Alkhalil (2021), nos da a conocer que para hacer una correcta definición de lo que es un sistema cibernético es preciso mencionar que es algo estrictamente complicado ya que su significado se extiende y se propaga no solo del derecho en su totalidad o generalidad, también a la parte del derecho penal, es así que podemos entender que un sistema informático es aquel conjunto o vínculo entre dispositivos electrónicos, partes que lo componen tanto inmateriales como materiales los cuales ayudan a permitir poder recopilar, establecer, poder procesar la información y la data, mediante la aplicación de software como también del sistema operativo el cual está orientado para aportar y apoyar las actividades humanas.

Es por ello que no se percibe al software o hardware únicamente como parte del sistema informático, sino también al propio personal, técnicos encargados de poder dar mantenimiento a los sistemas como también a los propios usuarios que vendríamos a ser todos nosotros que hoy en día consumimos canales de información o sistemas informáticos.

Asimismo, las concepciones del sistema informático según los expertos en nuestra legislación peruana prescriben que la definición más correcta y acertada sería la que podemos encontrar en el artículo 1, precisamente en la novena disposición de la Ley de Delitos Informáticos, la misma que lo defino como todo conjunto de dispositivos electrónicos que están conectados entre sí vinculados, cuya función principal es la de ejecutar programas informáticos.

Akamai. (2020), sustenta que si bien es cierto dentro de nuestra legislación peruana debe darse a entender que dentro de un sistema informático lo que todos conocemos como la parte física de este sistema son sus componentes corpóreos como también su hardware , en la parte de los componentes corpóreos nos referimos a los dispositivos electrónicos que tienen que cumplir ciertos requisitos y características como la unidad principal de procesado , los puertos de salida y de entrada y accesorios que complementan el sistema para dar un uso adecuado siempre y cuando se ejecuten determinados programas ya que se trata del software.

En cuanto a la Naturaleza físico – patrimonial del sistema informático Alcívar (2018). Explicó que, en nuestro sistema informático de la legislación peruana, dentro de su naturaleza material, podemos saber que estamos frente a un tipo de bien mueble, gracias a la utilidad en la sistematización del desarrollo, y tiene un carácter patrimonial y económico, y así conforma los principales pilares del sistema empresarial, consolidando su patrimonio como persona jurídica y como persona natural.

Por tanto, como ya sabemos y mencionamos brevemente, los bienes muebles estaban regulados antes de la publicación de la Ley N° 30096 en el Código de Delitos Informáticos, y ya son un fin y un amparo en nuestra legislación peruana vigente, desde que fueron descubiertos. sección de delitos contra la propiedad.

Es así que, si bien es cierto nuestra presente Ley de Delitos Informáticos, Ley 30096 prescribe concretamente en su artículo 4 que el bien jurídico que se protege en este tipo de delitos es la integridad como también la prestación de servicios de sistemas cibernéticos, además también nos aclara que en este tipo de delitos claramente como ya ha sido mencionado se atenta en contra de nuestro patrimonio.

De acuerdo a las Deficiencias legislativas en nuestro ordenamiento jurídico Alvarado (2017), nos da a conocer que dentro de nuestro ordenamiento jurídico podemos presenciar distintas deficiencias legislativas tipificadas en este tipo de delitos cometidos, según lo que expresa tanto la legislación comparada como la doctrina internacional se puede dar a conocer que nuestros legisladores peruanos no se dedicaron a regular de manera correcta aquellas contramedidas que constituyan un adecuado control, esto con el único fin de poder identificar cual es verdaderamente la conducta que vendría a ser penalmente notable.

En cuanto a La ciberdelincuencia y su evolución tecnológica tenemos que dentro del Desarrollo histórico de los delitos informáticos o de la tecnología. Blossier (2018) afirma que: “La revolución digital que comenzó en la segunda mitad del siglo XX es comparable solo a la revolución industrial del siglo XIX por su impacto socioeconómico. De hecho, la tecnología posterior a la Segunda Guerra Mundial permitió hablar de una "revolución tecnológica" en la que la tecnología de la información, especialmente los microchips, fue un componente clave que facilitó la construcción de todos los artefactos comunes de la vida. Día del Trabajo.”

El siglo XX vio cambios tecnológicos tan drásticos como los provocados por la Revolución Industrial en el siglo XIX. Los sistemas informáticos que impulsaron la revolución digital, donde las computadoras salen de la oficina y entran en el hogar, aprendiendo sobre todos los llamados y actividades de la humanidad.

De acuerdo con Díaz (2018), nos da a conocer que la primera revista relacionada con el tema de los ciberdelitos tuvo como nombre Crimen Computarizado y este tuvo su origen en las revistas científicas, precisamente en los años 60s y unos años después en 1983 cuando se dio una reunión de la Organización para la cooperación y el desarrollo económico o conocido por sus siglas también como OECD, en esta reunión se admite por primera vez el término y definición del crimen computarizado.

Espinoza (2017) explica que si bien es cierto aún existe aquella dificultad para poder identificar debidamente cuáles son aquellas conductas que se suelen usar los ciberdelincuentes para cometer delitos informáticos

como el fraude informático, es por esto que se afirma que actualmente no existe una debida definición correcta de los delitos cibernéticos.

Figueroa (2018) afirma que “en general, el uso de computadoras en el delito no cambia el hecho de que ocurrió el delito, es decir, no cambia la categoría del delito cometido”.

Hanko (2018) nos a conocer que: “El ciberdelito engloba una gama de conductas que son difíciles de minimizar o categorizar en una sola definición porque no existe el delito informático, sino solo una forma de ejecución”.

Forbes (2021) define “el término delito informático como cualquier posible uso de un ordenador. Los delitos cometidos mediante delito informático son aquellos que afectan a bienes jurídicos protegidos, por lo que no existe una definición única de lo que es delito informático, pero en general se puede definir como un delito cometido con la ayuda de un sistema automatizado de procesamiento de datos.

Hernández (2018) considera a los delitos informáticos como aquella versión actualizada de los delitos comunes y corrientes que la mayoría conocemos y esta afirmación es parcialmente cierta debido a que una de las principales funciones de la tecnología actual es ser como un medio de comunicación a nivel global, pero por otra parte junto con la aparición de la tecnología aparecieron nuevos bienes jurídicos tutelados y aquellas conductas que definen a la informática.

De esta forma según Guerrero, (2018) podemos expresar que los delitos informáticos hasta el día de hoy se usaron de una manera común, pero actualmente cada día estamos siendo testigos que se está usando los sistemas informáticos para facilitar los delitos como en este caso el fraude informático usando las redes sociales para cometer el delito causado por los ciberdelincuentes.

Seguidamente se puede considerar que la denominación correcta de los delitos cibernéticos responde a aquella conducta la cual afecta directamente a un bien jurídico en específico, el cual actualmente no se encuentra resguardado dentro de nuestra legislación jurídica peruana, como lo es la ciberseguridad de la base de datos que son almacenados o que se trasmiten cibernéticamente.

Podemos señalar que el cibercrimen o delito informático según Banco Interamericano de Desarrollo y Organización de los Estados Americanos, (2020) es un delito de soberanía propia, por lo que se considera que la definición de delito informático es una definición precisa de ciberdelito o ciberdelincuencia, que debería vincularse con la nueva ley, que vale la pena, custodia y no incluye el simple uso de tecnología o tecnología de la información como un medio para menoscabar los diversos derechos legales ya protegidos por el Código.

Así, Herrera (2017) menciona que, con el auge de la tecnología en el siglo XXI, el uso de los sistemas informáticos y la tecnología actual se convierte en una importante herramienta de los ciberdelincuentes para afectar los bienes jurídicos de las personas protegidas. De acuerdo con nuestra legislación penal peruana y lo establecido por nuestros legisladores en la Ley nro. 30096, se están victimizando de forma anónima en lo que denominan delitos informáticos o popularmente conocidos como ciberdelincuencia o cibercrimen.

Existes diversas Implicaciones de los intereses legales protegidos en el fraude informático a lo cual Hiplán (2019) menciona que con el único propósito de identificar si usar los sistemas informáticos vulneran los intereses jurídicos, aquellos que entran dentro de las categorías del bien jurídico tutelado, es así que de esta forma podemos determinar cuáles son aquellas conductas que a través de la tecnología actual se atenta en contra de los bienes jurídicos tutelados y que además se lesiona aquel interés que no es objeto de la tutela.

Es de esta forma que se constata que la utilización de la informática y las novedosas tecnologías vulneran un nuevo interés que merece y requiere defensa, en nuestro estado hasta principios del siglo 21 no se tuvo una idónea tipificación penal ni cualquier tipo de defensa que respalde, es por esto que, en la ley de Colombia, Ley N.° 1273, del 2009 prescribe existente ese resguardo de toda la data o información de datos, lo que pasaría a ser el bien jurídico que se tutela.

Ugarte (2020) nos da a conocer que: "Se intentaría un bien jurídico supraindividual vinculado a la estabilidad e intangibilidad del tráfico de información en la red y plantear y asegurar la independiente colaboración de los individuos denominados además usuarios en la red".

León (2018) ha señalado que la nueva propiedad jurídica penal protegida puede ser información como un costo económico para la organización y quiere mencionar en su experiencia como abogado que esta nueva propiedad jurídica penal protegida referencia refleja a quienes reclaman protección y quién necesita protección dice.

Como ya se mencionó anteriormente, si no se almacenan, procesan, sistematizan, se debe tener en cuenta que la información con contenido inherente, datos de relaciones confidenciales, secretos comerciales, secretos de estado o medios contables, costos financieros de la organización no es suficiente o se distribuye en la organización o llamada la red.

Es por ello que, según la Defensoría del Pueblo, (2019) afirma que cuando la información o los datos en términos informáticos representan o tienen un coste económico, en realidad nos referimos al legado o estabilidad de las comunicaciones informáticas o telemáticas.

Por otro lado, López (2019) argumenta que, si bien esto es cierto, al hablar de la protección de un bien jurídico protegido, debemos referirnos a la posibilidad de determinar si cumple con los requisitos de de su protección para determinar que está fuera de nuestra vida actual.

También es muy importante mencionar que la adecuada protección de los datos informáticos y su seguridad actualmente no está debidamente regulada por la Ley de Delitos Informáticos 30096, que aún no regula sus métodos.

Por lo tanto, Mayer (2017) afirmó que "La información, simplemente, o la información fuera de un sistema informático no es un objeto específico que se deposita a través de un sistema informático, pero la información

que se almacena o procesa fuera de un sistema informático es una amenaza para privacidad, el delito de violación del secreto oficial y violación del secreto de las comunicaciones tiene capacidad de defensa.

Mesa (2017) afirma: “La estabilidad de la comunicación e información informática o la estabilidad de la información o datos transmitidos a través de una red es el único requisito que satisface la necesidad de defensa y sanción para que tengamos el potencial de propagar delitos informáticos bajo la ley N° 30096 Sanciones en virtud de la Ley de Delitos Informáticos.

Moncada (2020) nos expresa que la Ley de Delitos Informáticos, Ley 30096 aun cuenta con una deficiencia al instante de decidir cuál es el bien jurídico salvaguardado en esta clase de delitos, es de esta forma que esta realidad puede llegar a dañar evaluación penal y poder decidir cuál es el nivel de acusación a causa de que el ministerio público debido a que poseemos que considerar que la ley de delitos informáticos tiene como objetivo proteger la apariencia corpóreo del bien jurídico salvaguardado, en esta situación los sistemas informáticos, así mismo cabe determinar que de acuerdo con la disposición N°9 de la Ley de Delitos informáticos, Ley 30096 prescribe que el sistema informático está construido por los computadoras y sus interconexiones”.

Así como el tipo de delito tiene por objeto proteger objetos físicos más que bienes jurídicos, existe una diferencia cualitativa entre los dos tipos de bienes: uno es el objeto físico en sí, y el otro es la naturaleza general de todos los objetos físicos útiles para el desarrollo de sociedades.

Mori (2019) afirma: “La distinción puede tener un impacto significativo en la regulación del derecho penal, ya que proteger los activos físicos, como los sistemas informáticos, no protege otros activos, como los sistemas de transporte, los sistemas de telecomunicaciones y todas las advertencias antes mencionadas son un comienzo.

La regla de la constitución es declarar permitido lo que no está prohibido, lo que nos hace entender que son necesarias infinitas reglas como infinitos bienes jurídicos a defender.

Por otro lado en cuanto a la ciberdelincuencia y su interacción con la estabilidad e intangibilidad del tráfico de información en la red Paredes (2019) afirmó: “Dada la dinámica económica, jurídica, social y cultural en constante cambio en la que vivimos, este debe servir como un estudio de la intervención estatal en la prevención y sanción del delito, analizando sus causas y consecuencias; como delito va en aumento cada día, Este comportamiento, que es nocivo y afecta a países y sociedades, muchas veces está determinado por diversos componentes que están implícitos en el entorno en el que las personas nacen y existen como seres vivos. - Psicosocial.

Pero hoy vemos cómo ha sido reemplazada por la hiperconexión de los sistemas informáticos, asociada a una serie de avances y cambios tecnológicos en diversos modos de interacción y, en consecuencia, como resultado de fenómenos sociales antes localizados solo en las relaciones sociales físicas. y tecnología, interés general.

En consecuencia, Pardo (2018) sustenta que gracias al avance de la tecnología y el avance informático han surgido las Tecnologías de la Información y la Comunicación o también llamadas TIC, aquellas que abrieron muchos caminos para que existan múltiples y diversos tipos de conductas penalmente sancionadas, usando estas nuevas tecnologías como herramientas principales al momento de cometer estos ciberdelitos como el fraude informático que atenta contra el patrimonio.

Ruiz (2020) nos pregunta con severidad: "Transición de Homo sapiens a Digitalis, enfatizando: "En el ciberespacio, todos pueden ser emisor y receptor en un entorno con diferenciación cualitativa, donde todos los individuos se comunican con todos menos con los internautas, no principalmente con su nombre, condición social o ubicación geográfica, sino desde el centro de interés, por así decirlo, "en un mundo virtual aislado de la comunicación, que requiere la criminología". Aproveche el día para desarrollar un nuevo perfil criminal que se ajuste a las características únicas de este nuevo crimen que se está apoderando del planeta".

En América Latina, el potencial de grandes ganancias para los ciberdelincuentes es alto, gracias a las principales economías de la región, ubicadas en el término medio más relevante del mundo y al mismo tiempo, el peligro percibido más bajo, fue procesado y condenado por delitos informáticos y delincuencia activa en los Estados Unidos y la Unión Europea.

Romero (2017) menciona: "Por un lado, la cara positiva de las TIC incluye útiles herramientas interconectadas para el mejoramiento del planeta, destacando la IA o inteligencia artificial, que antes era característica del cerebro humano, pero basada en criterios negativos, constituye varios riesgos potenciales para las empresas y los adultos, principalmente niños, niñas y jóvenes, que pueden convertirse en víctimas de la demencia digital o de los sistemas informáticos, muchas veces porque son incapaces y suficientemente capaces de ver las verdaderas intenciones de aquellos con quienes todavía casi cooperan y romper los sistemas de seguridad".

De esta forma, analizando este problema, podremos entender y entender la verdadera escala y desarrollo de los medios informáticos o cibernética, Internet y los ordenadores personales con los que interactuamos a diario, quizás sin darnos cuenta de las consecuencias.

En este sentido, como acertadamente apunta Pérez, las TIC "le dan a la gente de nuestra época la oportunidad de comunicarse personalmente y en tiempo real sin parámetros espaciales ya que el Internet es la gran revolución de nuestro tiempo, cuyas consecuencias se dejan sentir también en la esfera de la libertad, han creado nuevas formas de ejercer los derechos y pueden ayudar a fortalecer las estructuras participativas de las sociedades democráticas.

En el Perú se cuenta con la Separación de Averiguación de Delitos de Alta Tecnología de la DIRINCRI – PNP, empero no obstante su trabajo, a pesar de sus esfuerzos, es insuficiente por la carencia de apoyo logístico, presupuesto y posicionamiento en la sociedad, unificado a ello la cifra negra que todavía pesa en esta gama de delitos, que bastante a pesar existente una Ley de delitos informáticos, esta no instituye en qué momento estamos ante un delito informático o una vez que estamos frente a un delito tipificado en el Código Penal.

Sin embargo, se debe reconocer que el desarrollo de las tecnologías de la información es una de las características más importantes y llamativas de los últimos milenios, y para ello, la implementación incluye diversas modalidades que son importantes para combatir los excesos ya evaluados.

Los avances en las tecnologías de la información y la comunicación han permitido las comunicaciones electrónicas a larga distancia, cambiando la forma en que nos comunicamos entre nosotros, haciéndolas accesibles a más y más personas y cerrando la brecha digital en los sistemas que aún crean barreras para el desarrollo. Si bien la implementación de estas medidas trae importantes beneficios, también se acompañan de incidentes delictivos por su uso inapropiado, por parámetros no autorizados o no autorizados en la red.

Como acertadamente subraya García (2018): "Reflexionar sobre el horizonte de sentido entre la modernidad y la posmodernidad es reconocer una transición compleja que es también una época histórica sin luz, al menos de una manera que nos advierte sobre dónde se encuentra ese viraje o tendencia histórica se acertado.

Por lo tanto, la posmodernidad se ha convertido en un criterio bastante amplio para la experimentación relacionada con corrientes culturales, artísticas y filosóficas que aparecieron recién a fines del siglo pasado.

En general, se puede decir que la posmodernidad está asociada con el culto a la personalidad, el desinterés por la paz común y el rechazo al racionalismo.

El desplazamiento posmoderno, a enormes aspectos dice que la modernidad fracasó al pretender renovar las maneras de pensamiento y expresión, es por esto que se asocia al desencanto y la apatía debido a que parte de lo entiende como un fracaso de la sociedad".

Sánchez, (2020) menciona que: "Es individuo a enorme disputa, en el extremo que hay quien ha sugerido que su uso desmesurado lo ha vuelto en exceso frágil y postmoderno que se refiere a algo nuevo y distinto que ha sucedido en los últimos tiempos y que por el momento no podría ser explicado en términos de modernidad".

Por tanto, más que conceptualizar el entorno actual, quizás la clave esté en determinar si las reformas penales actuales o futuras son una continuación del pasado o, por el contrario, estamos asistiendo a verdaderos quiebres que interrumpen el pasado y siguen creando algo nuevo, cosas diferentes, por lo tanto, necesitamos adoptar un enfoque analítico y un plan diferente para la modernización criminal.

El discurso de la justicia penal de la modernidad, en diversas etapas de su desarrollo interno y externo, ha considerado fundamentalmente que la conducta delictiva es un comportamiento anormal e indeseable, pero el inevitable discurso de fe y creencia que a través del discurso de la justicia penal es debidamente sustentado o adecuado, con habilidades de participación, las personas tienen la capacidad de cambiar, desviar o inhibir su comportamiento delictivo.

Es por ello que para entender la expansión del crimen es necesario examinar lo que apunta Girón (2019), su interpretación de la expansión del crimen como una nueva insignificancia del espacio, como una transición a la modernidad fácil disfrazada de borrado del tiempo.

En primer lugar, hemos desarrollado medios que brindan una inmediatez casi global a quienes los manejan, así como invisibilidad para quienes no tienen acceso a esos medios.

En segundo lugar, implica una penalización del costo regional en sentido estricto, cabe señalar que el costo del espacio es supersticioso, y en el caso de George Simmel, el espacio vale dinero, y hoy en día se puede compensar con una gran cantidad de kilómetros por hora.

Llinares (2018) confirma que el canon del espacio virtual se suele utilizar como sinónimo de ciberespacio frente al espacio real dominante, y de esta forma la simultaneidad, la unicidad del momento puede dar la impresión del espacio es una falta de lugar, quizás por la falta de asimilación de la iniciativa espacial desde la distancia.

También es importante señalar que el ciberespacio es real en el sentido existente, pero es un espacio nuevo, invisible a nuestros propios sentidos directos, en el que las coordenadas de espacio y tiempo han adquirido un significado diferente y redefinen su alcance y parámetros.

La volatilidad del web, traducidas en la evolución de las redes inalámbricas y del propio hardware móvil, las cámaras digitales y las videograbadoras, es cada más accesible para los cibernautas de las monumentales mayorías, así como de los sistemas de defensas bancarios y financieros, lo que ha realizado una totalmente nueva faceta de cibercriminal que debería igualar inmediatamente para hacerle ante la mutación del delito.

Sequeiros, (2017) estima que se puede nombrar a un delito informático como ese acto o conducta que perjudica a un bien jurídico en específico debido a que en la actualidad este delito como tal no está debidamente salvaguardado por el código penal sino por una ley particular.

Es de esta forma que este delito viola la estabilidad y la intangibilidad de los datos almacenados debido a que dichos datos no tienen la posibilidad de ser ni transmitidos ni tratados de forma informática, en esta situación se estaría hablando que el delito informático una vez que es considerado como un delito autosuficiente puesto que consecuentemente la utilización de las pcs y de la tecnología constituye a que este delito perjudique a bienes jurídicos tutelados denominándose como delito informático.

Es así que a día de hoy pleno siglo 21 donde el índice de delitos informáticos ha aumentado considerablemente a diferencia de años anteriores, es por ello que tenemos que considerar y poder investigar cual es el comportamiento de los ciberdelincuentes actuales para poder descubrir su modus operandi y teniendo en consideración que todo esto lo podemos identificar a través de las personas vulneradas a las cuales ya han sido afectadas y fue afectado su bien mueble, es por ello que la presente ley 30096, Ley de Delitos Cibernéticos busca salvaguardar el bien jurídico tutelado que es afectado constantemente por este tipo de delitos informáticos.

Igualmente, la doctrina peruana, esta nos da a conocer respecto a saber cuál es la verdadera naturaleza de los sistemas informáticos, a analizando las diferentes etapas del comportamiento criminal dentro de la red, ya que esto ayudaría considerablemente a la DIVINDAT a capturar de manera más rápida y eficiente a estos ciberdelincuentes, de las mismas formas que se protege el bien jurídico tutelado por las leyes peruanas como es el caso de la ley 30096.

De igual manera siempre se menciona que el tema de los delitos cibernéticos es un tema que no solo afecta a nuestra legislación peruana, ya que esta afecta de manera global en cualquier parte del mundo, a esto se le denomina y es conocido como Crime Computer o crimen computarizado y fue mencionado por primera vez en la década de los 60s en donde empezaba a nacer esta modalidad de delitos.

II. MATERIALES Y MÉTODO

Para determinar el tipo y diseño de la investigación y teniendo en cuenta el propósito del tema de investigación, se realizará una investigación básica, que según Larigée (2019) expresa que la investigación básica es un estudio teórico o fundamental para desarrollar una nueva teoría o para modificar una existente, teniendo en cuenta el propósito, para poder señalar claramente que con este tipo de investigación, su objetivo es aumentar el conocimiento científico mediante la creación de nuevas teorías sin pruebas reales, con métodos cualitativos, por otro lado en la presente investigación el diseño utilizado fue no experimental, ya que en realidad se inspiró en la observación de fenómenos que ocurren en el medio natural y su análisis.

En cuanto al escenario de estudio en el presente trabajo de investigación se desarrolló el escenario en el Módulo Básico de Justicia del Juzgado Penal José Leonardo Ortiz y la Fiscalía de la Persona Jurídica Penal de la Segunda Provincia José Leonardo Ortiz, como resultado de las observaciones, toma de datos y entrevistas, se obtiene toda la información desde cada punto de vista relevante para el fenómeno objeto de estudio.

De acuerdo a la Categorización de sujetos se realizó un estudio de las diferentes opiniones y estándares de diferentes autores deja claro que ayudará a dar una visión certera de la investigación en curso, como el análisis de la Ley de Delitos Informáticos 30096 en su aplicación al delito de fraude informático en el Perú, 2022"

Por tanto, para los sujetos involucrados sujetos de investigación o informantes de este estudio, se escogieron las personas idóneas José Leonardo Ortiz, representante del Departamento de Estado, juez penal del módulo básico de justicia en el juzgado penal de José Leonardo Ortiz. como experto legal debido a su comprensión de los temas generales y específicos identificados en este trabajo de investigación.

Tabla 1

Nota: Datos de los sujetos participantes

N° de trabajadores públicos	**N°**
1.- Juez	15
2.- Fiscal	15
3.- Abogados	20
TOTAL DE LA MUESTRA	**50**

En cuanto a la Categorías, subcategorías y matriz de categorización, cabe señalar que está relacionada con el tema de investigación, la categorización mediante la agrupación de temas utilizando hipótesis o unidades temáticas relacionadas con diferentes temas y datos hace que este trabajo de investigación sea lógicamente significativo, y estas cosas están relacionadas entre sí, con anexos relacionados. y con suficiente bibliografía y sustento teórico.

Tabla 2

Categorización

Categorías A	Categorías B
Ley 30096 de delitos informáticos	Delito de fraude informático
Deficiencias legislativas de la ley 30096	Conducta ilícita del ciberdelincuente
Reglamentación de la ley 30096	Elementos del delito de fraude informático

Tabla 3 *Categorización, Subcategorías Ítems*

OBJETIVOS	CATEGORIZACIÓN	SUBCATEGORÍA	ITEMS (PREGUNTAS)
OBJETIVO GENERAL Analizar la aplicación de la ley 30096 de delitos informáticos para prevenir los delitos de fraude informático en el Perú, 2022.	Ley 30096 de delitos informáticos	Deficiencias legislativas de la ley	1.Consecuencias jurídicas de alterar el ingreso de datos de manera ilegal. 2. Deficiencias o vacíos legales en la ley 30096 ley de delitos informáticos. 3.Implementarse más unidades fiscales especializadas en ciberdelincuencia. 4. Sistemas o software con propósitos fraudulentos. 5. Conductas ilícitas que afectan los sistemas y datos informáticos informático. 6. Finalidad garantizadora de la lucha eficaz contra la ciberdelincuencia. 7. Efectividad de la Ley 30096 al momento de sancionar a los ciberdelincuente. 8. Pena privativa de libertad impuesta a los ciberdelincuentes que cometen delitos de fraude informático. 9. Tipicidad subjetiva en el delito de fraude informático. 10. Criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático.

Por consiguiente, dentro de las técnicas e instrumentos de recolección de datos para escribir este informe de investigación, todos los datos deben recopilarse utilizando instrumentos y técnicas y métodos de investigación adecuados y compatibles para contribuir al objeto de investigación.

Dentro de las técnicas de recolección de datos tenemos a la entrevista que: Según Hernández (2014), la técnica de recolección de datos es significativa y relevante porque refleja las opiniones de expertos que responden a varias preguntas de los entrevistadores, en el presente caso nos ayudó a poder llegar a determinar cuáles fueron las opiniones de los expertos en la materia, las mismas que nos ayudaron a poder llegar a poder concluir de manera acertada el presente trabajo de investigación.

En cuanto a los instrumentos de recolección de datos tenemos que las herramientas de recolección de datos utilizadas en el desarrollo de este estudio son la guía de entrevista, esta es la herramienta idónea de recolección de datos con 10 preguntas abiertas diseñadas en base tanto al objetivo general como a los específicos con parámetros para sus respuestas.

Por consiguiente, para el procedimiento de recolección de datos se hizo aplicación de la guía de entrevista la cual nos fue de mucha utilidad para obtener información detallada sobre la ley 30096 y como poder aplicarla en los delitos de fraude informático en nuestra legislación actual.

Para ello se siguió los siguientes pasos, primero se definió el propósito de la entrevista, aquí se detalló cual sería el objetivo de la entrevista y nos aseguramos de comprender de forma legible cual sería la información requerida a obtener de los entrevistados.

Luego se identificó a los expertos, para ello se seleccionó a expertos en materia penal los cuales poseen conocimientos específicos sobre los delitos informáticos, despues se contactó a los expertos y se solicito su participación explicando claramente el propósito de la entrevista, su duración estimada y cómo se utilizará la información recopilada.

Para la obtención del consentimiento informado antes de comenzar la entrevista, nos aseguramos de obtener el consentimiento informado de los participantes, explicándoles la naturaleza de la investigación, la confidencialidad de la información y su derecho a retirarse en cualquier momento.

Se preparo un cuestionario estructurado y se diseñó un cuestionario que contiene preguntas específicas y estructuradas sobre el tema de materia penal, esto ayudo a mantener la entrevista enfocada en los aspectos relevantes.

En cuanto a realizar la entrevista esto condujo la entrevista de manera profesional y ética, se comienzo con preguntas generales antes de pasar a detalles más específicos, luego de ello se fomentó la discusión y permitió que los expertos expresen sus opiniones.

Después se tuvo que registrar la Información y se tomó notas detalladas durante la entrevista para capturar la información de manera más precisa, para ello se hizo un análisis de datos después de la entrevista, se analizó y organizo la información recopilada, con ello se identificó patrones, tendencias o conceptos clave

que surgieron de las respuestas de los expertos.

Se hizo un Procedimientos de análisis de datos para el trabajo de campo, en el desarrollo de las 8 entrevistas realizadas, se coordinaron con los encuestados en sus respectivas oficinas de empleo y les explicaron los motivos de la entrevista y se detalló cual era la necesidad de aportar su experiencia en el ámbito del derecho penal en el presente proyecto de investigación titulado: "Análisis de la ley 30096 en su aplicación a los delitos de fraude informático en el Perú, 2022, los entrevistados participantes accedieron y voluntariamente se permitieron ser entrevistados en fechas distintas que fueron las mismas que las obtenidas en sus respectivas oficinas.

Los pasos en el proceso de análisis de datos son los Analizar la realidad para determinar si la pregunta de investigación es relevante, luego para la investigación, identificar continuamente la realidad del problema y formular preguntas y objetivos específicos, se ha fijado un lugar para el desarrollo de la investigación, se seleccionaron y realizaron métodos de análisis documental, entrevistas y sus herramientas relacionadas con el estudio de investigación, la información recopilada se analiza y los resultados se estructuran.

Los resultados obtenidos se explican y discuten, con la ayuda de los cuales se pueden determinar las consideraciones finales, en cuanto a los criterios éticos el proyecto se basa en los siguientes principios éticos fundamentales:

Autonomía: Los investigadores deben expresar voluntariamente y de manera informada su voluntad de cooperar con las empresas u organizaciones que opten por realizar investigaciones y aprobar el uso de la información para fines específicos de investigación.

El bien común: El fin último de la investigación debe ser hacer recomendaciones que ayuden a mejorar la organización y la sociedad misma.

Difusión del conocimiento: La investigación debe ser comunicada a los involucrados en la investigación.

La justicia: Los investigadores y las personas involucradas en la investigación obtendrán lo que les corresponde.

Revisión independiente: La investigación en cualquier etapa debe someterse a una revisión independiente para garantizar su calidad ya sea un proceso de aprobación por parte del asesor de tesis o de la facultad, si es necesario, y una revisión del jurado de la tesis en la presentación final.

Dentro de los criterios de rigor científico existen algunos criterios para evaluar el rigor y la calidad científica de la investigación cualitativa, y existe un consenso parcial sobre estos criterios.

Veracidad: Respetar los hechos y circunstancias creados en el contexto espacial de este estudio, teniendo en cuenta las estimaciones de los valores de los datos obtenidos aplicando la información obtenida con los instrumentos de investigación.

Confiabilidad: Se refiere al grado de consistencia o certeza de los resultados analíticos y de los resultados luego del procesamiento de la información obtenida por el instrumento.

Confirmabilidad: En la medida en que no se rechace la participación en la investigación y en todo caso extienda la certeza plena del proceso mencionado en este estudio, y los resultados se obtengan a partir de información sobre los instrumentos utilizados, donde los datos aún están sesgados, es menos probable que respondan a cualquier forma de manipulación personal.

III. RESULTADOS Y DISCUSION

En el presente capitulo se podrán dar a conocer los resultados en tablas y figuras obtenidos a partir de todas las fuentes de información recopilada, en las cuales se incluyó una entrevista y el debido análisis para la discusión de los resultados. El debido análisis de los datos se pudo realizar con el apoyo de herramienta que funciona como hoja de cálculos perteneciente a Microsoft 365 que tiene por nombre Excel 2019, con esta herramienta informática se pudo realizar las tablas y figuras organizadas con el único fin de poder facilitar la debida interpretación de estas mismas mostradas a continuación.

3.1. Resultados

Tabla 4

Consecuencias jurídicas de alterar el ingreso de datos de manera ilegal.

Códigos	Frecuencia
Pena privativa de la libertad	8
Afectación del bien jurídico tutelado	2
Multa correspondiente	2
Afectación a la integridad de datos informáticos	2

Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales

Análisis e Interpretación: Dentro de las consecuencias jurídicas que existen luego de alterar de manera ilegal el ingreso de datos en sistemas informáticos los ocho entrevistados estuvieron de acuerdo al manifestar que los ciberdelincuentes que cometen este acto ilícito deben ser reprimidos con pena privativa de la libertad, solo dos consideraron como consecuencia valida la afectación del bien jurídico tutelado como afectación del presente acto ilícito, dos entrevistados manifestaron que además de una respectiva pena privativa de la libertad también se considera una multa correspondiente, dos entrevistados manifestaron que una de las consecuencias jurídicas al alterar el ingreso de datos de manera ilegal es la afectación a la integridad de datos informáticos.

Para ser más concretos veamos a continuación las respuestas brindadas por cada uno de los abogados y fiscales entrevistados:

A1: Bueno, definitivamente considero que sí, ya que debido a que nuestro ordenamiento jurídico tiene por finalidad la protección de los bienes jurídicos como son, los bienes patrimoniales y por su parte el estado condena aquellas personas que, ingresan de manera ilegal ósea me refiero a la manipulación de datos en un sistema netamente informático.

A2: Sí, este tipo de delitos en si se rigen por la ley especial y la ley 3096 de delitos informáticos y en ella se determina sanciones penales según el tipo de delito cometido y los actos ilícitos que realice el ciberdelincuente con la ayuda de internet.

A3: Pues claro que sí, es por ello que existe la ley 30096 de delitos informáticos, la cual sanciona severamente este tipo de conductas de los delitos informáticos en todas sus modalidades ya que el objetivo de los legisladores al momento de crear la presente ley fue poder prevenir y sanciona todo tipo de conductas ilícitas que de manera ilegal los sistemas o datos informáticos en nuestra legislación.

A4: Mire si bien es cierto hay una ley no? La ley 30096 que mencionaste, si mi mente no me falla, espérame lo busco mejor, aquí mira, en el artículo 8 prescribe que si cualquier persona altera ilegalmente datos para su beneficio propio mediante el uso de sistemas informáticos será castigado con una pena de entre los cinco a diez años según la gravedad del acto delictivo además que también existe multa correspondiente de más de setenta días calendario para este tipo de delitos especiales.

F1: Si, efectivamente estas modalidades están estipuladas en la ley especial y establecen cual es la sanción penal que corresponde por el tipo o cada hecho que se realice en la red informática.

F2: Si hay consecuencias jurídicas de orden penal en el marco de la ley 30096 reformada y por ello quien lo hace comete el delito de atentado a la integridad de datos informáticos, además que es objeto de sanción correspondiente y multa por atentar contra un bien jurídico tutelado.

F3: En efecto, dicha conducta se encuentra regulada en el artículo 3 de la ley 30096 que reprime las conductas ilícitas cometidas contra los sistemas informáticos que a la letra reporta lo siguiente: Atentado a la integridad de datos informáticos: El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa, dado que ahí contiene toda alteración a la data de cualquier sistema informático, entendiéndose que el verbo rector del tipo penal se relaciona con ilegitimo, lo cual es un término más adecuado que ilegal, porque lo ilegal es algo que se encuentra fuera de la ley, pero lo ilegítimo encierra conductas que además de encontrarse fuera de ley, de darse el caso que se hallen en la norma como legales, no se encuentran autorizadas por quien debe hacerlas.

F4: A tenor del artículo 3º de la Ley Nº 30096, dicha conducta constituye delito informático y dentro de las consecuencias según este artículo son la pena privativa de la libertad y multa por atentar contra un bien jurídico tutelado.

Tabla 5

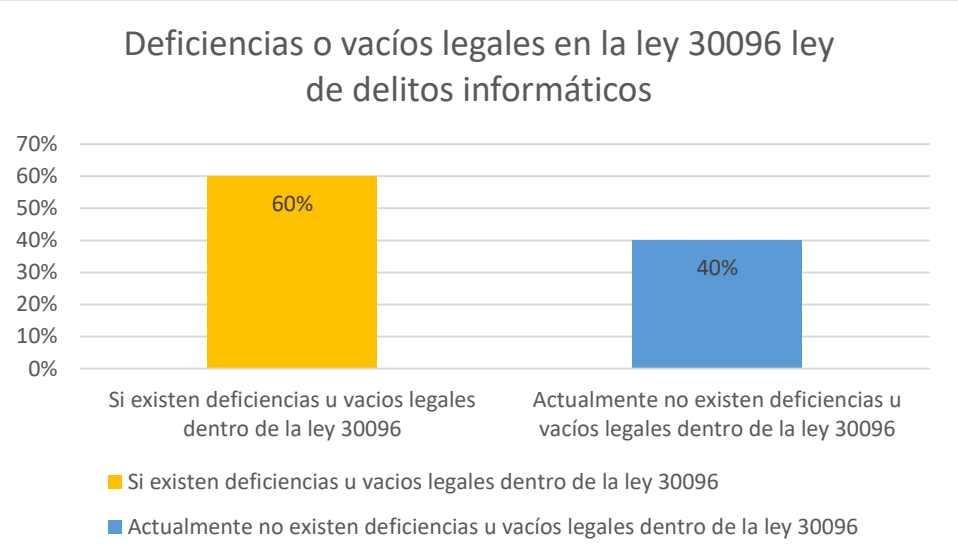
Deficiencias o vacíos legales en la ley 30096 ley de delitos informáticos.

Códigos	Frecuencia
Deficiencias y vacíos legales	5
Falta de buena interpretación de los operadores de justicia	1
Se debe considerar una modificatoria o reforma en la ley 30096	3
Afectación a la integridad de datos informáticos	1

Nota: Elaboración propia del autor a partir del resultado de las entrevistar aplicadas a abogados y fiscales penales.

Figura 1

Deficiencias o vacíos legales en la ley 30096 de delitos informáticos



Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales

Análisis e Interpretación: Con respecto a las deficiencias o vacíos legales en la ley 30096, ley de delitos informáticos, en la presente tabla 5 de los entrevistados dentro de su posición manifestaron que, si existen deficiencias y vacíos legales dentro de la ley 30096, 1 entrevistado expreso que falta una buena interpretación de los operadores de justicia, 3 entrevistados dieron a manifestaron que se debe considerar una modificatoria o reforma en la ley 30096, mientras solo 1 expreso que por las deficiencias o vacíos legales en la ley 30096 de delitos informáticos se está afectando la integridad de datos informáticos, con respecto a la presente figura se puede observar que el 60% de la población considera que existen deficiencias u vacíos legales dentro de la ley 30096, mientras que el 40% considera que actualmente no existen deficiencias u vacíos legales dentro de la presente ley.

Para ser más concretos veamos a continuación las respuestas brindadas por cada uno de los abogados y fiscales entrevistados:

A1: Yo, considero que la Ley N° 30096 es aquella que tiene por finalidad prevenir y sancionar aquellas conductas ilícitas las cuales afectan los sistemas y datos informáticos y otros bienes jurídicos que si bien es cierto son de gran relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con el fin de garantizar la lucha eficaz contra la ciberdelincuencia, sin embargo, considero que no tanto es la deficiencia y/o vacíos legales, si no la falta de buena interpretación por parte de los operadores de justicia.

A2: Si, ya que aparentemente nuestros legisladores no contaron con la participación o consentimiento de personal debidamente capacitado al momento de desarrollar la especificación de las leyes, hasta donde podemos observar, no existen expertos en computación ni conocimientos de cómo utilizar las redes sociales, y más aún nuestras normas y leyes son para copiar y pegar legislación extranjera básicamente.

A3: Sí, considero que aún existen vacíos legales en la presente ley, además que con el paso del tiempo van naciendo nuevos modus operandi de los ciberdelincuentes al momento de cometer el delito de fraude informático o cualquier otro tipo de delito informático que atente contra el bien jurídico tutelado y que aún no se encuentran debidamente regulados en la presente ley, es por ello que considero pertinente se tome en cuenta una nueva modificatoria en esta ley.

A4: Mira para serte sincero no considero que la Ley 30096 de Delitos informáticos tenga deficiencias o vacíos legales como mencionas, pero como me mencionaste al principio durante y post pandemia cada vez se crean mayores delitos informáticos usando nuevas modalidades delictivas gracias a los sistemas informáticos que trasgredan la norma y que estos aún no se encuentran dentro de la presente ley que mencionaste, así que lo que sugiero es que se adicionen nuevos artículos o en todo caso realizar un reforma a la ley en la cual si se establezcan todas las formas delictivas referente al fraude informático.

F1: Si, toda vez que nuestros legisladores al parecer no han contado con la participación o concurrencia de personal capacitado idóneo al momento de redactar la norma ya que podemos observar que en la misma no cuenta con los especialistas en informáticas, ni se conoce del uso de las redes sociales, además muchas de nuestras leyes son copiadas de legislaciones vecinas pero que al momento de aplicarlas en nuestro país no siempre traen el mismo resultado debido a que el entorno es distinto.

F2: Si existen deficiencias, por ejemplo, no se regulan aspectos procesales de colaboración en la investigación de esta clase de delitos, como sería captar un hacker para llegar a los integrantes de una de informática criminal; en lo sustantivo no hay regulación expresa de la clonación fraudulenta en sitios web (pishing), así como de otras figuras que están contenidas en el convenio de Budapest pero que no han sido incorporadas a nuestra legislación.

F3: Si, por cuanto no se identifica de manera adecuada las conductas específicas que constituyen actos delictivos dentro del contexto informático, además que no identifica por ejemplo la competencia, puesto que las plataformas virtuales pueden habilitarse en diversas zonas, sin que exista claridad sobre donde se perfecciona el delito o consuma el delito.

F4: Considero que la ley 30096 debería tener una reforma, esto debido a que el desarrollo de la tecnología tiene un ritmo muy acelerado, por lo que cualquier legislación que pretenda regular conductas perniciosas derivadas del mas uso de la misma, no podría abarcar todos los supuestos, por el ritmo de desarrollo de la informática y la comunicación en red, sin embargo, la Ley constituye un paso importante para incorporar la represión penal contra aquellas conductas que se valen del desarrollo de las herramientas tecnológicas para cometer delitos.

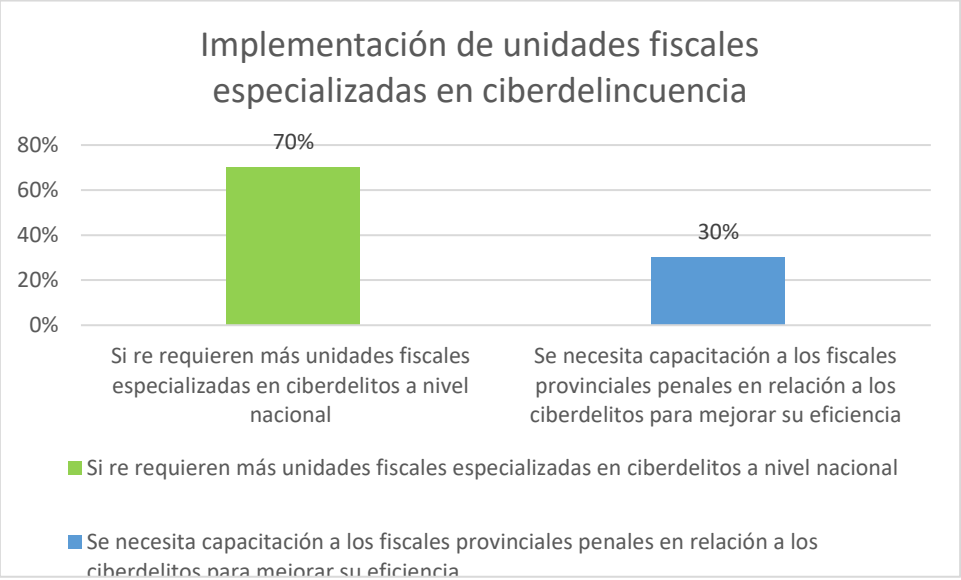
Tabla 6

Implementación de unidades fiscales especializadas en ciberdelincuencia.

Códigos	**Frecuencia**
Implementación de más unidades fiscales especializadas en ciberdelitos a nivel nacional.	7
Capacitación a los fiscales provinciales penales en relación a los ciberdelitos a nivel nacional.	3
Implementación de logística y personal especializado para combatir los delitos informáticos.	2
No existencia de unidades fiscales especializadas en ciberdelincuencia en todas las regiones del país.	1

Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales.

Figura 2 *Implementación de unidades fiscales especializadas en ciberdelincuencia.*



Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales

Análisis e Interpretación: En relación a la implementación de unidades fiscales especializadas en ciberdelincuencia 5 de los entrevistados expresaron que se debería Implementar más unidades fiscales especializadas en ciberdelitos a nivel nacional, por su parte 3 entrevistados expresaron que se debería capacitar a los fiscales provinciales penales en relación a los ciberdelitos para mejorar su eficiencia, 2 entrevistados expresaron que se debería poder Implementar logística y personal especializado para combatir los delitos informáticos, y solo 1 entrevistado manifestó que aún no existen unidades fiscales especializadas en ciberdelincuencia en todas las regiones del país, con respecto a la presente figura se puede evidenciar que el 70% de la población manifiesta que si se requieren más unidades fiscales especializadas en ciberdelitos a nivel nacional mientras que el 30% opina que lo que realmente se necesita es capacitación a los fiscales provinciales penales en relación a los ciberdelitos para mejorar su eficiencia.

Para ser más concretos veamos a continuación las respuestas brindadas por cada uno de los abogados y fiscales entrevistados:

A1: Si, por mi parte considero que deberíamos tener una Fiscalía Especializada en delitos Informáticos, con la finalidad de poder hacer una mejor investigación, por parte del Representante del Ministerio Publico en cuento a la ciberdelincuencia.

A2: Sí, pero lo más importante es capacitarlos, ellos son los que muchas veces conocen la IP, que es la huella de la red, se sabe que en nuestro país no están bien definidos y no existe la infraestructura, ellos deben estar registrado para crear un filtro para poder hacer algunos registros de varias entidades como EE. UU.

A3: Mira, claro que sí, ya que a día de hoy son un poco más de 65 fiscales especialistas en ciberdelincuencia que se encuentran laborando a nivel nacional, pero afirmo que son muy pocos ya que día a día los delitos informáticos se vuelven el pan y cada día y casi todos los días vemos nuevos casos de fraude informático, por lo que se tiene que tomar medidas con carácter de urgencia si no queremos que el número de delitos de fraude informático aumente exponencialmente en nuestro país.

A4: Mira si bien es cierto y como me comentaste, antes de la pandemia no había unidades fiscales especializadas en ciberdelincuencia en todas las regiones del país y cuando empezó la pandemia exploto el boom de los ciberdelitos y en especial el fraude informático, y es que no hace mucho se crearon las unidades fiscales especializadas en ciberdelincuencia, iniciaron su labor a finales del año 2020 en la ciudad de lima, pero a día de hoy siguen siendo pocas las unidades fiscales especializadas en ciberdelincuencia, por lo que considero que nuestra legislación si debe implementar más unidades fiscales especializadas en ciberdelincuencia en todas las regiones del Perú para poder combatir con este tipo de delitos.

F1: Si, pero sobre todo capacitarlos y que sean personas que sepan muchas veces el IP que es una huella dactilar de las redes se sepa que en nuestro país no están debidamente definidas ni se cuenta con la infraestructura debiendo crearseun registro, un filtro para poder realizar una forma de empadronamiento de los diferentes dispositivos como sucede en Estados Unidos.

F2: En el Perú si bien es cierto aún no hay unidades fiscales especializadas en Ciber delincuencia en todas las regiones del país, hay una coordinación de enlace centralizada y a nivel nacional hay fiscales de coordinación, pero ellos no investigan delitos informáticos

F3: Como está ocurriendo en la mayoría de las unidades que forman el aparato de justicia, existe necesidad no solo de personal sino también de logística, más aún ahora, que existe una diversidad de conductas criminales vinculadas al contexto informático. En el distrito Fiscal de Lambayeque no existe una fiscalía especializada, sino que es una que en adición a sus funciones se encarga de ver todos los casos de delitos informáticos, y no para conocerlos sino para coordinar con las demás fiscalías acciones con la división especializada en la ciudad de Lima; esto es, que dichos delitos no son conocidos por fiscales especializados.

F4: Por supuesto, no solo implementar más unidades fiscales, sobre todo se debe dotar de infraestructura, equipos y personal especializado en este complejo y cambiante ámbito del desarrollo tecnológico.

Tabla 7

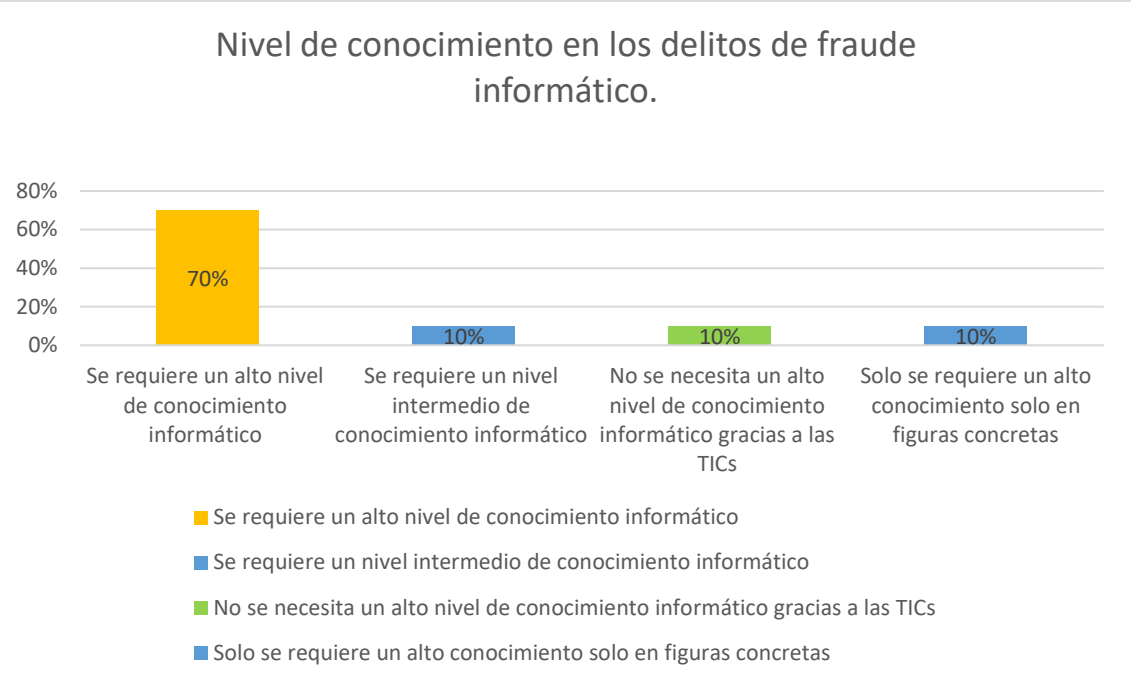
Nivel de conocimiento en los delitos de fraude informático.

Códigos	**Frecuencia**
No se necesita un alto nivel de conocimiento informático gracias a las TICs	5
Depende de las circunstancias en cada acto delictivo	3
Solo para las unidades fiscales que investigan los delitos informáticos	2
Existen figuras en las que si se refiere conocimientos avanzados	1
Si se requiere un alto nivel de conocimiento informático	1
Se requiere un nivel intermedio de conocimiento informático	1

Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales.

Figura 3

Nivel de conocimiento en los delitos de fraude informático.



Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales.

Análisis e Interpretación: En relación al nivel de conocimiento en los delitos de fraude informático en la tabla podemos notar que 5 de los entrevistados manifiestan que no se necesita un alto nivel de conocimiento informático gracias a las TICs , mientras que 3 entrevistados expresan que al nivel de conocimiento de los ciberdelincuentes en los delitos de fraude informático dependerá de las circunstancias en cada acto delictivo, por su parte 2 entrevistados expresan que solo las entidades especialistas en este tipo de delito tienen un alto nivel de conocimiento en este tipo de delitos informáticos, 1 entrevistado sustenta que en efecto si se requiere un alto nivel de conocimiento informático, mientras que por ultimo un entrevistado manifiesta que se requiere un nivel intermedio de conocimientos informáticos para este delito de fraude informático, es por ello que en el grafico podemos percibir que el 70% considera que si se requiere un alto nivel de conocimiento informático, mientras que el 10% de la población considera que solo se requiere un nivel intermedio de conocimiento informático, mientras que el 10% de la población expresa que no se necesita un alto nivel de conocimiento informático gracias a las TICs, el 10% expresa que si se requiere un alto nivel de conocimiento informático pero solo en figuras concretas.

Para ser más concretos veamos a continuación las respuestas brindadas por cada uno de los abogados y fiscales entrevistados:

A1: Considero que la tecnología está en cualquier dispositivo y no tanto es el nivel de conocimiento recodemos que existen muchos tutoriales en las páginas web, indicando el paso a paso de como cometer este tipo de ciber delitos.

A2: No, no las personas que cometen estos delitos, demasiado fáciles para las mismas personas que quieren cometer fraudes informáticos, sino las personas que los investigan.

A3: Esto depende las circunstancias y los agravantes, por lo que sí y no dependiendo en que caso nos encontremos, por ejemplo, si alguien quisiera dar mal uso de los sistemas o software con propósitos fraudulentos perjudicando al estado de gravedad pues el conocimiento que debe tener ese ciberdelincuente debe ser mayor y estructurado , pero para poder cometer este delito a cualquier persona ahora con la tecnológica actual y el libre acceso a la información el ciberdelincuente solo con ver tutoriales o guías en internet es más que suficiente para poder lograr su objetivo de forma sencilla a través de aplicaciones que facilitan su propósito fraudulento llegando a concretar este acto delictivo.

A4: Pues estoy seguro que no se necesita ser un experto en el uso de sistemas informáticos al nivel de un ingeniero de sistemas o software para poder delinquir en la modalidad de fraude informático ya que si bien es cierto con el nacimiento de las TICs cualquier persona tiene acceso libre a casi todo tipo de información que necesite y en el internet se puede encontrar múltiples tutoriales de como poder hackear sistemas, alterar información fácilmente a través de aplicaciones que les facilita todo el trabajo .

F1: No, para quien los comete por la alta cantidad de información que podemos encontrar a día de hoy en la web, pero sí para quien los investiga como los fiscales especialistas en ciberdelincuencia.

F2: No existe la figura con el nomen iuris de fraude cibernético, pero si fraude informático; para ciertas figuras como el acceso ilícito simple no se requiere conocimiento especiales, teniendo en cuenta que muchas veces es la victima quien proporciona los datos al delincuente informático ; pero hay figura en la que si se requiere conocimientos especiales para romper los protocolos de seguridad de los sistemas informáticos como por ejemplo en el delito de interceptación de datos informáticos.

F3: En efecto, por cuanto el delincuente común no maneja leguajes de programación o interfaz de los programas o plataformas digitales.

F4: En principio no, basta con conocimientos intermedios. La experiencia indica que los sujetos activos en la comisión de este tipo de delitos, son generalmente trabajadores o dependientes de empresas tecnológicas, quienes por razón del servicio que brindan, tienen acceso al software de datos de los clientes. En el caso de los delitos informáticos sexuales, no se necesita conocimientos especiales, basta conocer el funcionamiento de cualquier dispositivo que tenga acceso a internet.

Tabla 8

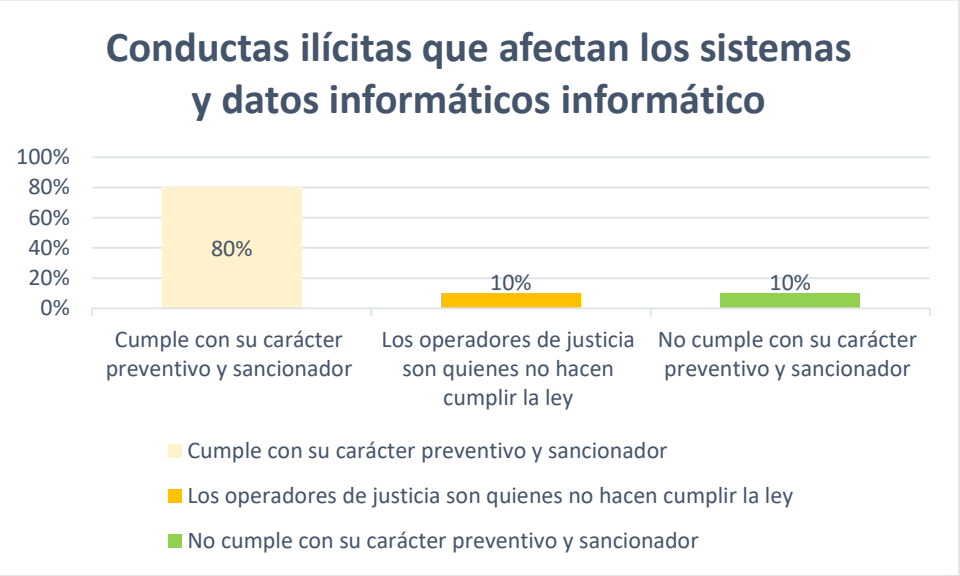
Carácter preventivo y sancionador de la ley 30096 para las conductas ilícitas que afectan los sistemas y datos informáticos.

Códigos	Frecuencia
Si cumple con su carácter preventivo y sancionador	7
Los operadores de justicia no hacen cumplir la ley	1
No cumple con su carácter preventivo y sancionador	1

Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales

Figura 4

Conductas ilícitas que afectan los sistemas y datos informáticos informático.



Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales

Análisis e Interpretación: Se les pregunto a los entrevistados si consideran que la ley 30096 de delitos informáticos cumple con su carácter preventivo y sancionador de aquellas conductas ilícitas que atentas contra los datos y sistemas informáticos a lo que 6 entrevistados expresaron que efectivamente si cumple con su carácter preventivo y sancionador, por su parte 1 entrevistado menciona que son Los operadores de

justicia aquellos que no hacen cumplir la ley, 1 entrevistado afirma que la ley 30096 no cumple con el carácter preventivo y sancionador que debería contar, de acuerdo al grafico planteado el 80% de la población expresa que la ley 30096 si cumple con su carácter preventivo y sancionador, mientras que el 10% afirma que son operadores de justicia son quienes no hacen cumplir la ley, por su parte el 10% restante de la población expresa que la ley de delitos informáticos no cumple con su carácter preventivo y sancionador que la debería caracterizar.

Para ser más concretos veamos a continuación las respuestas brindadas por cada uno de los abogados y fiscales entrevistados:

A1: Reitero, lo que mencione hace unos momentos y como dije la Ley N° 30096 tiene por finalidad prevenir y sancionar las conductas ilícitas en cuanto a los delitos informáticos, pero quienes deberían hacer cumplir las normas, son los operadores de justicia.

A2: Este es el fin de la ley, pero los tipos de delitos que se pueden cometer siguen evolucionando, siendo el más común el robo de dinero a través de Internet.

A3: Claro que sí, ya que ese es el objeto de la Ley 30096, prevenir y sancionar este tipo de conductas dolosas que afectan los sistemas y datos informáticos y bienes jurídicos tutelados de gran relevancia penal como cuando se afecte e patrimonio del estado.

A4: Pues sí, la ley 30096 se creó para poder combatir con la llegada de los delitos informáticos y todas sus modalidades contando con un carácter preventivo y sancionador de todas aquellas conductas atípicas e ilegales que afectas los sistemas informáticos cometidos utilizando herramientas informáticas como celulares o computadoras, es por ello que se creó la ley 30096 con el objetivo de luchar y acabar con la ciberdelincuencia en nuestra legislación.

F1: Este es el fin de esta ley sin embargo aún falta mayor desarrollo de los tipos dedelitos que se pueden cometer, siendo el más común el robo de dinero por páginas web.

F2: Los delitos informáticos son figuras pluriofensivas en las que no solo se sanciona la afectación a bienes jurídicos vinculados con la seguridad informática sino también, la intimidad, la fe pública, etc.

F3: Si en cuanto a los tipos penales que reprime, asimismo considero que lapregunta debe estar dirigida a si la expresada ley logra la finalidad de frenar la incidencia de delitos informáticos.

F4: Si en cuanto a los tipos penales que reprime, asimismo considero que lapregunta debe estar dirigida a si la expresada ley logra la finalidad de frenar la incidencia de delitos informáticos.

Tabla 9

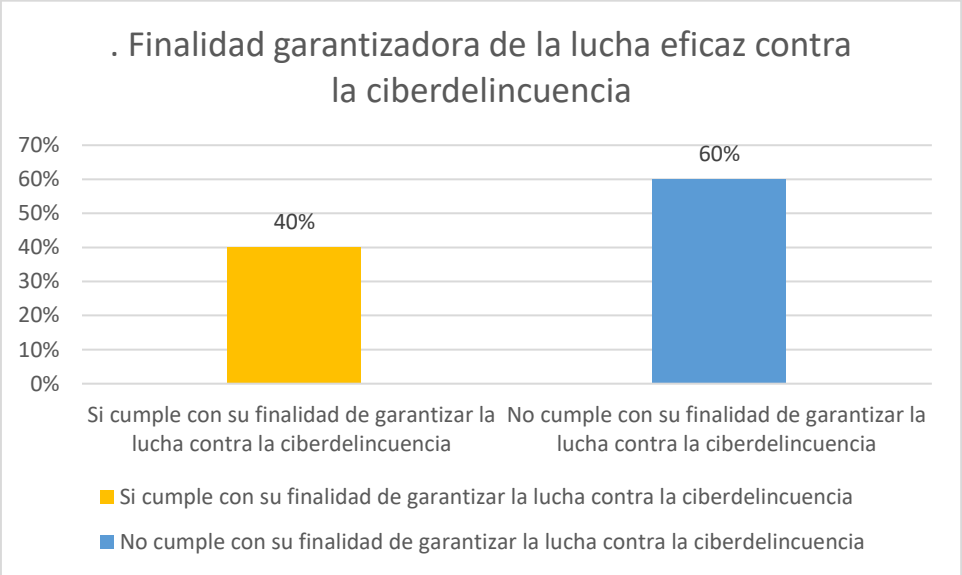
Finalidad garantizadora de la lucha eficaz contra la ciberdelincuencia.

Códigos	
Si cumple con su finalidad de garantizar la lucha contra la ciberdelincuencia	4
No cumple con su finalidad de garantizar la lucha contra la ciberdelincuencia	5
Depende tanto del tipo penal cometido como también la proporcionalidad entre el hecho y el delito	1

Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales

Figura 5

Finalidad garantizadora de la lucha eficaz contra la ciberdelincuencia.



Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales

Análisis e Interpretación: En la presente tabla podemos visualizar que respecto a la pregunta de si creen si la ley 30096 cumple con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia, a lo que 4 de los entrevistados manifestaron que efectivamente sí, sí cumple con su finalidad de garantizar la lucha contra la ciberdelincuencia, mientras que 5 expresaron que esta ley no está diseñada para garantizar la lucha contra la ciberdelincuencia debido a que ese no era su finalidad, por su parte 1 entrevistado menciono que esto depende tanto del tipo penal cometido como también la proporcionalidad entre el hecho y el delito, visualizando el grafico podemos connotar que el 40% de la población considera que la ley 30096 si cumple

con su finalidad de garantizar la lucha contra la ciberdelincuencia, mientras que el 60% opina que la ley 30096 no cumple con esta finalidad de garantizar la lucha contra la ciberdelincuencia.

Para ser más concretos veamos a continuación las respuestas brindadas por cada uno de los abogados y fiscales entrevistados:

A1: Sí, es una ley especial y su finalidad es prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnología.

A2: Realmente no, creo que se necesitan otros tejidos para lograr este objetivo.

A3: Efectivamente, ya que la función de esta ley como mencione reiteradas veces es poder prevenir y sancionar los delitos informáticos, contribuyendo a la lucha contra la ciberdelincuencia, es por ello que nuestros legisladores elaboraron esta ley detallando en 7 capítulos los delitos informáticos existentes que existen actualmente en nuestra legislación peruana.

A4: Si, pues efectivamente mira yo considero que la ley si cumple con su finalidad, ya que fue elaborada con ese fin, poder luchar contra ciberdelincuencia, el problema en si radica en que nuestros legisladores muchas veces no usan la ley correctamente, es cierto que la ley 30096 pueda tener falencias, pero si cumple con su rol de acabar con la delincuencia informática y en este caso a tratar el fraude informático.

F1: No por sí sola, considero que hace falta otras formas que entrelacen estepropósito a conseguir.

F2: En realidad, no es una ley para luchar contra la ciberdelincuencia sino de punición de conducta delictivas. La lucha contra la delincuencia informática tiene que ser a través de otros documentos técnicos y jurídicos.

F3: A criterio personal no, porque es muy general, hay conductas que podrían ser sujetos de mecanismos de defensa mediante las improcedencias de acción por lo difusa que es la norma.

F4: Considero que es un primer paso debido a que el combate a este tipo de delito no solo debe tener un componente normativo, sino que se debe complementar con otras medidas de carácter policial. Si bien es cierto, existe la unidad policial especializada de la PNP DIVINDAT, sin embargo, es necesario dotarla de equipos y especializar más al personal.

Tabla 10

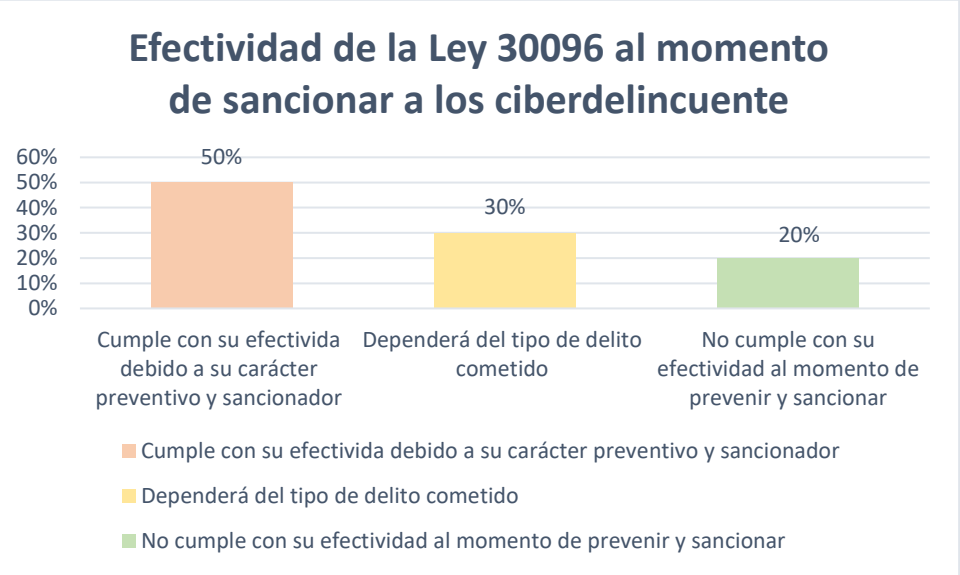
Efectividad de la Ley 30096 al momento de sancionar a los ciberdelincuente.

Códigos	Frecuencia
Es efectiva al momento de sancionar los ciberdelincuentes	3
La efectividad de la ley depende de los operadores de justicia	1
Dependerá del tipo de delito cometido	2
No se aplica adecuadamente la ley 30096	2
Es muy pronto para estimar su efectividad	1

Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales

Figura 6

Efectividad de la Ley 30096 al momento de sancionar a los ciberdelincuente.



Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales

Análisis e Interpretación: Como se ha podido evidenciar en la presente tabla 3 de los entrevistados expresan que la ley 300969 si cumple con este carácter de efectividad que permite poder tanto prevenir como sancionar a los ciberdelincuentes, un entrevistado manifestó que si hablamos de efectividad en la presente ley solo dependerá de los operadores de justicia, 2 de los entrevistados expresan que la efectividad

dependerá del tipo de delito cometido, 2 entrevistados expresan que aun a día de hoy no se aplica adecuadamente la ley 30096 de delitos informáticos mientras que por su parte un entrevistado manifiesto que aún es muy pronto para estimar la efectividad de la ley, en el grafico podemos visualizar que del 100% de la población, un 50% empresa que la ley 30096 si cumple con su efectividad debido a su carácter preventivo y sancionador, el 30% expresa que la efectividad dependerá del tipo de delito cometido, mientras que el 20% sustenta que la ley 30096 no cumple con su efectividad al momento de prevenir y sancionar.

Para ser más concretos veamos a continuación las respuestas brindadas por cada uno de los abogados y fiscales entrevistados:

A1: Considero que la efectividad depende de los operadores de justicia debido a que en muchas ocasiones no usan el carácter sancionador de forma correcta

A2: Esto dependerá del tipo de delito cometido y de la proporcionalidad entre el hecho y la infracción.

A3: Mira si hablamos de efectividad de la ley en si pues es correcto, es muy efectiva debido a que cuenta con un carácter sancionador cuando se trata de delitos informáticos contra el patrimonio como lo es el fraude informático, el problema radica en que no siempre se hace el uso correcto de la ley a la hora de sancionar dejando impunes a muchos ciberdelincuentes a día de hoy, lo cual es algo muy absurdo ya que en la ley 30096 prescribe correctamente cada pena a cada acto ilícito.

A4: Como ya había mencionado hace unos momentos no, la ley 30096 si es efectiva, el problema aquí en si es que muchas veces los legisladores no actúan de manera correcta al momento de aplicar penas privativas de la libertad de acuerdo a ley no siendo acordes al delito cometido, aquello que se puede evidenciar muchas veces en todos los medios de información pública en nuestro país cabe recalcar que esta mala praxis es algo que comúnmente también se practica por los legisladores en otros países latinoamericanos.

F1: Eso va depender del tipo penal que haya cometido, y de la proporcionalidad entre el hecho y el delito.

F2: Entiendo que lo que quiere decir el entrevistador es si considero que la ley 30096 es efectiva para sancionar el delito de fraude informático, en ese caso mi respuesta es que si, en la medida que se aplique correctamente la sanción y se dosifique la pena conforme corresponde.

F3: Considero que si bien, el legislador ha optado por considerar solo el aspecto doloso, existen situaciones en las que se pueden presentar hechos por culpa, por un exceso de confianza al momento del manejo de un programa por un experto que haga un uso indebido de tal circunstancia material que la ley no comprende, y que debe ser superado a través de una modificatoria.

F4: Es difícil decirlo a estas alturas, considero que es muy pronto para estimar si la ley 30096 cumple o no con su efectividad para sancionar los actos ilícitos cometidos por los ciberdelincuentes

Tabla 11

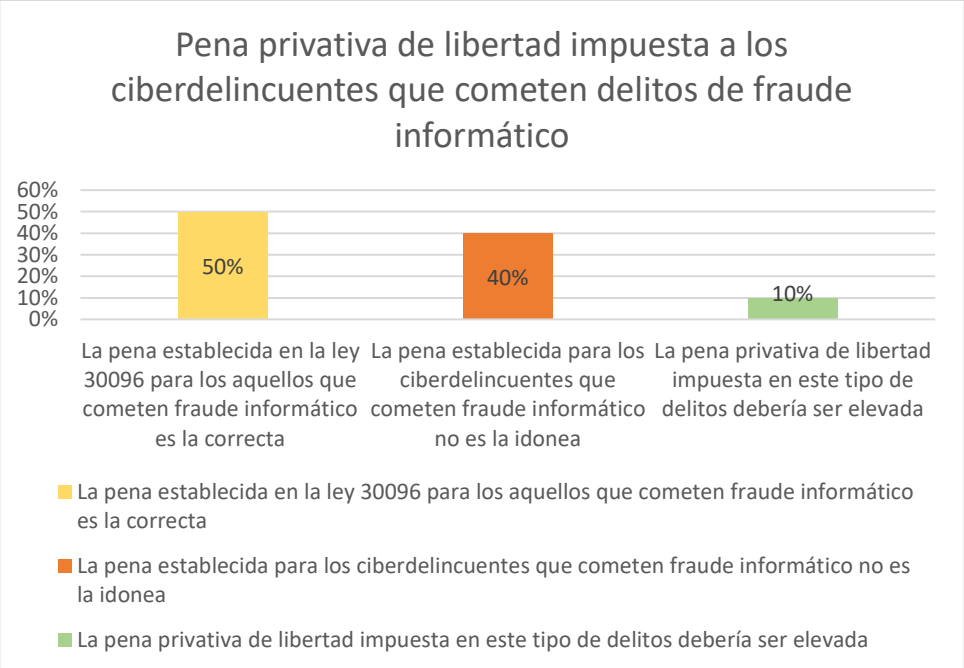
Pena privativa de libertad impuesta a los ciberdelincuentes que cometen delitos de fraude informático.

Códigos	Frecuencia
La pena establecida para los ciberdelincuentes que cometen fraude informático es la correcta	4
La pena establecida para los ciberdelincuentes que cometen fraude informático no es la adecuada	3
La pena privativa de libertad impuesta en este tipo de delitos debería ser mayor	1
El juzgador deberá fijar una pena concreta en función del impacto del acto ilícito cometido	1

Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales.

Figura 7

Pena privativa de libertad impuesta a los ciberdelincuentes que cometen delitos de fraude informático.



Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales.

Análisis e Interpretación: Dentro de la entrevista se le realizo a los entrevistados la pregunta de si ellos consideraban que la pena privativa de la libertad impartida por la ley 30096 para los ciberdelincuentes que cometen fraude informático es la adecuada a lo que 4 entrevistados expresaron que efectivamente la pena establecida para los ciberdelincuentes que cometen fraude informático es la correcta, mientras que 3 expresaron que la pena establecida para los ciberdelincuentes que cometen fraude informático no es la adecuada por lo cual se debe hacer una modificatoria, por su parte 1 entrevistado expreso que la pena privativa de libertad impuesta en este tipo de delitos debería ser mayor de acuerdo a los agravantes de cada delito, mientras que 1 entrevistado expreso que el juzgador es aquel que deberá fijar una pena concreta en función del impacto del acto ilícito cometido, por ello en el grafico mostrado podemos evidenciar que del 100% de la población , el 50% opina que la pena establecida en la ley 30096 para los aquellos que cometen fraude informático es la correcta, mientras que el 40% de la población expresa que la pena establecida para los ciberdelincuentes que cometen fraude informático no es la idónea, mientras que el 10% manifiestan que la pena privativa de libertad impuesta en este tipo de delitos debería ser elevada.

Para ser más concretos veamos a continuación las respuestas brindadas por cada uno de los abogados y fiscales entrevistados:

A1: Considero que si debido a que cuando hablamos de una pena privativa de la libertad si se determina la responsabilidad del imputado, pues debería ser privado de su libertad.

A2: Quizás este sea un enfoque erróneo, pero debemos recordar que tenemos un código penal que pertenece al autor del delito, como comúnmente se le llama, es decir, premia al delincuente dándole una salida legal para mitigar su castigo.

A3: Cuando hablamos de pena privativa de la libertad considero que de tres a ocho años no es una pena adecuada ya que considero que debería ser mayor cuando se trate de daños irreparables contra el patrimonio de la persona, y en esas instancias considero que la pena que está tipificada en el artículo ocho de la ley es un poco para lo que se le debería aplicar a los ciberdelincuentes en este tipo de delitos, así que considero que se debería modificar el artículo ocho de la ley 30096 Ley de delitos informáticos.

A4: Si, mira si nos enfocamos en cual debería ser la debida pena de libertad que merezca un ciberdelincuente tendríamos que determinar el grado del delito cometido y el tipo de fraude que ha sido cometido para poder aplicar una debida pena, pero considero que la pena impuesta por los legisladores en el artículo 8 de la ley 30096 es la adecuada.

F1: No por sí sola, considero que hace falta otras formas que entrelacen estepropósito a conseguir.

F2: Debo entender que se refiere al marco punitivo abstracto entre 3 y 8 años de pena privativa de la libertad. Y pena de multa SI se atiende a criterios de proporcionalidad en la imposición de la pena, es lo correcto; obviamente se tendrán en cuenta los criterios de determinación concreta de la pena, y sobre todo evaluar si se suspende la ejecución de la pena o se impone pena efectiva.

F3: Considero que sí, porque existen supuestos de gravedad que reconducen la pena a ser aplicada.

F4: La corrección o no de una pena es relativa. Es el Juzgador en cada caso concreto que debe fijar la pena en función a los criterios establecidos en el artículo 46° del Código Penal.

Tabla 12

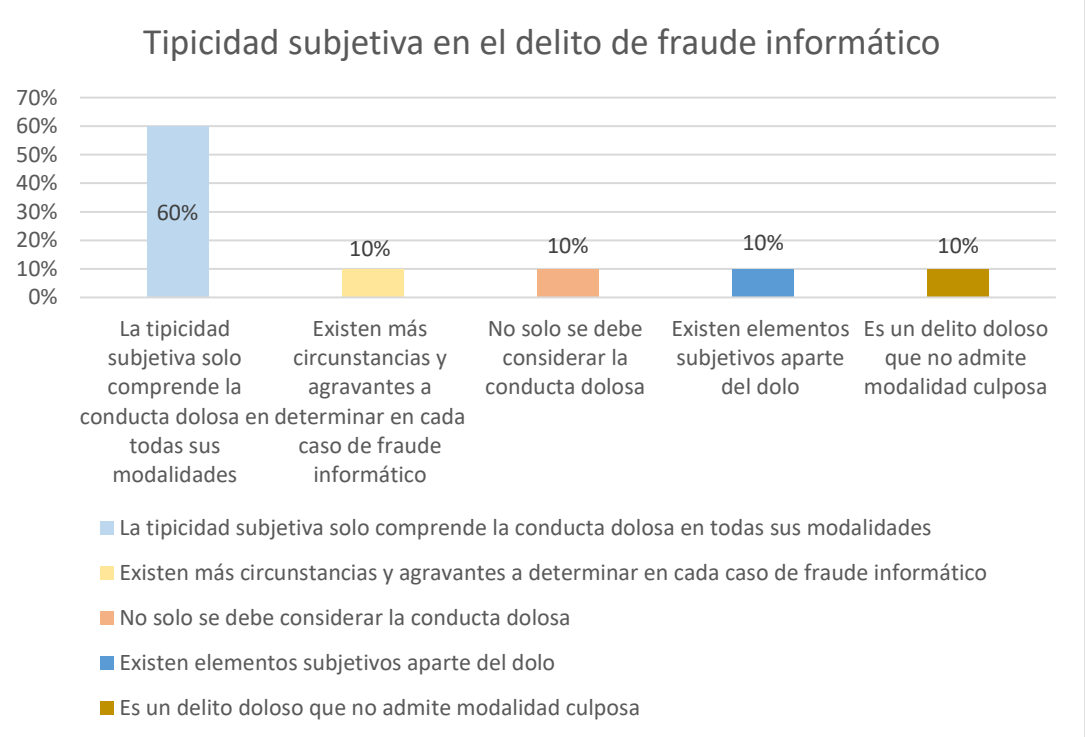
Tipicidad subjetiva en el delito de fraude informático.

Códigos	**Frecuencia**
La tipicidad subjetiva solo comprende la conducta dolosa en todas sus modalidades	5
Existen más circunstancias y agravantes a determinar en cada caso de fraude informático	1
No solo se debe considerar la conducta dolosa	1
Existen elementos subjetivos muy aparte del dolo	1
Es un delito doloso que no admite modalidad culposa	1

Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales

Figura 8

Tipicidad subjetiva en el delito de fraude informático.



Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales.

Análisis e Interpretación: Se le pregunto a los entrevistados si consideran que la tipicidad subjetiva en el delito de fraude informático comprende solo el análisis de la conducta dolosa y ante ello 5 entrevistados respondieron que la tipicidad subjetiva solo comprende la conducta dolosa en todas sus modalidades, 1 entrevistado expreso que si bien es cierto existen más circunstancias y agravantes a determinar en cada caso de fraude informático, 1 entrevistado sustento que no solo se debe considerar la conducta dolosa, mientras que 1 entrevistado dijo que existen elementos subjetivos muy aparte del dolo, 1 entrevistado expreso que el fraude es un delito doloso que no admite modalidad culposa, por ello en el presente grafico podemos evidenciar que el 60% expresa que la tipicidad subjetiva solo comprende la conducta dolosa en todas sus modalidades, el 10 % sustento que existen más circunstancias y agravantes a determinar en cada caso de fraude informático, mientras que el 10% dio a conocer que no solo se debe considerar la conducta dolosa, el 10% expreso que existen elementos subjetivos aparte del dolo, y por último el 10% restante expreso que el fraude informático es un delito que no admite modalidad culposa.

Para ser más concretos veamos a continuación las respuestas brindadas por cada uno de los abogados y fiscales entrevistados:

A1: Considero que el "dolo" si en un factor muy importante en cuento a la tipicidad subjetiva, pues de ello depende la culpabilidad del sujeto activo.

A2: Pues sí, mira, sinceramente las autoridades en este tipo de delitos informáticos como lo que es el fraude informático solo toman en cuenta casi siempre el poder determinar la conducta dolosa siendo materia de análisis.

A3: ¿La tipicidad Subjetiva? Pues si hablamos de la conducta dolosa también tenemos que determinar qué tipo de dolo como el dolo eventual que se ve en muchos casos de fraude informático, pero en si mayormente si, nuestras autoridades solo tienen en cuenta la tipicidad subjetiva, cuando existen más circunstancias y agravantes a determinar para cada caso de fraude informático que afecte en contra del patrimonio afectando el bien jurídico tutelado.

A4: Considero según mi experiencia que nuestros legisladores en la mayoría de casos solo ven la tipicidad subjetiva, pero en si considero que no solo considera la conducta dolosa, existen muchos factores al momento de manipular o también alterar lo que son los sistemas informáticos y determinar el resultado que este podría provocar desencadenando un perjuicio patrimonial.

F1: Si, al igual que los legisladores solo consideran que existe tipicidad objetiva en este tipo de delito de fraude informático cuando nos referimos a conductas dolosas y que tipo de dolo es.

F2: La ley sólo ha tipificado conductas dolosas, no imprudentes. Lo que si hay que analizar es que en algunos tipos penales existen elementos subjetivos diferentes al dolo.

F3: Como se indicó en una respuesta anterior, el legislador solo se ha centrado en tipificar conductas dolosas, pero es probable que el delincuente haga un uso autorizado pero que en un momento se torna ilegítimo que la norma estaría excluyendo.

F4: Desde mi punto de vista, el delito de fraude informático es un delito doloso que no admite modalidad culposa.

Tabla 13

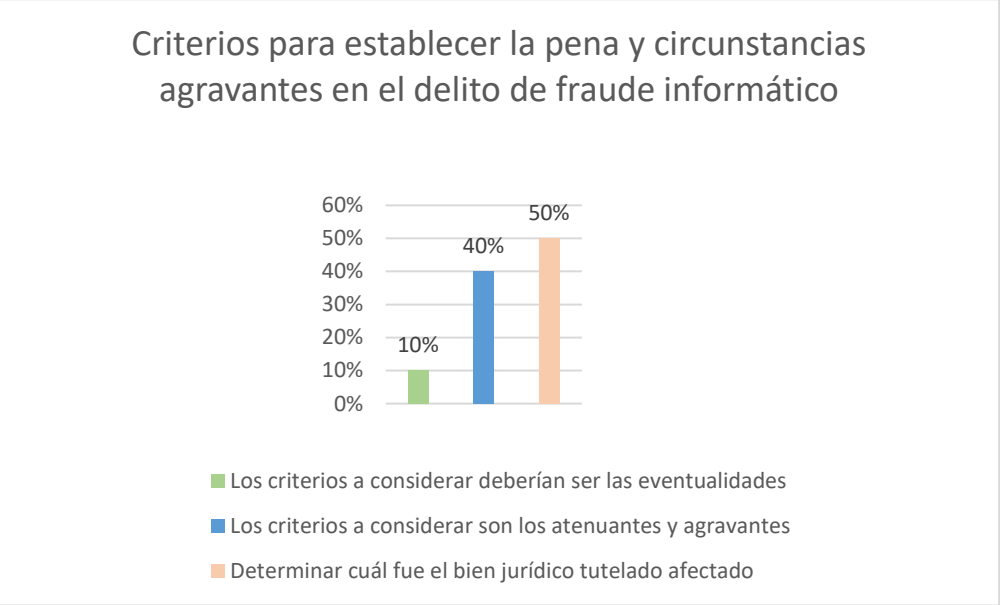
Criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático.

Códigos	**Frecuencia**
Los criterios a considerar deberían ser las eventualidades	1
Los criterios a considerar son los atenuantes y agravantes	3
Determinar cuál fue el bien jurídico tutelado afectado	4

Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales

Figura 9

Criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático.



Nota: Elaboración propia del autor a partir del resultado de las entrevistas aplicadas a abogados y fiscales penales

Análisis e Interpretación: Para la elaboración de la presente tabla se consideró pertinente como ultima interrogante preguntarle a los entrevistados cuales consideran que son los criterios para poder establecer

correctamente una pena en el delito de fraude informático y como se determinan las circunstancias agravantes en el presente delito, ante ello 4 de los entrevistados expresaron que primero se debe determinar cuál fue el bien jurídico tutelado afectado, 3 de los entrevistados sustentaron que los criterios a considerar son los atenuantes y agravantes, mientras que 1 entrevistado manifestó que los criterios a consideran deberían ser las eventualidades, con respecto a la presente figura podemos evidenciar que del 100% de la población el 50% manifiesta que se primero se debe determinar cuál fue el bien jurídico tutelado afectado, mientras que el 40% de la población expreso que los criterios a considerar son los atenuantes y agravantes, mientras que el 10% dio a conocer que Los criterios a considerar deberían ser las eventualidades.

Para ser más concretos veamos a continuación las respuestas brindadas por cada uno de los abogados y fiscales entrevistados:

A1: Los criterios deberían ser las eventualidades como por ejemplo (reincidencia, cuando se tenga como sujetos pasivos a personas adultos mayores, cuando estos inmersos temas vinculados a la salud entre otros).

A2: Según lo dispuesto en la parte general del Código Penal, en las circunstancias atenuantes, atenuantes y agravantes que reducirán la pena, así como en parte de la tercera parte de la pena, según determine el Ministerio publico según las circunstancias del agente.

A3: Bueno, por mi parte considero que para establecer la debida pena y circunstancias agravantes en este delito se tiene que determinar en primer lugar cual fue el bien jurídico afectado al momento de consolidar este delito.

A4: Bueno, para poder establecer cuáles son los criterios de la pena y agravantes en este delito tenemos que fijarnos en el bien jurídico protegido, por ejemplo, en el caso que se afecte un patrimonio del estado que perjudique gravemente la pena sería mucho más elevada.

F1: Los establecidos en el código penal parte general en su atenuantes, eximentesy agravantes que servirán para graduar la pena y también la porción de terciosde la pena que se determina por el ministerio publico dependiendo las circunstancias del agente.

F2: Los criterios de determinación de la pena están fijados en los art. 45, 45-A, 46 y 46 A del Código Penal. Respecto a las circunstancias agravantes se evaluará que en el delito de fraude informático existen agravantes de primer grado y de segundo grado, cuando se verifica la existencia de los elementos que fundamentan la agravante, la pea se determinará conforme a dicho marco punitivo.

F3: Estimo que el legislador ha considerado el bien jurídico protegido, en subordinación al principio de responsabilidad por el hecho.

F4: Esto dependerá del tipo de delito informático, en los delitos informáticos contra el patrimonio, el criterio será el origen y destino del patrimonio afectado, por su parte en los delitos informáticos sexuales, lo será la edad de la víctima y en los delitos contra las comunicaciones, el criterio es la afectación a la seguridad nacional.

3.2. Discusión

Teniendo como precedente tanto el objetivo general como los objetivos específicos que se buscó realizar un análisis de la ley 30096 de delitos informáticos en aplicación a los delitos de fraude informático y poder identificar aquellos vacíos o deficiencias legales dentro de la presente ley se tomó en cuenta lo establecido en la tabla 3 se señala que dentro de las consecuencias jurídicas que existen luego de alterar de manera ilegal el ingreso de datos en sistemas informáticos los ocho entrevistados estuvieron de acuerdo al manifestar que los ciberdelincuentes que cometen este acto ilícito deben ser reprimidos con pena privativa de la libertad.

Solo dos consideraron como consecuencia valida la afectación del bien jurídico tutelado como afectación del presente acto ilícito, dos entrevistados manifestaron que además de una respectiva pena privativa de la libertad también se considera una multa correspondiente, dos entrevistados manifestaron que una de las consecuencias jurídicas al alterar el ingreso de datos de manera ilegal es la afectación a la integridad de datos informáticos.

Por otra parte en la tabla 4 y figura 2 podemos evidenciar que con respecto a las deficiencias o vacíos legales en la ley 30096, ley de delitos informáticos, en la presente tabla 5 de los entrevistados dentro de su posición manifestaron que, si existen deficiencias y vacíos legales dentro de la ley 30096, 1 entrevistado expreso que falta una buena interpretación de los operadores de justicia, 3 entrevistados dieron a manifestaron que se debe considerar una modificatoria o reforma en la ley 30096, mientras solo 1 expreso que por las deficiencias o vacíos legales en la ley 30096 de delitos informáticos se está afectando la integridad de datos informáticos, con respecto a la presente figura se puede observar que el 60% de la población considera que existen deficiencias u vacíos legales dentro de la ley 30096, mientras que el 40% considera que actualmente no existen deficiencias u vacíos legales dentro de la presente ley.

Por otro lado en la tabla 5 y figura 3 podemos evidenciar que en relación a la implementación de unidades fiscales especializadas en ciberdelincuencia 5 de los entrevistados expresaron que se debería Implementar más unidades fiscales especializadas en ciberdelitos a nivel nacional, por su parte 3 entrevistados expresaron que se debería capacitar a los fiscales provinciales penales en relación a los ciberdelitos para mejorar su eficiencia, 2 entrevistados expresaron que se debería poder Implementar logística y personal especializado para combatir los delitos informáticos, y solo 1 entrevistado manifestó que aún no existen unidades fiscales especializadas en ciberdelincuencia en todas las regiones del país.

Con respecto a la presente figura se puede evidenciar que el 70% de la población manifiesta que si se requieren más unidades fiscales especializadas en ciberdelitos a nivel nacional mientras que el 30% opina que lo que realmente se necesita es capacitación a los fiscales provinciales penales en relación a los ciberdelitos para mejorar su eficiencia.

De igual manera en la tabla 6 y figura 4 podemos evidenciar que en relación al nivel de conocimiento en los delitos de fraude informático en la tabla podemos notar que 5 de los entrevistados manifiestan que no se necesita un alto nivel de conocimiento informático gracias a las TICs.

Mientras que 3 entrevistados expresan que al nivel de conocimiento de los ciberdelincuentes en los delitos de fraude informático dependerá de las circunstancias en cada acto delictivo, por su parte 2 entrevistados expresan que solo las entidades especialistas en este tipo de delito tienen un alto nivel de conocimiento en este tipo de delitos informáticos, 1 entrevistado sustenta que en efecto si se requiere un alto nivel de conocimiento informático, mientras que por ultimo un entrevistado manifiesta que se requiere un nivel intermedio de conocimientos informáticos para este delito de fraude informático, es por ello que en el grafico podemos percibir que el 70% considera que si se requiere un alto nivel de conocimiento informático, mientras que el 10% de la población considera que solo se requiere un nivel intermedio de conocimiento informático, mientras que el 10% de la población expresa que no se necesita un alto nivel de conocimiento informático debido a las TICs, el 10% expresa que si se requiere un alto nivel de conocimiento informático pero solo en figuras concretas.

Por otro lado en la tabla 7 y figura 5 podemos evidenciar que de acuerdo a lo que se les pregunto a los entrevistados si consideran que la ley 30096 de delitos informáticos cumple con su carácter preventivo y sancionador de aquellas conductas ilícitas que atentas contra los datos y sistemas informáticos a lo que 6 entrevistados expresaron que efectivamente si cumple con su carácter preventivo y sancionador, por su parte 1 entrevistado menciona que son Los operadores de justicia aquellos que no hacen cumplir la ley, 1 entrevistado afirma que la ley 30096 no cumple con el carácter preventivo y sancionador que debería contar.

De acuerdo al grafico planteado el 80% de la población expresa que la ley 30096 si cumple con su carácter preventivo y sancionador, mientras que el 10% afirma que son operadores de justicia son quienes no hacen cumplir la ley, por su parte el 10% restante de la población expresa que la ley de delitos informáticos no cumple.

En la tabla 8 y figura 6 podemos evidenciar que en la presente tabla podemos visualizar que respecto a la pregunta de si creen si la ley 30096 cumple con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia, a lo que 4 de los entrevistados manifestaron que efectivamente sí, sí cumple con su finalidad de garantizar la lucha contra la ciberdelincuencia, mientras que 5 expresaron que esta ley no está diseñada para garantizar la lucha contra la ciberdelincuencia debido a que ese no era su finalidad, por su parte 1 entrevistado menciono que esto depende tanto del tipo penal cometido como también la proporcionalidad entre el hecho y el delito.

Visualizando el grafico podemos connotar que el 40% de la población considera que la ley 30096 si cumple con su finalidad de garantizar la lucha contra la ciberdelincuencia, mientras que el 60% opina que la ley 30096 no cumple con esta finalidad de garantizar la lucha contra la ciberdelincuencia.

En la tabla 9 y figura 7 podemos visualizar que como se ha podido evidenciar en la presente tabla, 3 de los entrevistados expresan que la ley 300969 si cumple con este carácter de efectividad que permite poder tanto prevenir como sancionar a los ciberdelincuentes, un entrevistado manifestó que si hablamos de efectividad en la presente ley solo dependerá de los operadores de justicia, 2 de los entrevistados expresan que la efectividad dependerá del tipo de delito cometido, 2 entrevistados expresan que aun a día de hoy no se

aplica adecuadamente la ley 30096 de delitos informáticos mientras que por su parte un entrevistado manifiesto que aún es muy pronto para estimar la efectividad de la ley.

En el grafico podemos visualizar que del 100% de la población, un 50% expresa que la ley 30096 si cumple con su efectividad debido a su carácter preventivo y sancionador, el 30% expresa que la efectividad dependerá del tipo de delito cometido, mientras que el 20% sustenta que la ley 30096 no cumple con su efectividad al momento de prevenir y sancionar.

En la tabla 10 y figura 8 podemos constatar que dentro de la entrevista que se le realizo a los entrevistados la pregunta de si ellos consideraban que la pena privativa de la libertad impartida por la ley 30096 para los ciberdelincuentes que cometen fraude informático es la adecuada a lo que 4 entrevistados expresaron que efectivamente la pena establecida para los ciberdelincuentes que cometen fraude informático es la correcta, mientras que 3 expresaron que la pena establecida para los ciberdelincuentes que cometen fraude informático no es la adecuada por lo cual se debe hacer una modificatoria, por su parte 1 entrevistado expreso que la pena privativa de libertad impuesta en este tipo de delitos debería ser mayor de acuerdo a los agravantes de cada delito, mientras que 1 entrevistado expreso que el juzgador es aquel que deberá fijar una pena concreta en función del impacto del acto ilícito cometido.

Por ello en el grafico mostrado podemos evidenciar que del 100% de la población indica que el 50% opina que la pena establecida en la ley 30096 para los aquellos que cometen fraude informático es la correcta, mientras que el 40% de la población expresa que la pena establecida para los ciberdelincuentes que cometen fraude informático no es la idónea, mientras que el 10% manifiestan que la pena privativa de libertad impuesta en este tipo de delitos debería ser elevada.

En la tabla 11 y figura 9 podemos evidenciar que de acuerdo a lo que se les pregunto a los entrevistados si consideran que la tipicidad subjetiva en el delito de fraude informático comprende solo el análisis de la conducta dolosa y ante ello 5 entrevistados respondieron que la tipicidad subjetiva solo comprende la conducta dolosa en todas sus modalidades, 1 entrevistado expreso que si bien es cierto existen más circunstancias y agravantes a determinar en cada caso de fraude informático, 1 entrevistado sustento que no solo se debe considerar la conducta dolosa, mientras que 1 entrevistado dijo que existen elementos subjetivos muy aparte del dolo, 1 entrevistado expreso que el fraude es un delito doloso que no admite modalidad culposa.

Por ello en el presente grafico podemos evidenciar que el 60% expresa que la tipicidad subjetiva solo comprende la conducta dolosa en todas sus modalidades, el 10 % sustento que existen más circunstancias y agravantes a determinar en cada caso de fraude informático, mientras que el 10% dio a conocer que no solo se debe considerar la conducta dolosa, el 10% expreso que existen elementos subjetivos aparte del dolo, y por último el 10% restante expreso que el fraude informático es un delito que no admite modalidad culposa.

En la tabla 12 y figura 10 pudimos notar que para poder elaborar la presente tabla se consideró pertinente como ultima interrogante preguntarle a los entrevistados cuales consideran que son los criterios para poder

establecer correctamente una pena en el delito de fraude informático y como se determinan las circunstancias agravantes en el presente delito, ante ello 4 de los entrevistados expresaron que primero se debe determinar cuál fue el bien jurídico tutelado afectado, 3 de los entrevistados sustentaron que los criterios a considerar son los atenuantes y agravantes, mientras que 1 entrevistado manifestó que los criterios a consideran deberían ser las eventualidades.

Con respecto a la presente figura podemos evidenciar que del 100% de la población el 50% manifiesta que primero se debe determinar cuál fue el bien jurídico tutelado afectado, mientras que el 40% de la población expreso que los criterios a considerar son los atenuantes y agravantes, mientras que el 10% dio a conocer que Los criterios a considerar deberían ser las eventualidades.

Dentro del Aporte práctico para poder determinar una correcta definición de lo que es un sistema cibernético es preciso mencionar que es algo estrictamente complicado ya que su significado se extiende y se propaga no solo del derecho en su totalidad o generalidad, también a la parte del derecho penal, es así que podemos entender que un sistema informático es aquel conjunto o vínculo entre dispositivos electrónicos, partes que lo componen tanto inmateriales como materiales los cuales ayudan a permitir poder recopilar, establecer, poder procesar la información y la data, mediante la aplicación de software como también del sistema operativo el cual está orientado para aportar y apoyar las actividades humanas.

Es por ello que se puede dar a conocer que en nuestra legislación existe la ley 30096 de delitos informáticos, la misma que tiene poder tanto prevenir como sancionar todas aquellas conductas que son ilegales u ilícitas, las mismas que vulneran tanto los datos como sistemas informáticos o bienes jurídicos protegidos/tutelados que tengan relevancia penal como cuando ocurre vulneración de patrimonio del estado, es por ello que la ley 30096 cuenta con la finalidad de poder garantizar la lucha contra la delincuencia informática.

Alvarado (2017), nos da a conocer que dentro de nuestro ordenamiento jurídico podemos presenciar distintas deficiencias legislativas tipificadas en este tipo de delitos cometidos, según lo que expresa tanto la legislación comparada como la doctrina internacional se puede dar a conocer que nuestros legisladores peruanos no se dedicaron a regular de manera correcta aquellas contramedidas que constituyan un adecuado control, esto con el único fin de poder identificar cual es verdaderamente la conducta que vendría a ser penalmente notable.

Hernández (2018) considera a los delitos informáticos como aquella versión actualizada de los delitos comunes y corrientes que la mayoría conocemos y esta afirmación es parcialmente cierta debido a que una de las principales funciones de la tecnología actual es ser como un medio de comunicación a nivel global, pero por otra parte junto con la aparición de la tecnología aparecieron nuevos bienes jurídicos tutelados y aquellas conductas que definen a la informática.

De esta forma podemos expresar que los delitos informáticos hasta el día de hoy se usaron de una manera común, pero actualmente cada día estamos siendo testigos que se está usando los sistemas informáticos para facilitar los delitos como en este caso el fraude informático usando las redes sociales para cometer el delito causado por los ciberdelincuentes.

Hiplán (2019) menciona que con el único propósito de identificar si usar los sistemas informáticos vulneran los intereses jurídicos, aquellos que entran dentro de las categorías del bien jurídico tutelado, es así que de esta forma podemos determinar cuáles son aquellas conductas que a través de la tecnología actual se atenta en contra de los bienes jurídicos tutelados y que además se lesiona aquel interés que no es objeto de la tutela.

Moncada (2020) nos expresa que la Ley de Delitos Informáticos, Ley 30096 aun cuenta con una deficiencia al instante de decidir cuál es el bien jurídico salvaguardado en esta clase de delitos, es de esta forma que esta realidad puede llegar a dañar evaluación penal y poder decidir cuál es el nivel de acusación a causa de que el ministerio público debido a que poseemos que considerar que la ley de delitos informáticos tiene como objetivo proteger la apariencia corpóreo del bien jurídico salvaguardado, en esta situación los sistemas informáticos, así mismo cabe determinar que de acuerdo con la disposición N°9 de la Ley de Delitos informáticos, Ley 30096 prescribe que el sistema informático está construido por los computadoras y sus interconexiones.

Es por ello que de acuerdo a los resultados de la presente investigación llegamos a constatar que respecto a las consecuencias jurídicas que luego de poder alterar de manera ilegal el ingreso de datos en los sistemas informáticos el 100% de la población que se tomó como muestra manifestó que los ciberdelincuentes que incurren en el presente acto delictivo deben ser severamente reprimidos con pena privativa de la libertad de acuerdo a ley.

Con respecto a las deficiencias o vacíos que existen dentro de la ley 30096, ley de delitos informáticos, el 60% de la población expreso que debido a que rápidamente con el pasar del tiempo se crean nuevas modalidades para poder cometer actos delictivos informáticos a día de hoy si existen deficiencias u vacíos legales dentro de la ley 30096.

Respecto a la implementación de poder implementar más unidades fiscales especializadas en ciberdelitos a nivel nacional, el 70% de la población expreso que si bien es cierto efectivamente si se requieren más unidades fiscales especializadas en ciberdelitos a nivel nacional, pero que se debería priorizar es poder capacitar a los fiscales provinciales penales en relación a los ciberdelitos para mejorar su eficiencia.

Por otro lado, en relación al nivel de conocimiento que necesitan los ciberdelincuentes al momento de poder cometer delitos de fraude informático el 70 de la población consideran que efectivamente si requiere un alto nivel de conocimiento informático.

De igual manera respecto a poder constatar si la población considera que la ley 30096 de delitos informáticos cumple con su carácter preventivo y sancionador de aquellas conductas ilícitas que atentas contra los datos

y sistemas informáticos el 80% de la población expresa tajantemente que la ley 30096 de delitos informáticos si cumple con su carácter preventivo y sancionador.

Concretizando respecto a determinar si efectivamente la población considera que la ley 30096 cumple con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia el 60 % de la población expreso tajantemente que la ley 30096 aun a día de hoy no cumple con su finalidad de poder garantizar la lucha contra la ciberdelincuencia.

En síntesis, respecto al carácter de efectividad de la ley 30096 de delitos informáticos que permite poder tanto prevenir como sancionar a los ciberdelincuentes que cometan este tipo de actos delictivos tipificados en la presente ley el 50% expresa que la ley 30096 si cumple con su efectividad debido a su carácter preventivo y sancionador.

De igual forma podemos constatar que respecto a considerar si la pena privativa de la libertad impartida por la ley 30096 de delitos informáticos aplicada a aquellos ciberdelincuentes que cometen fraude informático es la adecuada o no, el 50% opina que la pena establecida en la ley 30096 para aquellos que cometen fraude informático es la correcta, mientras que el 40% de la población expresa que la pena establecida para los ciberdelincuentes que cometen fraude informático no es la idónea actualmente, por lo cual se entre en un debate para poder constatar verdaderamente cual sería la pena correcta para este tipo de delitos o cuales seria son factores a considerar para aplicar una sanción correcta correspondiente a aquel acto ilícito cometido en el delito de fraude informático.

Es de este modo que respecto a considerar si la tipicidad subjetiva en el delito de fraude informático comprende solamente el debido análisis de la conducta dolosa o no el 60% de la población expresa tajantemente que la tipicidad subjetiva solo comprende la conducta dolosa en todas sus modalidades

Por último, respecto a poder considerar cuales son los criterios para poder establecer correctamente una pena en el delito de fraude informático y como se determinan las circunstancias agravantes en el presente delito el 50% de la población llego a la conclusión de que primero se debe determinar cuál fue el bien jurídico tutelado afectado mientras que el 40% de la población expresa que los criterios a considerar son los atenuantes y agravantes.

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

A manera de conclusión se puede dar a conocer que al momento de analizar la ley 30096 de delitos informáticos y determinar cómo influía su aplicación en los delitos de fraude cibernético en nuestro país pudimos determinar que dentro de nuestro ordenamiento jurídico si pudimos evidenciar distintos vacíos como deficiencias legislativas que ya fueron tipificadas en este tipo de delitos cometidos, además pudimos evidenciar que nuestros legisladores no se dedicaron a regular de manera correcta e idónea aquellas contramedidas que constituyan un adecuado control pudiendo evidenciar la falta de interpretación de los operadores de justicia, es por ello que se debe considerar una modificatoria o reforma en la ley 30096.

Llegamos a la conclusión que existen consecuencias jurídicas para toda aquella persona que altere de manera ilegal el ingreso de datos en sistemas jurídicos y que esto tiene como resultado que todo ciberdelincuente que consuma el acto ilícito de alterar los sistemas jurídicos causando la afectación el bien jurídico tutelado será severamente reprimido con pena privativa de la libertad por el delito cometido de acuerdo a lo establecido por la ley 30096.

Concluimos en que la presente ley analizada si cumple con su rol preventivo y sancionador, pero lastimosamente aun a día de hoy no está diseñada para garantizar la lucha contra la ciberdelincuencia, además cabe resaltar que muchos de los operadores de justicia no hacen cumplir la ley 30096 por lo que no garantizan su rol preventivo y sancionador.

Concluimos en que la pena privativa de la libertad impartida por la ley 30096 de delitos informáticos para los ciberdelincuentes que cometen fraude informático es la adecuada, pero que la pena privativa de libertad impuesta en este tipo de delitos debería ser mayor de acuerdo a los agravantes de cada delito por lo cual el juzgador es aquel que deberá fijar una pena concreta en función del impacto del acto ilícito cometido, además que cabe recalcar que se consideró analizar a la tipicidad subjetiva en el presente delito para poder determinar si solamente comprende el análisis de la conducta dolosa y efectivamente pudimos evidenciar que comprende la conducta dolosa en todas sus modalidades, pero además existen más circunstancias y agravantes a determinar en cada caso de fraude informático, pero concluimos en que el fraude informático es un delito doloso es cual no admite modalidad culposa.

Se concluye dando a conocer que a raíz que van surgiendo nuevas modalidades para poder cometer este acto delictivo que atenta en contra el patrimonio y el bien jurídico tutelado la pena establecida en la ley 30096 no es la adecuada, es por ello que se recomienda que los legisladores puedan modificar o en su caso añadir nuevos artículos en el capítulo quinto de la presente ley que contemplen todas las nuevas modalidades de fraude informáticos qué aún no se ven contempladas en la ley.

4.2. Recomendaciones

Se recomienda que la Ley 30096 de delitos informáticos sea modificada, debido a que a día de hoy sigue teniendo vacíos legales y deficiencias legislativas referentes al capítulo quinto, precisamente en el artículo 8 el cual prescribe respecto al fraude informático que a todo ciberdelincuente que incurran en este tipo de delitos referentes al fraude informático deberían ser reprimidos con pena privativa de la libertad de acuerdo a la presente ley.

Como recomendación se pide a los operadores de justicia que consideren adecuadamente cuales son los criterios para realmente poder establecer una pena en los delitos de fraude informático contemplando todas sus modalidades, de igual forma determinar las circunstancias agravantes y atenuantes en el presente además de determinar la pena en base al bien jurídico afectado al momento de cometer fraude informático.

Se recomienda al gobierno poder implementar unidades fiscales especializadas en ciberdelitos a nivel nacional, en todas las regiones de país y no solo en lima norte, este y sur, esto con la finalidad de poder hacer efectiva y garantizar el rol preventivo y sancionador de la ley 30096 de delitos informáticos, de esta forma poder disminuir el índice de casos de ciberdelincuencia, debido a que tan solo en lima en los primeros meses del presente año la cifra de casos de este delito superaron los seis mil y aun no son resueltos más del 80% hasta el día de hoy.

REFERENCIAS

Alkhalil, Z. (2021) Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers. ttps://doi.org/10.3389/fcomp.2021.563060

Akamai, B. (2020). Informe sobre el Estado de Internet en materia de seguridad de Akamai. https://www.akamai.com/es/es/multimedia/documents/state-of-the-internet/soti-security-phishing-for-finance-report-2021.pdf

Alcívar, C. (2018). Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidad. http://www.revistaespacios.com/a18v39n42/a18v39n42p15.pdf

Alvarado, J. (2017) Análisis de las vulnerabilidades mediante el uso de phishing para mejorar la seguridad informática de los equipos de cómputo y redes de la Municipalidad distrital de Independencia [Tesis de posgrado, Universidad Nacional Santiago Antúnez de Mayolo] Repositorio Institucional UNASAM. http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2655/T033_46022813_M.pdf?sequence=1&isAllowed=y

Banco Interamericano de Desarrollo y Organización de los Estados Americanos, (2020). Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte Ciberseguridad 2020. Washington D.C. Obtenido de https://publications.iadb.org/es/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Blossiers, J. (2018). El delito informático y su incidencia en la empresa bancaria. Tesis de Maestría, Universidad Nacional Federico Villarreal. http://repositorio.unfv.edu.pe/handle/UNFV/2608

Congreso de la República del Perú. (2019). Ley que modifica la ley 30096, ley de delitos informáticos. Obtenido de https://leyes.congreso.gob.pe/Documentos/Leyes/30171.pdf

Defensoría del Pueblo, (2019). Por una atención policial de calidad con respeto de derechos fundamentales. Supervisión nacional de los departamentos de investigación criminal de la Policía 2018. Obtenido de https://www.defensoria.gob.pe/wp-content/uploads/2019/09/INFORME-DE-ADJUNT%C3%8DA-N%C2%B0-003-2019-DP-ADHPD-Supervisi%C3%B3n-Nacional-a-los-Departamentos-de-Investigaci%C3%B3n.pdf

Díaz, A. (2018). El Endurecimiento de las penas no disminuye la acción delictiva. Obtenido de https://derecho.usmp.edu.pe/sapere/ediciones/edicion_16/articulos/articulos_alumnos/endurecimiento_penas.pdf

Espinoza, M. (2017) Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control [Tesis de pregrado, Universidad Nacional del Antiplano] Repositorio Institucional UNAP. http://repositorio.unap.edu.pe/bitstream/handle/UNAP/6309/Espinoza_Coila_Michael.pdf?sequ

ence=1&isAllowed=y

Figueroa, E. (2018). Esencia de la Congruencia Procesal, El principio de Legalidad. Revista Jurídica. Obtenido de https://www.pj.gob.pe/wps/wcm/connect/728f5c004f2f714b90d5b8ecaf96f216/Principio+de+legalidad.pdf?MOD=AJPERES&CACHEID=728f5c004f2f714b90d5b8ecaf96f216.

Forbes. (2021). Covid-19 detona ciberataques en México: hasta 4 amenazas por segundo vía mail. https://www.forbes.com.mx/ciberataques-4-por-segundo-mexico-2020/

Guerrero, C. (2018). De Budapest al Perú: Análisis sobre el proceso de implementación del Convenio de ciberdelincuencia. Impacto en el corto, mediano y largo plazo. Lima, Hiperderecho y Derechos Digitales. Obtenido de https://www.derechosdigitales.org/wp-content/uploads/minuta_hiperderecho.pdf

Hancco, E. (2018). 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 [Tesis de pregrado, Universidad Nacional de San Agustín] Repositorio Institucional UNSA. http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/6436/DEhazaey.pdf?sequence=1&isAllowed=y

Hernández, R. (2018). Metodología de la Investigación. Recuperado de http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf

Herrera, E. (2017). El Phishing como delito informático y su falta de tipificación en el Código Orgánico Integral Penal [Tesis de pregrado, Universidad Central del Ecuador] Repositorio Institucional UCE. http://www.dspace.uce.edu.ec/bitstream/25000/8132/1/T-UCE-0013-Ab-399.pdf

Herrera, L. (2018) Eficacia de la ley de delitos informáticos en el distrito judicial de Huánuco 2017 [Tesis de pregrado, Universidad de Huánuco] Repositorio Institucional UDH. http://repositorio.udh.edu.pe/bitstream/handle/123456789/1058/HERRERA%20URSUA%2C%20Lesly%20Monica.pdf?sequence=1&isAllowed=y

Hiplán, S. (2019) La Ley 19.223 a 26 Años de su Promulgación [Tesis de grado, Universidad de Chile] Repositorio Institucional UCHILE. http://repositorio.uchile.cl/bitstream/handle/2250/173119/La-ley-N%C2%B019223-a-26-a%C3%B1os-de-su-promulgacion.pdf?sequence=1&isAllowed=y

Hugo, S. (2020). Tipificación de los delitos informáticos patrimoniales en la nueva Ley de delitos informáticos N° 30096. Alma Máter. https://revistasinvestigacion.unmsm.edu.pe/index.php/alma/article/view/11870

León, F. (2018). El Principio de proporcionalidad y la Jurisprudencia en el TC. Recuperado de https://www.mpfn.gob.pe/escuela/contenido/actividades/docs/2084_1_principio_proporcionalid

ad_y_jurisprudencia_tc_felipe_johan_leon_florian.pdf

López, J. (2019). Métodos y técnicas de detección temprana de casos de phishing [Tesis de posgrado, Universidad Oberta de Catalunya] Repositorio Institucional UOC. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/89225/6/jlopezsanchez012TFM0119memoria.pdf

Mayer, L. (2017). El bien jurídico protegido en los delitos informáticos. Scielo. https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-34372017000100011

Mesa, D. (2017). La ciberdelincuencia y sus consecuencias jurídicas. Obtenido de

https://uvadoc.uva.es/bitstream/handle/10324/26749/TFGD_0368.pdf?sequence=1&isAllowed=y

Moncada, A. (2020). Comparación de técnicas de machine learning para detección de sitios web de phishing. Revista Universidad de Lima. https://doi.org/10.26439/interfases2020.n013.4886

Mori, F. (2019). Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de lima, periodo 2008 al 2012. Obtenido de http://repositorio.unfv.edu.pe/handle/UNFV/3519

Oxman, N. (2021). Estafas informáticas a través de internet acerca de la imputación penal del "phishing" y el "pharming". Redalyc. https://www.redalyc.org/pdf/1736/173629692007.pdf

Paredes, J. (2019). De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el periodo 2009-2010 [Tesis de posgrado, Universidad Nacional Mayor de San Marcos] Repositorio Institucional UNMSM. http://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/10314/Paredes_pj.pdf?sequence=3&isAllowed=y

Pardo, A. (2018). Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018 [Tesis de posgrado, Universidad César Vallejo] Repositorio Institucional UCV. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf?sequence=1&isAllowed=y

Ruiz, T. (2020) Análisis de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos. Universidad Nacional de Loja - Ecuador https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Romero, M. (2017). Delitos informáticos cometidos a través de redes sociales y su tratamiento en el Ministerio Público en la ciudad de Huánuco, 2016. Obtenido de http://repositorio.udh.edu.pe/bitstream/handle/123456789/331/_047_%2025858529_T.pdf?sequence=1&isAllowed=y

Sánchez, D. (2020) Estudio teleológico del carding y bins. Su impunidad e impacto en el sistema mexicano [Tesis de pregrado, Bemérita Universidad Autónoma de Puebla] Repositorio Institucional BUAP.

https://repositorioinstitucional.buap.mx/bitstream/handle/20.500.12371/11702/20210223150451-5912-TL.pdf?sequence=2

Sánchez, J. (2017). Delitos informáticos. Academia de la Magistratura. http://repositorio.amag.edu.pe/bitstream/handle/123456789/623/MANUAL%20CURSO%20DELITOS%20INFORMATICOS.pdf?sequence=4&isAllowed=y

Sandín, M. (2019). Investigación Cualitativa en Educación. Fundamentos y tradiciones. Obtenido de https://www.academia.edu/5026577/Investigaci%C3%B3n_Cualitativa_en Educaci%C3%B3n_Fundamentos_y_tradiciones

Sequeiros, I. (2017) Vacíos legales que imposibilitan la sanción de los delitos informáticos en el Nuevo Código Penal Peruano - 2015 [Tesis de pregrado, Universidad de Huánuco] Repositorio Institucional UDH. http://repositorio.udh.edu.pe/bitstream/handle/123456789/286/IVETT%20CLARITZA%20SEQUEIROS%20CALDERON.pdf?sequence=1&isAllowed=y

Temitayo, O. (2018). The Impact of Fraud on the Performance of Deposit Money. Contenido de

file:///C:/Users/HP/Downloads/IJIFER-M-4-2018.pdf

Valle, J. (2019). El delito informático de phishing [Tesis de pregrado, Universidad Regional Autónoma de Los Andes] Repositorio Institucional UNIANDES. https://dspace.uniandes.edu.ec/bitstream/123456789/2819/1/TUQMDPC005-2013.pdf

Vega, J. (2017) Los delitos informáticos en el Código Penal [Tesis de grado, Universidad Católica de Santa María] Repositorio Institucional UCSM. http://tesis.ucsm.edu.pe/repositorio/bitstream/handle/UCSM/6824/88.0774.MG.pdf?sequence=1&isAllowed=y

Villavicencio, F. (2020). Delitos informáticos. Ius Et Veritas. http://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630/14253

Voraprane, E. (2018) “Enchancing the Security of Electronic commerce transactions” epartment of Mathematics Royal Holloway, University of London Egham, Surrey TW20 0EX, England. Recuperado de https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/5463/Le%C3%B3n%20Ochoa%20Yorli%20Adrian.pdf?sequence=1&isAllowed=y

Zorrilla, K. (2018). Inconsistencias y ambigüedades en la Ley de delitos informáticos Ley N° 30096 y su modificatoria Ley N° 30171, que imposibilitan su eficaz cumplimiento. http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2332/T033_70221905_T.pdf?sequence=1&isAllowe

ANEXOS

Anexo 1.- Resolución de aprobación de titulo

Universidad Señor de Sipán

FACULTAD DE DERECHO Y HUMANIDADES
RESOLUCIÓN N°1024-2022/FADHU-USS

Pimentel, 19 de octubre del 2022

VISTO:

El informe N° 0183-2022/FADHU-ED-USS de fecha 18 de octubre del 2022, presentado por la Escuela Profesional de Derecho, eleva el informe del docente de la asignatura de Investigación I el MG. MALDONADO GOMEZ RENZO JESUS, a fin de que se emita la resolución de aprobación del **Proyecto de Investigación (Tesis)** a cargo de los estudiantes registrados en el **semestre académico 2022-I**, Y,

CONSIDERANDO:

Que, la Constitución Política del Perú en su Artículo 18° establece que: *"La educación universitaria tiene como fines la formación profesional, la difusión cultural, la creación intelectual y artística y la investigación científica y tecnológica (...) Cada universidad es autónoma en su régimen normativo, de gobierno, académico, administrativo y económico. Las universidades se rigen por sus propios estatutos en el marco de la Constitución y de las leyes."*

Que, acorde con lo establecido en el Artículo 8° de la Ley Universitaria, Ley N° 30220, *"La autonomía inherente a las Universidades se ejerce de conformidad con lo establecido en la Constitución, la presente ley demás normativa aplicable. Esta autonomía se manifiesta en los siguientes regímenes: normativo, de gobierno, académico, administrativo y económico"*. La Universidad Señor de Sipán desarrolla sus actividades dentro de su autonomía prevista en la Constitución Política del Estado y la Ley Universitaria N° 30220.

Que, acorde con lo establecido en la Ley Universitaria N°30220, indica:

- Artículo N° 6°: Fines de la Universidad, Inciso 6.5) "Realizar y promover la investigación científica, tecnológica y humanística la creación intelectual y artística".

Según lo establecido en el Artículo 45° de la Ley Universitaria, Ley N° 30220, *"Obtención de Grados y Títulos; Para la obtención de grados y títulos se realiza de acuerdo a las exigencias académicas que cada universidad establezca en sus respectivas normas internas.*

Que, el Reglamento de Investigación de la USS Versión 8, aprobado con Resolución de Directorio N°015-2022/PD-USS, señala:

- Artículo 72°: Aprobación del tema de investigación: El Comité de Investigación de la escuela profesional eleva los temas del proyecto de investigación y del trabajo de investigación que esté acorde a las líneas de investigación institucional a Facultad para la emisión de la resolución.

- Artículo 73°: Aprobación del proyecto de investigación: El (los) estudiante (s) expone ante el Comité de Investigación de la escuela profesional el proyecto de investigación para su aprobación y emisión de la resolución de facultad.

Que, Reglamento de Grados y Títulos Versión 08 aprobado con resolución de directorio N° 020-2022/PD-USS, señala:

- Artículo 21°: "Los temas de trabajo de investigación, trabajo académico y tesis son aprobados por el Comité de Investigación y derivados a la facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El periodo de vigencia de los mismos será de dos años, a partir de su aprobación (...).

- Artículo 24°: *"La tesis, es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela académico profesional (...)".*

- Artículo 25°: *"El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C".*

Que, visto el informe N° 0183-2022/FADHU-ED-USS de fecha 18 de octubre del 2022, presentado por la Escuela Profesional de Derecho, eleva el informe del docente de la asignatura de Investigación I el MG. MALDONADO GOMEZ RENZO JESUS, a fin de que se emita la resolución de aprobación de los temas de Proyecto de Investigación (Tesis) a cargo de los estudiantes registrados en el **semestre académico 2022-I**, quienes cumplen con los requisitos, por lo que se debe proceder a su inscripción respectiva, con fines de sustentación.

Universidad Señor de Sipán

RESOLUCIÓN N°1024-2022/FADHU-USS

Estando a lo expuesto y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes.

SE RESUELVE:

ARTÍCULO PRIMERO APROBAR los **PROYECTOS DE INVESTIGACIÓN (TESIS)** de los estudiantes descritos en la lista que forma parte de la presente resolución.

N°	APELLIDOS Y NOMBRES	PROYECTOS DE INVESTIGACIÓN
1	YARLEQUE DAVILA KAREN MIRELLA	"ANÁLISIS DE LA EFICIENCIA EN LA EJECUCIÓN DE LAS MEDIDAS DE PROTECCIÓN POR ACTOS DE VIOLENCIA CONTRA LA MUJER, CHICLAYO 2022"
2	MAZA ODAR RUTH KARINA	"ANÁLISIS DE LOS CRITERIOS LEGALES Y JURISPRUDENCIALES APLICADOS A LA PENSIÓN ALIMENTICIA DE MENORES DE EDAD EN SITUACIÓN DE DISCAPACIDAD"
3	- NUÑEZ BENAVIDES LESLIE ANALI - OCUPA VIZCONDE SHEYLA LILIBETH	"CONSECUENCIAS JURÍDICAS DEL ALLANAMIENTO EN LOS PROCEDIMIENTOS ADMINISTRATIVOS DE PROTECCIÓN AL CONSUMIDOR ANTE INDECOPI, CHICLAYO 2020-2022"
4	QUEVEDO CASTILLO PABLO ARNULFO	"LA EJECUCIÓN DE LA PRISIÓN PREVENTIVA Y SU REGLA DE TRATAMIENTO EN LOS PROCESOS PENALES DE LAMBAYEQUE, 2017-2022"
5	- BALLONA RENTERIA DARWIN ALEXANDER - SANTISTEBAN YOCTUN JENIFER ESTEFANI	"EFICACIA DE LA APLICACIÓN DE LA MEDIDA SOCIOEDUCATIVA DE INTERNAMIENTO Y LA RESOCIALIZACIÓN DE LOS ADOLESCENTES INFRACTORES EN LAMBAYEQUE-2022"
6	- SUCHERO AGAPITO ROSA GIULIANNA - LLERENA DAVILA ROSALILA	"REGULACIÓN COMPLIANCE EN EL DELITO DE CONTAMINACIÓN AMBIENTAL COMETIDOS POR LAS PERSONAS JURÍDICAS SOCIETARIAS EN LA LEGISLACIÓN, CHICLAYO 2021- 2022"
7	MESTANZA LOPEZ STEFANIA ANDREA	"INEFICACIA DE MEDIDAS DE PROTECCIÓN Y EL INCREMENTO DE CASOS DE VIOLENCIA FÍSICA CONTRA LA MUJER EN MONSEFU, 2021"
8	- SANCHEZ MOLOCHO LISBETH NATALY - VASQUEZ SANTA CRUZ MERLING SHIRLEY	"EL CUMPLIMIENTO DE LAS MEDIDAS DE PROTECCIÓN EN EL ÁMBITO CIVIL POR AGRESIONES CONTRA LAS MUJERES, CHICLAYO, 2022"
9	- BUSTAMANTE CHAFLOQUE KIHARA PAOLA - CAJUSOL FIGUEROA YENNY	"ANALISIS DE ACTUACION PROCESAL DE REVOCACION DE COPARENTALIDAD SEGÚN LA MODIFICACION DEL ART. 84 DEL CODIGO DE NIÑOS Y ADOLESCENTES"
10	PEREZ QUINTANA NATALY ALEXANDRA	"ANÁLISIS DEL SISTEMA JURÍDICO PERUANO DE TRANSFERENCIA DE BIENES INMUEBLES Y LA SEGURIDAD JURÍDICA DEL ADQUIRIENTE MEDIANTE LA INSCRIPCIÓN REGISTRAL CHICLAYO, 2021-2022"
11	NANQUEN MACALOPU HERSSON OSWALDO	"EL BLOQUEO REGISTRAL EN LOS CONTRATOS DE COMPRAVENTA INMOBILIARIA FRENTE A LA CONCURRENCIA DE ACREEDORES, LAMBAYEQUE, 2022"
12	ROJAS MENDOZA PEDRO FRANCISCO	"LA CONCILIACIÓN EXTRAJUDICIAL Y SU EFICACIA EN LA DISMINUCIÓN DE PROCESOS JUDICIALES. CHICLAYO 2018-2022"
13	VASQUEZ OJEDA MANUEL RICARDO	"IMPLICANCIAS LABORALES EN ÉPOCA DEL COVID 19 EN LOS TRABAJADORES DE LA ACTIVIDAD PRIVADA, CHICLAYO, 2022 - 2023"
14	ALCANTARA DIAZ FABIAN EDUARDO	"ANÁLISIS DE LA LEY 30096 DE DELITOS INFORMÁTICOS EN SU APLICACIÓN A LOS DELITOS DE FRAUDE INFORMÁTICO EN EL PERÚ, 2022

15	DIAZ SANTISTEBAN MELISSA YARALI	"LA RESPONSABILIDAD DEL ESTADO FRENTE A LA REPARACIÓN CIVIL PARA RESARCIR LOS DAÑOS AMBIENTALES, CHICLAYO – 2022"
16	SANDOVAL MANAYAY JOSE MIGUEL	"LA EFICACIA DE LA LEY N° 30077, PARA CONTRARRESTAR EL CRIMEN ORGANIZADO, LAMBAYEQUE, (2020-2022)"
17	CASTILLO VASQUEZ HEYSER JUANA	"DERECHO A LA DEFENSA EN LA AUDIENCIA DE OTORGAMIENTO DE LA MEDIDAS DE PROTECCIÓN, CAYALTI - 2022"
18	- ZURITA GARCIA HARRY PAUL - BARCA CONTRERAS KARINA	"LA COLABORACIÓN EFICAZ Y SU IMPLICANCIA EN LA SOLICITUD DE LA PRISIÓN PREVENTIVA EN LOS CASOS DE ORGANIZACIÓN CRIMINAL, CHICLAYO, 2017- 2022"

ARTÍCULO SEGUNDO: DISPONER que las áreas competentes tomen conocimiento de la presente resolución con la finalidad de dar las facilidades para la ejecución de la presente Investigación.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Dra. Dioses Lescano Nelly
Decana de la Facultad de Derecho y Humanidades

Mg. Delgado Vega Paula Elena
Secretaria Académica Facultad de Derecho y Humanidades

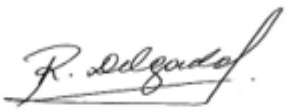
Anexo 2.- Acta de aprobación de asesor

Universidad Señor de Sipán

ACTA DE APROBACIÓN DEL ASESOR

Yo **Delgado Fernandez Rosa Elizabeth**. quien suscribe como asesor designado mediante Resolución de Facultad N° **1186-2022/FADHU-USS**, del proyecto de investigación titulado **"Análisis de la ley 30096 de delitos informáticos en su aplicación a los delitos de fraude informático en el Perú, 2022"**,, desarrollado por el estudiante: **Fabian Eduardo Alcantara Diaz**, del programa de estudios de la Escuela Profesional de Derecho y Humanidades de la Universidad Señor de Sipán S.A.C, acredito haber revisado, y declaro expedito para que continue con el trámite pertinentes.

En virtud de lo antes mencionado, firman:

Delgado Fernandez Rosa Elizabeth	DNI: 16452199	

Pimentel, 19 de marzo de 2024

Anexo 3.- Acta de Originalidad

Universidad Señor de Sipán

ACTA DE ORIGINALIDAD DE LA INVESTIGACIÓN

Yo, **Martha Olga Marruffo Valdivieso** coordinadora de investigación y Responsabilidad Social de la Escuela Profesional de Derecho, he realizado el segundo control de originalidad de la investigación, el mismo que está dentro de los porcentajes establecidos para el nivel de Pregrado según la Directiva de similitud vigente en USS; además certifico que la versión que hace entrega es la versión final de informe titulado.

"ANÁLISIS DE LA LEY 30096 DE DELITOS INFORMÁTICOS EN SU APLICACIÓN A LOS DELITOS DE FRAUDE INFORMÁTICO EN EL PERÚ, 2022"

Elaborado por la Bach. **ALCANTARA DIAZ FABIAN EDUARDO**. Se deja constancia que la investigación antes indicada tiene un índice de similitud del **15%,** verificable en el reporte final del análisis de originalidad mediante el software de similitud TURNITIN.

Por lo que se concluye que cada una de las coincidencias detectadas no constituyen plagio y cumple con lo establecido en la Directiva sobre índice de similitud de los productos académicos de investigación vigente.

Pimentel, 04 de Abril de 2024

Mg. Martha Olga Marruffo Valdivieso
Coordinadora de Investigación y Responsabilidad Social
Escuela Profesional de Derecho
DNI N° 43647439

Anexo 4.- Instrumento

Título: Análisis de la ley 30096 de delitos informáticos en su aplicación a los delitos de fraude informático en el Perú, 2022.

Indicaciones: El presente instrumento tiene como propósito recoger información respecto a la Ley 30096 de delitos informáticos en su aplicación a los delitos de fraude informático en el Peru, 2022, motivo por el cual se le solicita a su persona a responder las presentes preguntas con la mayor seriedad posible.

Nombre del Entrevistado:

Profesión:

Ocupación del entrevistado:

Genero: **Edad:**

Fecha: Chiclayo, ……de……del año 2022.

Hora de Inicio: …… Hora de finalización: …….

¿Sr. ……. Ud. da su consentimiento de la información brindada para efectos de que sus datos sean tratados exclusivamente para la tesis referente al Análisis de la ley 30096 de delitos informáticos en su aplicación a los delitos de fraude informático en el Perú, 2022?

Estimado entrevistado, tomando en cuenta su especialidad y experiencia en el ámbito del derecho penal, es relevante conocer su opinión sobre el tema materia de estudio.

Preguntas:

1. ¿Considera usted que existen consecuencias jurídicas al alterar el ingreso de datos de manera ilegal mediante sistemas

informáticos?

……

……

……
……..

2. ¿Considera usted que existen deficiencias o vacíos legales en la ley 30096 ley de delitos informáticos?

……
……
……
……
……

3 ¿Cree usted que deberían implementarse más unidades fiscales especializadas en ciberdelincuencia en todas las regiones del Perú?

……
……
……
……
……

4. ¿Cree usted que para alterar o dar un mal uso a sistemas o software con propósitos fraudulentos se requiere de un alto nivel de conocimiento informático en los delitos relacionados al fraude cibernético?……
……
……
……

5. ¿Considera usted que la ley 30096 previene y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal?

……
……
……
……

6. ¿Cree usted que la ley 30096 cumple con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia?.……

……
……
……
……
……

7. ¿Considera usted la efectividad de la Ley 30096 al momento de sancionar a los ciberdelincuentes por los delitos ocasionados de fraude informático?……
……
……
……
……

8. ¿Considera usted que la pena privativa de libertad impuesta a los ciberdelincuentes que cometen delitos de fraude informático es la
correcta?……
……
……
……
……

9. ¿Considera usted que la tipicidad subjetiva en el delito de fraude informático comprende solo el análisis de la conducta dolosa?
……
……
……
……
……

10. ¿Cuáles son los criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático?
……
……

Firma del entrevistado

(Nombre del entrevistado)

DNI:

Firma del entrevistador

Fabian Eduardo Alcantara Diaz

DNI: 75556039

Anexo 5.- Validación del instrumento

FICHA DE VALIDACION DE INSTRUMENTO POR JUICIO DE EXPERTOS

1.	**NOMBRE DEL EXPERTO**	MG. JUAN MANUEL CALDERON SECLEN
2.	**PROFESIÓN**	ABOGADO
	ESPECIALIDAD	ABOGADO
	GRADO ACADEMICO	MAGISTER
	EXPERIENCIA PROFESIONAL	15
	CARGO	ABOGADO LITIGANTE

TESIS

TITULO DE LA INVESTIGACION:
"ANÁLISIS DE LA LEY 30096 DE DELITOS INFORMÁTICOS EN SU APLICACIÓN A LOS DELITOS DE FRAUDE INFORMÁTICO EN EL PERÚ, 2022"

3. DATOS DEL TESISTA	
3.1 NOMBRES Y APELLIDOS	**1.** Alcantara Diaz Fabian Eduardo
3.2 ESCUELA PROFESIONAL	DERECHO
4. INSTRUMENTO EVALUADO	1. Entrevista (X) 2. Cuestionario ( ) 3. Lista de Cotejo ( ) 4. Diario de campo ( )
5. OBJETIVO DEL INSTRUMENTO	GENERAL: Analizar la aplicación de la ley 30096 de delitos informáticos para prevenir los delitos de fraude informático en el Perú, 2022. ESPECIFICOS: Identificar los vacíos legales y omisiones que posee la ley 30096 de delitos informáticos en función al delito de

	fraude cibernético. Definir si la ley 30096 cumple adecuadamente con su rol preventivo y sancionador en relación al delito de fraude informático. Determinar si se deberían implementar más unidades fiscales especializadas en ciberdelincuencia en todas las regiones del país para garantizar la eficacia de la ley 30096.
A continuación se detallara los indicadores en forma de pregunta o propuestas para que usted los evalue marcando con un aspa (x) en "A" si está de ACUERDO o en "D" si está en DESACUERDO, SI ESTA EN DESACUERDO POR FAVOR ESPECIFIQUE SUS SUGERENCIAS	

N° 6. DETALLE DE LOS ITEMS DEL INSTRUMENTO	**ALTERNATIVAS**
1. ¿Considera usted que existen consecuencias jurídicas al alterar el ingreso de datos de manera ilegal mediante sistemas informáticos?	A (X) D ( ) Sugerencias…… …… ……
2.- ¿Considera usted que existen deficiencias o vacíos legales en la ley 30096 ley de delitos informáticos ?	A (X) D ( ) Sugerencias…… …… ……
3.- ¿Considera usted que deberían implementarse más unidades fiscales especializadas en ciberdelincuencia en todas las regiones del Peru?	A(X) D ( ) Sugerencias…… …… ……
4. ¿Cree usted que para alterar o dar un mal uso a sistemas o software con propósitos fraudulentos se requiere de un alto nivel de conocimiento informático en los delitos relacionados al fraude cibernético?	A(X) D ( ) Sugerencias…… …… ……
5. ¿Considera usted que la ley 30096 previene y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal?	A (X) D ( ) Sugerencias…… …… ……
6.- ¿Cree usted que la ley 30096 cumple con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia?	A (X) D ( ) Sugerencias…… …… ……
7.- ¿Considera usted la efectividad de la Ley 30096 al momento de sancionar a los ciberdelincuentes por los delitos ocasionados de fraude informático?	A (X) D ( ) Sugerencias…… …… ……
8.- ¿Considera usted que la pena privativa de libertad impuesta a los ciberdelincuentes que cometen delitos de fraude informático es la correcta?	A (X) D ( ) Sugerencias…… …… ……

9.- ¿Considera usted que la tipicidad subjetiva en el delito de fraude informático comprende solo el análisis de la conducta dolosa?	A (X) D ( ) Sugerencias…… …… ……
10.- ¿Cuáles son los criterios para establecer la pena y circunstancias agravantes en el delito de fraude informático?	A (X) D ( ) Sugerencias…… …… ……
PROMEDIO OBTENIDO:	A (X) D ( )
7. COMENTARIOS GENERALES **----------Listo para ser aplicado----------**	
8. OBSERVACIONES: **NINGUNA**	

……

FIRMA DEL EXPERTO

Anexo 6.- Autorización para recojo de información

CARTA DE AUTORIZACION PARA EL RECOJO DE LA INFORMACIÓN

Pimentel, 21 de diciembre de 2023

Quien suscribe:

Mg. Abg. Juan Manuel Calderon Seclen

Representante Legal

AUTORIZA: Permiso para recojo de información en función del proyecto de investigación, denominado "Análisis De La Ley 30096 De Delitos Informáticos En Su Aplicación A Los Delitos De Fraude Informático En El Perú, 2022"

Por el presente, el que suscribe Juan Manuel Calderon Seclen, abogado penalista laborando en el distrito de Chongoyape, provincia de Chiclayo departamento de Lambayeque, Perú, AUTORIZO al estudiante Fabián Eduardo, Alcántara Díaz, identificado conDNI 75556039, estudiante del Programa de Estudios de DERECHO y autor del trabajo de investigación denominado "Análisis De La Ley 30096 De Delitos Informáticos En Su Aplicación A Los Delitos De Fraude Informático En El Perú, 2022" al uso de dicha información que conforma el expediente técnico así como hojas de memorias, cálculos entre otros como planos para efectos exclusivamente académicos de la elaboración de tesis, enunciada líneas arriba de quien solicita se garantice la absoluta confidencialidad de la información solicitada.

Atentamente.

Anexo 7.- Matriz de consistencia

TÍTULO: Análisis de la ley 30096 de delitos informáticos en su aplicación a los delitos de fraude informático en el Perú, 2022.

AUTOR: Fabian Eduardo Alcantara Diaz

<table>
<tr><th>PROBLEMAS</th><th>OBJETIVOS</th><th colspan="2">CATEGORIZACIÓN</th><th>METODOLOGÍA</th></tr>
<tr><td>PROBLEMAGENERAL</td><td>OBJETIVO GENERAL</td><td colspan="2">1. CATEGORÍA
Ley 30096 de delitos informáticos</td><td>ENFOQUE
Cualitativo</td></tr>
<tr><td rowspan="2">¿Es posible la aplicación de la ley 30096 para prevenir los delitos de fraude informático en el Perú, 2022?</td><td rowspan="2">Analizar la aplicación de la ley 30096 de delitos informáticos para prevenir los delitos de fraude informático en el Perú, 2022.</td><td colspan="2" rowspan="2"><table><tr><th>Sub Categorías:</th><th>Indicadores</th></tr><tr><td>Deficiencias legislativas de la ley 30096</td><td>Análisis de la ley 30096</td></tr><tr><td>Reglamentación de la ley 30096</td><td>Código Penal Peruano</td></tr></table></td><td>Cualitativo
Tipo de Investigación
Básica</td></tr>
<tr><td>PROBLEMAS ESPECÍFICOS</td><td>OBJETIVOS ESPECÍFICOS</td><td>Nivel de Investigación
Descriptivo
Diseño
No experimental
Población
Representantes del Ministerio Público, y abogados penalistas especialistas en la materia.</td></tr>
<tr><td>PROBLEMA ESPECÍFICO 01:
¿Existen vacíos legales y omisiones que posee la ley 30096 de delitos informáticos en función al delito de fraude cibernético?

PROBLEMA ESPECÍFICO 02:
¿La ley 30096 cumple adecuadamente con su rol preventivo y sancionador en relación al delito de fraude informático?

PROBLEMA ESPECÍFICO 03:
¿Se deberían implementar más unidades fiscales especializadas en ciberdelincuencia en todas las regiones del país para garantizar la eficacia de la ley 30096?</td><td>OBJETIVO ESPECÍFICO 01:

Identificar los vacíos legales y omisiones que posee la ley 30096 de delitos informáticos en función al delito de fraude cibernético.

OBJETIVO ESPECÍFICO 02:

Definir si la ley 30096 cumple adecuadamente con su rol preventivo y sancionador en relación al delito de fraude informático.

OBJETIVO ESPECÍFICO 03:
Determinar si se deberían implementar más unidades fiscales especializadas en ciberdelincuencia en todas las regiones del país para garantizar la eficacia de la ley 30096.</td><td colspan="2">2. CATEGORÍA:
Delito de fraude informático

<table><tr><th>Sub Categorías:</th><th>Indicadores</th></tr><tr><td>Conducta ilícita del ciberdelincuente</td><td>Ley 30096</td></tr><tr><td>Elementos del delito de fraude informático</td><td>Código Penal Peruano</td></tr></table></td><td>Técnicas de Recolección de Datos
Entrevista
Instrumentos de Recolección de Datos
- Guía de Entrevista</td></tr>
</table>