Universidad César Vallejo

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Perspectivas y desafíos legales en la prevención de delitos informáticos y delincuencia organizada transnacional en el Perú: Implicancias de la Ley N° 30096

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTORES

Córdova Zapata, Francisco Arturo (orcid.org/0000-0001-7856-5368)

Rosas Ramírez, Edith Elena (orcid.org/0000-0001-6861-455X)

ASESOR

Mgtr. Chávez Suarez, Giancarlo Renán (orcid.org/0000-0001-8053-6136)

LÍNEA DE INVESTIGACIÓN

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

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA

Fortalecimiento de la democracia, liderazgo y ciudadanía.

LIMA - PERÚ

2023

Dedicatoria

En agradecimiento al esfuerzo de nuestros padres, por su apoyo incondicional en todo momento. Asimismo, dedicamos esta tesis a quienes nos brindaron un apoyo durante el camino recorrido, para lograr cumplir nuestra meta.

Agradecimiento

A cada docente que nos brindó su tiempo y sus conocimientos durante el tiempo que permanecimos en aulas, y a las instituciones que mediante sus especialistas nos apoyaron para realizar el presente trabajo de investigación.

ACTA DE DECLARATORIA DE AUTENCIDAD DEL ASESOR

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES
ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Autenticidad del Asesor

Yo, CHAVEZ SUAREZ GIANCARLO RENAN, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, asesor de Tesis titulada: "Perspectivas y desafíos legales en la prevención de delitos informáticos y delincuencia organizada transnacional en el Perú: Implicancias de la Ley N° 30096", cuyos autores son CORDOVA ZAPATA FRANCISCO ARTURO, ROSAS RAMIREZ EDITH ELENA, constato que la investigación tiene un índice de similitud de 7.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 08 de Enero del 2024

Apellidos y Nombres del Asesor:	**Firma**
CHAVEZ SUAREZ GIANCARLO RENAN **DNI:** 46877136 **ORCID:** 0000-0001-8053-6136	Firmado electrónicamente por: GRCHAVEZS el 08-01-2024 22:37:29

Código documento Trilce: TRI - 0727376

INVESTIGA UCV

ACTA DE DECLARATORIA DE ORIGINALIDAD DE LOS AUTORES

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES
ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Originalidad de los Autores

Nosotros, CORDOVA ZAPATA FRANCISCO ARTURO, ROSAS RAMIREZ EDITH ELENA estudiantes de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, declaramos bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Perspectivas y desafíos legales en la prevención de delitos informáticos y delincuencia organizada transnacional en el Perú: Implicancias de la Ley N° 30096", es de nuestra autoría, por lo tanto, declaramos que la Tesis:

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

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

Nombres y Apellidos	**Firma**
FRANCISCO ARTURO CORDOVA ZAPATA **DNI:** 40001282 **ORCID:** 0000-0001-7856-5368	Firmado electrónicamente por: FCORDOVAZ el 08-01-2024 15:24:42
EDITH ELENA ROSAS RAMIREZ **DNI:** 09569588 **ORCID:** 0000-0001-6861-455X	Firmado electrónicamente por: EEROSASR el 08-01-2024 15:27:09

Código documento Trilce: TRI - 0727340

INVESTIGA UCV

ÍNDICE DE CONTENIDOS

Carátula…… ……i
Dedicatoria……..…….…… …ii
Agradecimiento..…….iii
Declaratoria de autenticidad del asesor…..……..……iv
Declaratoria de originalidad de los autores……..……v
Índice de contenidos vi
Índice de tablas vii
Índice de figuras viii
Resumen.....ix
Abstract x
I **INTRODUCCIÓN**..... 1
II **MARCO TEÓRICO**..... 4
III **METODOLOGÍA**..... 10
3.1 Tipo y diseño de la investigación. 10
3.2 Categorías, subcategorías y matriz de categorización..... 10
3.3 Escenario de estudio..... 12
3.4 Participantes 12
3.5 Técnicas e instrumentos de recolección datos..... 13
3.6 Procedimientos 13
3.7 Rigor Científico..... 16
3.8 Método de análisis de datos..... 16
3.9 Aspectos éticos 16
IV **RESULTADOS Y DISCUSIÓN**..... 17
V **CONCLUSIONES**..... 37
VI **RECOMENDACIONES**..... 38
REFERENCIAS..... 39
ANEXOS …… 45

ÍNDICE DE TABLAS

Tabla 1: Matriz de categorización y subcategorización……11

Tabla 2: Proceso de selección de expertos……12

Tabla 3: Criterios de inclusión y exclusión de los participantes……..13

Tabla 4. Codificación de entrevistados……15

Tabla 5: Codificación de artículos de investigación científica…….24

Tabla 6: Codificación de tesis nacionales e internacionales……..27

Tabla 7: Tabla de origen……29

ÍNDICE DE FIGURAS

Fig. N° 1 Delitos Informáticos en el Perú según la DIVINDAT……4

Fig. N° 2 Tipos de Delitos Informáticos en el Perú……6

Fig. N° 3 Flujograma de fuente documental……..14

Fig. N° 4 Aplicación de medidas judiciales……17

Fig. N° 5 Recursos y capacidades de las instituciones……..18

Fig. N° 6 Ámbito de aplicación……18

Fig. N° 7 Creación de autoridades y agencias específicas……19

Fig. N° 8 Asignación de recursos……19

Fig. N° 9 Desarrollo de normativas y directrices……..20

Fig. N° 10 Tipificación de los delitos informáticos en el Perú……...20

Fig. N° 11 Tasa de delitos informáticos……21

Fig. N° 12 Capacidad de investigación y procesamiento……..22

Fig. N° 13 Cumplimiento empresarial……..22

Fig. N° 14 Naturaleza de la delincuencia organizada transnacional……..23

RESUMEN

En nuestro país, los delitos informáticos son realizados mediante tecnologías de información, lo que vulnera la seguridad en el desenvolvimiento personal de los individuos; los delitos informáticos que se emplean y las diferentes acciones que se toman para combatirlos están en la Ley de Delitos Informáticos Nº 30096, sin embargo, estos delitos también son cometidos por bandas organizadas transnacionales, las cuales operan desde cualquier parte del mundo sin tener fronteras que las detenga, valiéndose de la modernidad de la tecnología con respecto a los sistemas cibernéticos, usando esta tecnología para realizar fraudes informáticos. En la actualidad existen diferentes tipos de fraudes que atentan contra la seguridad del estado, sus diferentes instituciones y a las personas que utilizan las diferentes redes para desenvolverse o hacer trabajos cotidianos.

De manera que, el objetivo general fue: Determinar cuál es el impacto de la Ley N° 30096 en la mitigación de delitos informáticos y la lucha contra la delincuencia organizada transnacional en el contexto peruano. Por lo tanto, los objetivos específicos de la tesis fueron: a) Analizar de qué manera ha contribuido la Ley N° 30096 a la reducción de delitos informáticos en el Perú y a la desarticulación de grupos de delincuencia organizada transnacional; b) Analizar cuáles son los principales desafíos y limitaciones legales que enfrenta la aplicación de la Ley N° 30096 en la prevención y persecución de delitos informáticos y la delincuencia organizada transnacional en el país.

Palabras clave: Fraude, delitos informáticos, tecnología, riesgos informáticos, modalidades delictivas.

ABSTRACT

In our country, computer crimes are carried out through information technologies, which violates the security in the personal development of individuals; The computer crimes that are used and the different actions that are taken to combat them are in the Computer Crime Law Nº 30096, however, these crimes are also committed by transnational organized gangs, which operate from anywhere in the world without having borders. to stop them, using the modernity of technology with respect to cybernetic systems, using this technology to carry out computer fraud. Currently, there are different types of fraud that threaten the security of the state, its different institutions and the people who use different networks to function or do daily work.

Therefore, the general objective was to determine the impact of Law Nº 30096 on the mitigation of computer crimes and the fight against transnational organized crime in the Peruvian context. Therefore, the specific objectives of the thesis were: a) Analyze how Law Nº 30096 has contributed to the reduction of computer crimes in Peru and the dismantling of transnational organized crime groups; b) Analyze what are the main challenges and legal limitations faced by the application of Law Nº 30096 in the prevention and prosecution of computer crimes and transnational organized crime in the country.

Keywords: Fraud, computer crimes, technology, computer risks, criminal modalities.

I INTRODUCCIÓN

Para el desarrollo de la presente tesis ha sido importante analizar los datos recolectados por el Diario Oficial El Peruano, el cual señala que en nuestro país existe un alto índice de delitos cibernéticos, de acuerdo a las estadísticas recogidas del Observatorio Nacional de Política Criminal del Ministerio de Justicia y Derechos Humanos, durante el año 2021 en el Ministerio Público, se recibieron 18,596 denuncias por fraudes informáticos, esto simboliza un considerable crecimiento de 92.9% con respecto al año 2020; adicionalmente durante el año 2021 la Policía Nacional del Perú registro 14,671 denuncias por fraudes informáticos, lo que representó un incremento del 65% de casos con respecto al año 2020; Una de las regiones con mayor índice de denuncias por este tipo de delito es Lima con 7,324 casos. Mientras que en la región de Arequipa se registraron 877 denuncias, en la Libertad 835 y en la provincia constitucional del Callao 774. (Diario Oficial El Peruano, 2023).

Acorde a lo mencionado anteriormente los delitos informáticos no solo se cometen en nuestro país, sino que también existe delincuencia organizada transnacional que comete estos fraudes informáticos desde cualquier parte del mundo, la Organización Internacional de la Policía (INTERPOL), manifiesta que, durante el año 2022 se realizó una encuesta de las diferentes modalidades más recurrentes en delincuencia internacional, que fueron enviados por los países que integran la INTERPOL, se notificaron 60,000 denuncias de delitos internacionales, entre los más frecuentes son: terrorismo, **ciberdelitos**, delitos financieros /corrupción, tráfico ilícito, y **delincuencia organizada**. De acuerdo al presente informe estos cinco (5) tipos de delitos internacionales se han incrementado. (INTERPOL, 2022).

En ese sentido, la División de Estafas y Otras Defraudaciones (DIVIEOD), cumple con la función principal de investigar y denunciar los diversos delitos informáticos, siendo los más usados la suplantación de identidad para obtener información bancaria, Phishing, Carding, SIM Swapping, Thief Transfer, entre otros. Para tal efecto se creó la Ley de Delitos Informáticos Nº 30096, con la finalidad de prevenir y sancionar la actividad ilegal que ocasionen los fraudes informáticos que

produzcan perjuicio económico tanto a las personas como al Estado peruano. Para Custodio, ante las nuevas modalidades delictivas, surge la necesidad de que las normas legales estén de acuerdo con los delitos que se comenten actualmente en nuestra sociedad, con el fin de garantizar la sanción del delito cometido (Custodio, 2021).

Sin embargo, por el incremento de fraudes informáticos realizado por bandas organizadas transnacionales, nuestro país se suscribió al convenio de Budapest, debido a que los delitos informáticos van en continuo apogeo e incluso se pueden cometer desde cualquier parte del mundo, dicho convenio promueve la colaboración internacional para combatir estos ilícitos. Según Huamán, el constante avance de la tecnología que permite el desarrollo tanto económico como social de las personas, ha motivado que los delincuentes se perfeccionen en estos rubros, creando nuevas formas de cometer delitos informáticos (Huamán, 2018).

Por lo tanto, se considera que la Ley de Delitos Informáticos N°. 30096 que fue creada para combatir dichos delitos no va acorde con las nuevas formas de fraude informático, ya que realmente no considera del todo las conductas delictivas que son cometidas desde el interior como del exterior del país, quedando muchas de ellas sin sanción.

Por lo anteriormente expuesto, planteamos la siguiente interrogante. ¿Cuál es el impacto de la Ley N° 30096 en la mitigación de delitos informáticos y la lucha contra la delincuencia organizada transnacional en el contexto peruano? De la misma forma, los problemas específicos planteados son: a) ¿De qué manera ha contribuido la Ley N° 30096 a la reducción de delitos informáticos en el Perú y a la desarticulación de grupos de delincuencia organizada transnacional?; b) ¿Cuáles son los principales desafíos y limitaciones legales que enfrenta la aplicación de la Ley N° 30096 en la prevención y persecución de delitos informáticos y la delincuencia organizada transnacional en el país?

El objetivo general fue: Determinar Cuál es el impacto de la Ley N° 30096 en la mitigación de delitos informáticos y la lucha contra la delincuencia organizada transnacional en el contexto peruano. Por lo tanto, los objetivos específicos de la tesis fueron: a) Analizar de qué manera ha contribuido la Ley N° 30096 a la

reducción de delitos informáticos en el Perú y a la desarticulación de grupos de delincuencia organizada transnacional; b) Analizar cuáles son los principales desafíos y limitaciones legales que enfrenta la aplicación de la Ley N° 30096 en la prevención y persecución de delitos informáticos y la delincuencia organizada transnacional en el país.

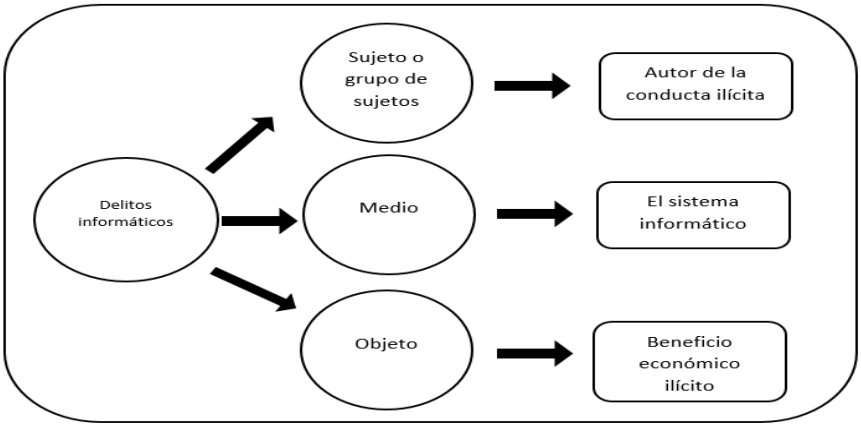
En conclusión, se desarrollaron las siguientes hipótesis de investigación, siendo la hipótesis general: Existe una mitigación de delitos informáticos y la lucha contra la delincuencia organizada transnacional en el contexto peruano, al aplicar la Ley N° 30096; además se formula las hipótesis específicas: a) la Ley N° 30096 contribuye a la reducción de delitos informáticos en el Perú y a la desarticulación de grupos de delincuencia organizada transnacional**;** b) los desafíos y limitaciones legales que enfrenta la aplicación de la Ley N° 30096, mejorara la prevención y persecución de delitos informáticos y la delincuencia organizada transnacional en el país.

II MARCO TEÓRICO

El continuo avance de la tecnología fomento el uso de computadoras y los programas informáticos para diversos fines, lo cual ha permitido el progreso tecnológico que está avanzado rápidamente, pero nos hacen más dependientes de la tecnología, la pandemia contribuyó a un mayor uso de la tecnología informática, muchos se vieron forzados a actualizarse y otros lograron afianzar más sus conocimientos. Actualmente su uso es más amplio abarcando los centros de trabajo, el hogar, centros de esparcimiento y en cualquier lugar que tenga conexión a internet, situación que es aprovechada por los delincuentes para lograr un beneficio negativo.

Figura 1:

Delitos Informáticos



Arellano y Galindo mencionan que la Ley N° 30096 tiene fallas legislativas en la identificación de los delitos informáticos orientados a la estafa, si bien define la tipicidad e ilegalidad de los delitos de estafa informática, las disposiciones antes mencionadas carecen de protección para las víctimas de los delitos de estafa informática, debido a que no establece que las víctimas deben detectar la prevención o las medidas de protección que podrían tomarse después de un ataque, y la ausencia de obstáculos burocráticos en el proceso de identificación de beneficiarios a quienes los titulares de cuentas bancarias realizaron transferencias bancarias no autorizadas, son todos consistentes con el objetivo de presentar cargos penales contra los sospechosos eludiendo una investigación preliminar por

la falta de personalidad del sospechoso, lo que se convierte en una de las causales para abrir un caso y proceder con impunidad en la investigación (Arellano y Galindo, 2022 p. 102) siguiendo la misma línea nuestras autoridades están en desventaja contra estas nuevas formas de delitos realizados en el ciberespacio por la falta de preparación y de tecnologías adecuadas para combatir estas modalidades de delitos.

De acuerdo a los autores Vega y Arévalo en nuestra nación no se ha creado una ley especifica que se refiera en concreto a definir la palabra ciberdelincuencia, por el contrario, para regular los delitos realizados en el ciberespacio se les ha definido como delitos informáticos. Esa terminología nace con la publicación de la ley N° 27309, esta ley integra los nuevos ilícitos informáticos a nuestro Código Penal, que es la primera ley en tratar e incorporar estos ilícitos en nuestro Código Penal, perdurando en el tiempo y luego promulgándose la Ley N° 30096. Ley de Delitos Informáticos, y aprobándose su reforma con la Ley N° 30171, en pocas palabras, en nuestro país no existe el termino ciberdelitos y ciberdelincuencia en la norma, pero si el termino delitos informáticos (Vega y Arévalo, 2022). Por esta razón, en nuestro ordenamiento jurídico es necesario la implementación de nuevos tipos penales relacionados a la ciberdelincuencia transnacional.

Olivares y Ceras indican que en la norma penal peruana existe un requerimiento de instrucción para policiales y Fiscales de nuestro país debido al incumplimiento de los principios penales de sanción o razonabilidad de los delitos de hurto de carácter informático, así como los relacionados con sabotaje informático y fraude cibernético, a pesar de la presencia de evidencia digital, existe una necesidad urgente de funcionarios para atrapar a estos delincuentes que están causando un gran daño a personas y empresas en diferentes industrias. Se necesita implementar urgentemente leyes adecuadas para repeler la delincuencia cometida en el ciberespacio, y que obstaculizan el progreso científico y profesional (Olivares y Ceras 2021, p. 22). Por ende, es necesario que existan nuevas políticas por parte de las autoridades, para poder capacitar a nuestra policía, operadores de justicia y dotarlos de equipos modernos.

Por otro lado, los autores Acosta et al, refiere que los delitos informáticos se realizan cuando se sustrae información de una o varias personas usando el

ciberespacio, creando una problemática que atenta contra la tranquilidad de nuestra sociedad, causando daños en el patrimonio de los individuos como de las organizaciones del estado y privadas producto de detraer estos datos, usualmente esta clase de delitos se realiza desde fuera del país, por lo que requiere que las autoridades actúen rápidamente, por lo tanto, se requiere que nuestras normas se actualicen de acuerdo al delito cometido y que se dé una adecuada protección a la información en el ciberespacio (Acosta et al, 2020). por otra parte, es necesario saber cómo están conformadas estas organizaciones delictivas.

para el autor Espinoza, la ciberdelincuencia es un nuevo desafío para nuestra normativa en derecho penal, también representa nuevos retos tanto para la Policía Nacional como para la Fiscalía y nuestro sistema judicial, que muchas veces son burlados por estos delincuentes que operan en el ciberespacio desde cualquier parte del mundo, estos delincuentes son especialistas y tienen conocimiento en informática, mientras que nuestras autoridades muchas veces no tienen conocimiento en informática. (Espinoza, 2022).

Figura 2:

Tipos de Delitos Informáticos en Perú

Adicionalmente, Huamán señala que ante la situación del ciberdelito, los diferentes países comunidad internacional han respondido con diferentes reuniones que han dado lugar a acuerdos, métodos, principios y alternativas para solucionar los problemas que generan los nuevos delitos, la probabilidad de que puedan ser cometidos desde algún lugar del mundo o porque la información está en servidores que se encuentran en distintos países, por lo que a quién lleva a cabo la investigación, le crea una serie de problemas tales como la normatividad y la jurisdicción que le corresponde (Huamán, 2020). Luego de que se incrementaran los delitos informáticos en diferentes países, estos optaron por reunirse para poder tratar esta problemática, dando lugar a diferentes acuerdos.

La ciberdelincuencia en el Perú: estrategias y retos de estado Diferentes instituciones internacionales, como la Organización de las Naciones Unidas o el Banco Interamericano de Desarrollo, han efectuado un estudio en los diferentes países del mundo sobre la ciberdelincuencia, los resultados que se encontraron de nuestro país arroja una problemática que se incrementa y no se puede controlar, relacionadas a la baja asignación de recursos tanto económicos como humanos que se asignan a las diferentes instituciones que combaten estos delitos. (La ciberdelincuencia en el Perú: estrategias y retos de estado, 2023). De acuerdo a la internacionalización de estos delitos por las bandas internacionales que buscan expandirse, estos delitos son tratados por la comunidad internacional por medio de sus diferentes acuerdos.

Mientras que, el autor Devia define que el ciberdelito es tratado por las autoridades de diversos países, así como también por organizaciones internacionales con el fin de reforzar el apoyo entre los países, así como la concordancia en la normatividad penal para combatir los delitos informáticos. Actualmente en nuestras vidas ya no podemos dejar la tecnología, lo que implica el uso de estas nuevas herramientas para cometer delitos que van cada vez en aumento, representando un riesgo y perjuicio para el agraviado ya que la normas no abarcan todos los tipos de delitos informáticos. Ante lo cual surge la necesidad de una calificación exclusiva para los delitos informáticos (Devia, 2017). Al igual estas organizaciones solo buscan obtener una economía ilícita y muchas veces un reconocimiento entre las bandas delictivas.

Paredes menciona, las organizaciones criminales están estimuladas por obtener beneficios económicos ilícitos, obteniendo estas ganancias de los mercados donde existe un flujo económico amplio, estas organizaciones están diseñadas y estructuradas como pequeñas empresas para poder operar y obtener un lucro de la forma ilícita, de esta forma pueden minimizar los riesgos. Estas organizaciones suelen ofrecer bienes y servicios de forma fraudulenta, muchas veces de forma violenta, el corazón de estas organizaciones son muchas veces familias que se dedican a estos actos ilícitos, las formas de operación de estas redes criminales son la de financiar a los políticos los cuales cuando llegan al poder, retribuyen a estas organizaciones delictivas. (Paredes, 2023). Por esta razón nuestro país se unió al convenio de Budapest para fortalecer sus leyes en contra de estos delitos informáticos.

Tenorio manifiesta que, desde el establecimiento de la Convención de Budapest sobre Ciberdelincuencia en el 2001, el gobierno peruano se unió al Convenio, siendo importante la adecuación de la norma. De la misma manera, era notoria la necesidad de un ente que encabezara, brindara los lineamientos a implementar y fomentara Nuevos proyectos relacionados con el ciberespacio, las tecnologías (Tenorio 2018).

Por su parte, el autor Rodríguez señala que los mecanismos utilizados por las instituciones públicas y privadas para garantizar la seguridad de los datos personales, y estos no sean sustraídos desde cualquier parte del planeta, son denominadas medidas de seguridad, si estas no existieran sería muy difícil proteger esta información violándose el derecho a proteger nuestros datos personales (Rodríguez, 2020). Por otra parte, estas instituciones están obligadas a dar una protección a los datos personales.

Para la autora Chauca, señala que la finalidad es que, algunas tienen como fin el enriquecimiento es decir buscan obtener dinero en grandes cantidades, otras buscan ser reconocidas en el bajo mundo como entidades criminales efectivas, otras buscan llegar al poder mediante la política, se caracterizan por la personalidad de sus integrantes, por sus habilidades, conocimientos, son personas ambiciosas de poder sin respeto hacia las demás personas, pero aun así son consideradas piezas reemplazables dentro de la organización, además suelen contar con

personas que no integran las organizaciones, pero son útiles para desempeñar otras actividades importantes que permite la sobrevivencia de la organización (Chauca, 2019). De la misma forma, por el desarrollo de la tecnología se crean nuevos riesgos que conllevan a nuevas formas de delitos informáticos.

Para Daza, en la actualidad, el avanzado desarrollo tecnológico, en un mundo integrado y el desarrollo de diferentes tecnologías que crean nuevos riesgos, recientemente han brotado nuevos delitos cibernéticos que amenazan la seguridad de un país, por esta razón las fronteras deben limitar estos actos, siendo un filtro para evitar etas acciones delincuenciales, a la fecha representa un enlace para permitir el acceso de estas bandas organizadas hacia los países (Daza, 2020). De igual forma no solo los países son los afectados, también lo son las instituciones públicas y privadas al igual que las personas que usan estas tecnologías.

Al mismo tiempo, los autores Morán e infante señalan que las instituciones del estado deben impulsar sus respectivos órganos de control institucional, para que este perfeccione y adecue un mejor uso de los recursos asignados por el estado, y a su vez pueda sancionar a los integrantes cuando estos estén inmersos en aptos de corrupción o estén denunciados por diversos delitos. (Morán e infante, 2020) Siguiendo lo anteriormente mencionado debemos saber que los recursos asignados por el estado deben ser administrados correctamente para que las instituciones cumplan con su función.

III METODOLOGÍA

El presente capitulo, se diseñó para encauzar la metodología que se usó durante la investigación, la cual fue de enfoque cualitativo.

Al respecto, el autor Sánchez en su investigación refiere que una investigación bajo el enfoque cualitativo tiene que sustentarse con evidencias recabadas por los investigadores, las cuales describen el fenómeno y tiene por objeto la interpretación empleado los diferentes métodos y técnicas (Sánchez, 2019).

3.1 **Tipo y diseño de la investigación**.

La naturaleza de la actividad de investigación fue de tipo básico, con el fin de poder extraer información sobre la problemática social existente, con los cimientos teóricos basados en teorías, principios y leyes, para presentar la información de manera formal y presentar un resultado que aporte nuevos conocimientos científicos (Hernández et al., 2014).

La investigación se llevó a cabo, bajo un diseño exploratorio con una revisión documental, de esta forma nos permitió poder recolectar información y poder efectuar un estudio de los datos obtenidos y nos permita construir una teoría con resultados favorables (Canese et al, 2020; Chávez y Palomino, 2019).

3.2 **Categorías, subcategorías y matriz de categorización**

En relación los autores Montes et al, señalan que este tipo de instrumento nos permitió desarrollar un sistema de categorías gracias al estudio de las historias de vida. Porque este tipo de instrumento representa una forma de organizar el pensamiento con el objetivo de comprender el tema sobre la investigación (Montes et al, 2019).

Tabla 1: Matriz de categorización y subcategorización

Título: "Perspectivas y Desafíos Legales en la Prevención de Delitos Informáticos y Delincuencia Organizada Transnacional en el Perú: Implicancias de la Ley N° 30096"

Problema	Objetivo	Hipótesis	Variables	Categoría generales	Categorías especificas
¿Cuál es el impacto de la Ley N° 30096 en la mitigación de delitos informáticos y la lucha contra la delincuencia organizada transnacional en el contexto peruano?	Determinar Cuál es el impacto de la Ley N° 30096 en la mitigación de delitos informáticos y la lucha contra la delincuencia organizada transnacional en el contexto peruano	Existe una mitigación de delitos informáticos y la lucha contra la delincuencia organizada transnacional en el contexto peruano, al aplicar la Ley N° 30096	**Independiente:** La implementación y aplicabilidad de la Ley N° 30096.	- Tipos de delitos informáticos en el Perú.	**-** Aplicación de medidas legales. - Aplicación de medidas judiciales. - Recursos y capacidades de las instituciones. - Ámbito de aplicación. -Creación de autoridades y agencias específicas. -Asignación de recursos -Desarrollo de normativas y directrices. .
			Dependiente: La efectividad de la prevención de delitos informáticos y la lucha contra la delincuencia organizada transnacional en el Perú.	- Naturaleza de la delincuencia organizada transnacional	-Tipicidad de delitos informáticos en el Perú. -Tasa de delitos informáticos -Capacidad de investigación y procesamiento -Cumplimiento empresarial -Naturaleza de la delincuencia organizada transnacional

3.3 **Escenario de estudio**

Este estudio se realizó por medio de entrevistas a personal de instituciones públicas, que aplican una acción judicial en el tema de delitos informáticos y delincuencia organizada internacional.

Esta muestra que utilizamos no es probabilística ya que incluye solo abogados, personal de la Marina de Guerra del Perú y Policía Nacional del Perú, que cumplen con ciertos criterios. Es decir, 4 abogados, 4 miembros de la Marina y 2 miembros de la Policía, que cumplieron con los criterios descritos en la Tabla de criterios de inclusión de encuestados para respaldar nuestra entrevista.

3.4 **Participantes**

En la presente investigación, se realizó con una búsqueda y selección de especialistas en delitos informáticos y delincuencia organizada transnacional, cpn la especialidad jueces, fiscales, efectivos policiales y miembros de la Marina de Guerra del Perú.

Tabla 2:

Proceso de selección de expertos

Criterios	Inclusión	Exclusión
Primer criterio Especialidad	especialidad en DP-DPP	que no posean especialidad DP-DPP
Segundo criterio Grado Académico	Que tengan una maestría y/o doctorado.	Que no tengan una maestría y/o doctorado.
Tercer criterio Trayectoria	Que el abogado tenga más de dos años de experiencia materia de. DP-DPP	Que el abogado no tenga más de dos años de experiencia materia de DP-DPP..

- DP Derecho Penal.
- DPP Derecho procesal penal

Tabla 3:

Criterios de inclusión y exclusión de los participantes

Abogados en DP-DPP			
Criterios Para inclusión.	➢ Abogados que se desempeñen en Lima Metropolitana. ➢ Que los abogados tengan la especialidad en DP – DPP ➢ Que los abogados tengan practica mayor a 2 años en DP – DPP. ➢ Abogados que se desempeñen en casos de delitos informáticos y delincuencia organizada transnacional.	**Criterios para exclusión**	➢ Abogados que no se desempeñen en Lima Metropolitana. ➢ Que los abogados no tengan la especialidad en DP – DPP ➢ Que los abogados no tengan practica mayor a 2 años en la DP – DPP ➢ Abogados que no se desempeñen en casos de delitos informáticos y delincuencia organizada transnacional.

- DP Derecho Penal.
- DPP Derecho procesal penal

3.5 **Técnicas e instrumentos de recolección datos**

Las entrevistas estructuradas que fueron realizadas individualmente. Las entrevistas fueron realizadas por cada miembro del grupo de investigación, las entrevistas se realizaron de forma presencial para obtener respuestas rápidas de los entrevistados. La entrevista duró unos 20 minutos, se mantuvieron registros para asegurar la calidad de la información obtenida. De igual manera, se transcribió las entrevistas empleando el programa Word y posteriormente se analizó la información obtenida.

3.6 **Procedimientos**

- Las entrevistas se realizarán con los participantes que fueron seleccionados de acuerdo a los criterios establecido, se realizó individualmente de presencial y virtualmente. Asimismo, cada entrevista no excedió los 30 minutos.

- Las entrevistas de trabajo virtuales se realizaron a través de videoconferencia mediante la plataforma Zoom, se coordinó el día y la hora por medio telefónico o SMS antes de la entrevista con el especialista.
- Las entrevistas que se realizaron fueron grabadas y posteriormente se analizarán para la obtención de las respuestas dadas por los especialistas en el tema.

Figura 3:

Flujograma de Fuente Documental

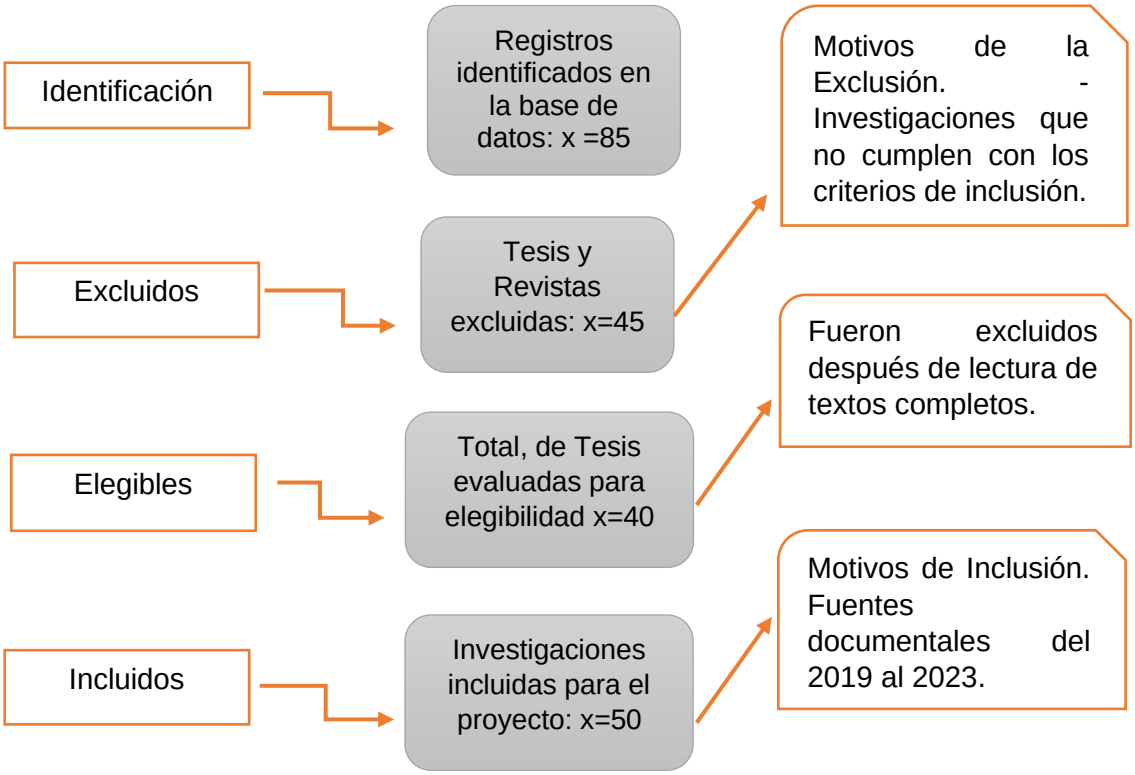


Tabla 4: Codificación de entrevistados

Entrevistado	Especialidad/ Grado	Centro donde labora /cargo	Fecha de entrevista	Tiempo	Virtual / presencial	Fuente	Codificación
Henry Flores Cuadros	Abogado	Fiscal Adjunta Provincial.	29 / 09 / 2023	00:29:22	ZOOM	Video /audio	R1
Oshin Jimena Panebra Alfaro	Abogado	Fiscal Adjunta del 4to despacho de la 2da fiscalía especializada.	29 / 09 / 2023	00:24:35	ZOOM	Video /audio	R2
Luis Diego Malqui Siguas	Suboficial de Segunda. PNP	Departamento de inteligencia región Lima.	01 / 10 / 2023	00:27:00	ZOOM	Video /audio	R3
Idver Yosdao Toratto Flores	Abogado	Oficina de Asesoría Legal de la Dirección de Telemática de la Marina.	02 / 10 / 2023	00:30:00	ZOOM	Video /audio	R4
Abel Osccorima Leon	Técnico Segundo TEL.	Departamento de Ciberseguridad .	02 / 10 / 2023	00:18:30	Presencial	Audio	R5
Roberto Barrantes Arce	Capitán de Navío	Sub director de la Dirección de Telemática de la Marina	06/ 10/ 2023	00:20:10	Presencial	Audio	R6
Monroy Meza, Juan Carlos	Abogado	Fuero Militar Policial	08/ 10/ 2023	00:19:15	ZOOM	Video /audio	R7
Carlos Java luyo	Abogado – Magister en Derecho Penal	SUNAFIL	09/ 10/ 2023	00:21:10	Presencial	Audio	R8
Rander Sinchi del Águila	Abogado	Asistente en Función Fiscal	17/ 10 / 2023	00:14:30	ZOOM	Video /audio	R9
Jilmer Altamirano Cieza	Técnico Tercero ECO	Departamento de ciberseguridad	20 / 10 /78	00:17: 20	Presencial	Audio	R10

3.7 Rigor Científico

A fin de, comprobar que sea confiable y valido este estudio, se empleó la prueba numero V Aiken para especificar la importancia de cada ítem y la idoneidad asignada por el especialista. De hecho, el rigor científico dió una credibilidad al trabajo de investigación. Porque va más allá de los resultados obtenidos en esta investigación y otorga al trabajo de investigación la credibilidad necesaria para contribuir a la difusión del conocimiento relacionado con el problema estudiado.

3.8 Método de análisis de datos

Como parte de esta investigación, se efectuó entrevistas y se revisaron tesis, antecedentes, libros y trabajos de investigación. Asimismo, se siguió un método de análisis de contenido diseñado para su presentación y posterior debate.

3.9 Aspectos éticos

Esta investigación respeta la autoría de las revisiones bibliográficas anteriores. Asimismo, se mantuvo la opinión y objetividad de cada entrevista y no se adulteraron las respuestas de los entrevistados. Por lo tanto, se tomó en cuenta las disposiciones difundidas por la Universidad Cesar Vallejo con la intensión de asegurar su traslucidez y legalidad de la presente.

IV RESULTADOS Y DISCUSIÓN

4.1 Resultados

En el presente capítulo se describe los resultados obtenidos, de acuerdo a la guía de entrevista a profundidad semiestructurada, la cual ha sido llevada a la práctica al entrevistar a 10 especialistas con conocimiento en delitos informáticos y delincuencia organizada transnacional. Recopilando las respuestas se procedió a codificar los resultados.

Aplicación de medidas legales

¿Considera usted que la Ley 30096 de Delitos Informáticos es suficiente para sancionar adecuadamente los delitos informáticos?

Figura 4

Aplicación de medidas judiciales

¿Considera usted que la falta de una adecuada tipificación de los delitos informáticos en nuestra legislación contribuye al aumento de estos delitos por parte de la delincuencia organizada transnacional?

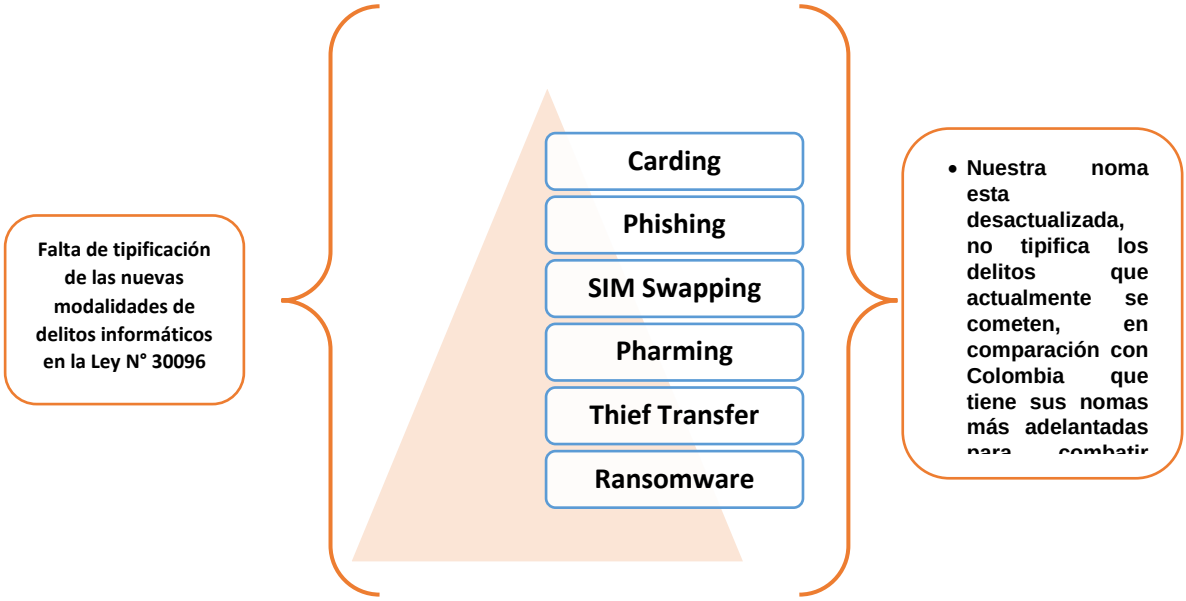


Figura 5

Recursos y capacidades de las instituciones.

¿Cree usted que es necesario fortalecer las capacidades y estrategias de los fiscales para combatir los delitos informáticos?

Figura 6

Ámbito de aplicación.

¿Opina usted que la Ley N° 30096 presenta desafíos y limitaciones en su aplicación?

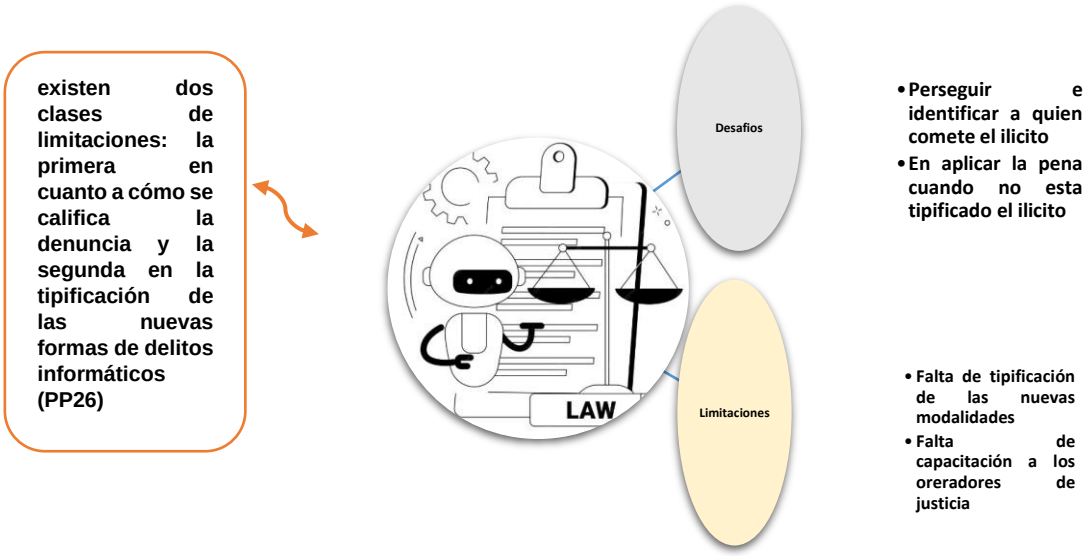


Figura 7

Creación de autoridades y agencias específicas

¿Considera usted que el Poder Judicial, el Ministerio Público y la División de Investigación de Alta Tecnología (DIVINDAT) cuentan con los recursos necesarios para combatir los delitos informáticos transnacionales?

Figura 8

Asignación de recursos.

¿Opina usted que el Estado peruano asigna los recursos necesarios para fortalecer las capacidades y la labor de los principales operadores de la administración de justicia?

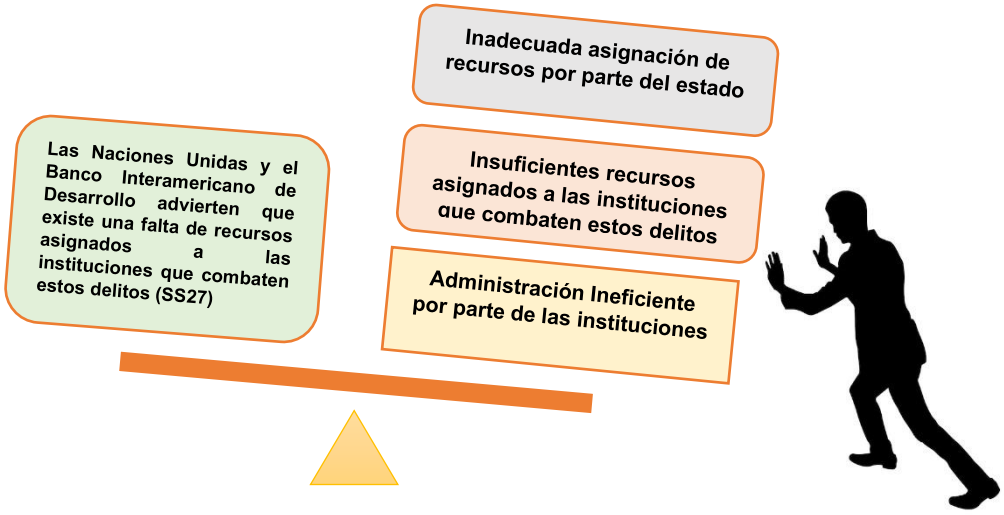


Figura 9

Desarrollo de normativas y directrices.

¿Considera usted que se debe fortalecer la cooperación internacional y promover la adhesión del Perú a los diferentes organismos internacionales en relación con los delitos informáticos?

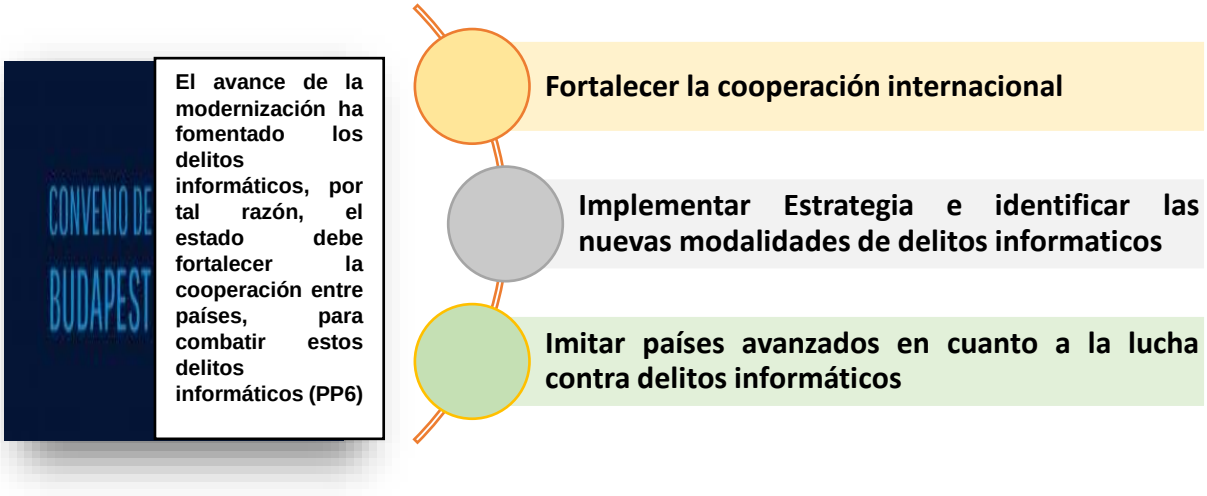


Figura 10

Tipificación de los delitos informáticos en el Perú

¿Opina usted que deberían tipificarse en nuestro ordenamiento jurídico las nuevas formas de delitos informáticos, como el Phishing, Carding, SIM Swapping y Thief Transfer?

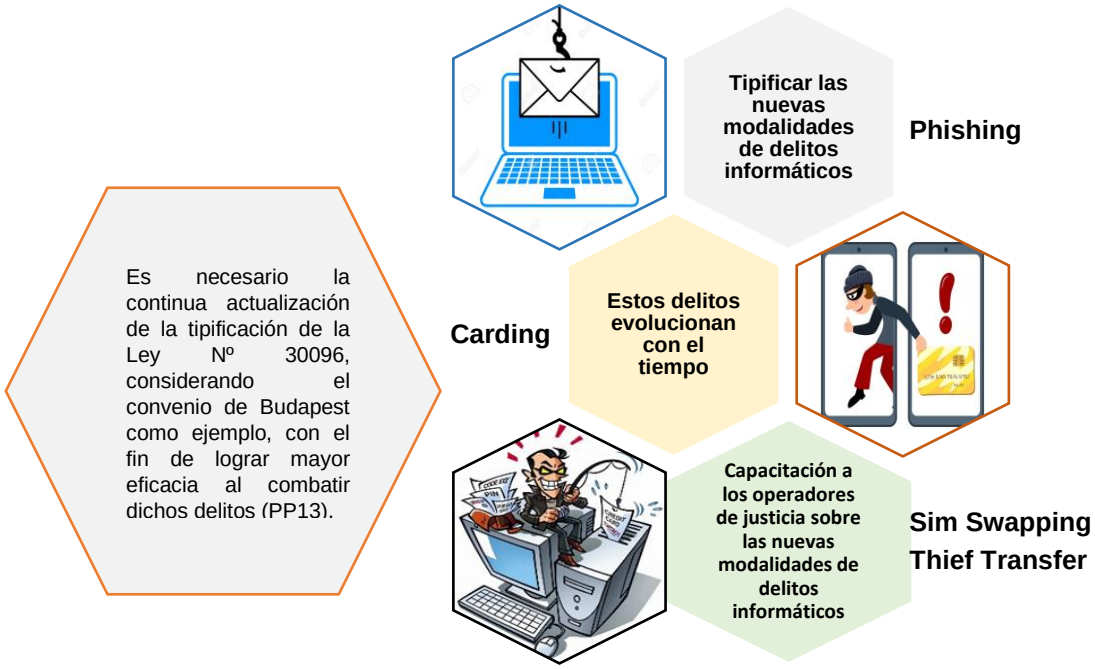


Figura 11

Tasa de delitos informáticos.

¿Cree usted que la inseguridad ciudadana contribuye al crecimiento de los delitos informáticos?

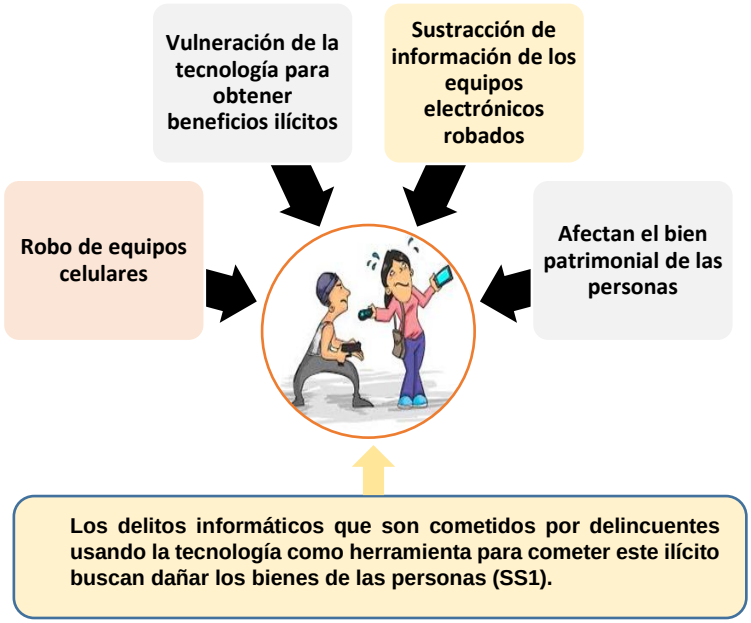


Figura 12

Capacidad de investigación y procesamiento

¿Cree usted que en nuestro país la evidencia digital es suficiente para respaldar la acusación y permitir una penalización adecuada de estos delitos?

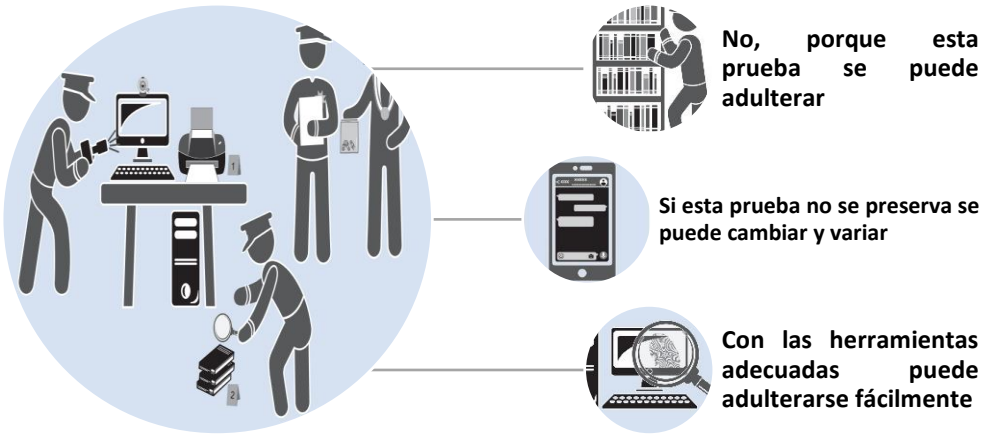


Figura 13

Cumplimiento empresarial

¿Cree que las entidades, tanto públicas como privadas, aplican adecuadamente el cumplimiento empresarial en el Perú?

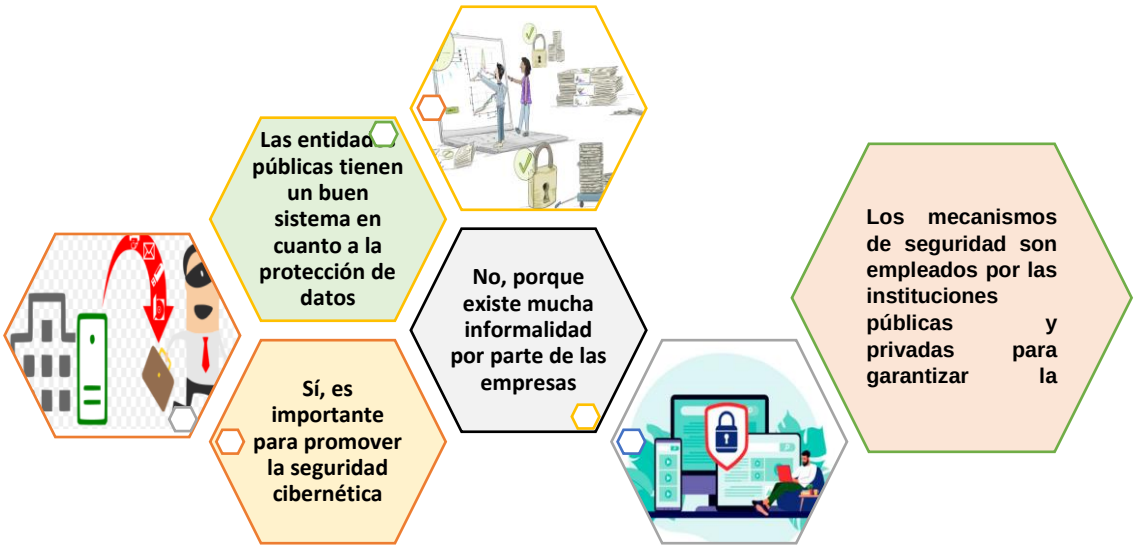


Figura 14

Naturaleza de la delincuencia organizada transnacional

¿Cuál es la naturaleza de la delincuencia organizada transnacional?

Tabla 5:

Tabla de origen (entrevistados del 1-5)

Ítem	Entrevistados / Preguntas	R1	R2	R3	R4	R5
1	P1	Sí, Depende de su implementación De la ley	Sí, Da respuesta a las necesidades de combatir las actividades ilícitas	No porque estas conductas varían	No es suficiente debido a que los delitos informáticos van evolucionando	No, porque le falta hacer una correcta tipificación de los delitos informáticos
2	P2	No, porque nuestra normativa está en un proceso de desarrollo para tipificar estos delitos	Sí, porque está técnicamente bien diseñada para sancionar todas las modalidades actuales	Si contribuye porque es imposible poder tipificar cada conducta	No, por ser una inadecuada legislación que contribuye a que estos delitos se perfeccionen	Si porque muchas veces estos delitos se cometen desde fuera del país y la ley no contempla este hecho
3	P3	Sí, al tipificación estos delitos contribuye a fortalecer las capacidades para mitigar el aumento de estos delitos	No, porque actualmente el ministerio publico recurre a la policía especializada para poder esclarecer una denuncia sobre delitos informáticos	Si es importante una forma de fortalecer las capacidades y estrategias es la capacitación de los fiscales	Considero que si es necesario no solo capacitar tanto en aspectos técnicos, como también en la forma de aplicar la ley.	Sí, hay que darle las herramientas necesarias para combatir estos delitos
4	P4	Si, presenta desafíos y limitaciones en su aplicación en cuanto tipificar los nuevos delitos informáticos	Pienso que no, porque está estructurada a la realidad de los delitos que se cometen	Sí, presenta limitaciones porque no se puede alcanzar estos nuevos delitos	Si presenta desafíos en cuanto a su actualización para que contemple los nuevos delitos informáticos	Si presenta desafíos y limitaciones ante los nuevos delitos informáticos que van evolucionando
5	P5	Si deben contar con los recursos necesarios para afrontar las nuevas amenazas	Sí, pero se debería incrementar más unidades en la policía	No cuenta, existe una escases tanto en el ámbito de capacitación y logístico	No se cuentan con los recursos necesarios, falta darle las herramienta necesarias	En la actualidad estas instituciones no cuentan con los recursos necesarios por una mala administración
6	P6	En la actualidad no hay un enfoque directo para asignar los recursos necesarios	El estado no cumple con asignar el suficiente presupuesto	No, se debería incrementarse para todos los operadores de justicia	No, porque es una ineficiente administración de los recursos asignados	No asigna los recursos correctamente para que estas instituciones puedan cumplir sus funciones
7	P7	Sí, es fundamental fortalecer la cooperación internacional para combatir estos delitos	Sí, es muy importante que el Perú tenga convenios con países de todo el mundo	Si es fundamental para poder combatir estos delitos	Considero de que sí, es una estrategia muy importante	Si, considero que es necesario para combatir estos delitos informáticos
8	P8	Sí, porque es importante tipificar las formas de delitos informáticos, cada delito tiene un procedimiento	No, porque estos delitos se adecuan a lo establecido en la ley	Sí, tenemos que hacer un estudio de estas nuevas tendencias para poder dar una pena	Sí, es necesario que nuestro ordenamiento jurídico contemple estos delitos para que sean sancionados	Si lo considero porque facilitaría la labor de las instituciones que combaten estos delitos

9	P9	Sí, los delincuentes ven una forma de obtener beneficios sin tener riesgos	Considero que no, porque ahora las personas prefieren hacer sus transacciones de forma virtual que presencial.	Sí , porque pueden vulnerar el bien jurídico usando la tecnología	Sí, es uno de los principales factores al no tener una adecuada gestión de seguridad	Sí, porque la delincuencia día a día va en aumento
10	P10	Es esencial que se recolecte y se preserve adecuadamente para garantizar su valides en un proceso judicial	Sí, porque sin esta evidencia no se podría sancionar a las personas que cometen estos delitos	Sí, es la carga de la prueba que va ayudar a poder sancionar estos ilícitos	Considero de que si, esto tiene que ver con la capacitación de los involucrados en investigar estos hechos	Sí, porque nos sirve como prueba fehaciente
11	P11	Sí, es importante para promover la seguridad cibernética	Si tanto en el sector público como privado	Aun no todas las empresas lo cumplen	Si, en las entidades públicas tenemos un adecuado nivel de protección pero en el ámbito privado no es el adecuado	No, porque existe mucha informalidad por parte de las empresas
12	P12	Cooperación de grupos criminales que operan a nivel internacional	Coordinar entre ellos ataques cibernéticos a otros países y eludir a la justicia	Es la obtención del patrimonio de forma ilícita	La afectación de un bien desde fuera del país usando equipos informáticos	Cometer delitos para satisfacer sus necesidades económicas de una manera ilícita

Tabla de origen (entrevistados del 6-10)

Ítem	Entrevistados / Preguntas	R6	R7	R8	R9	R10
1	P1	No es suficiente es una norma muy gaseosa debería aterrizarse en algo más concreto	Sí, es una norma adecuada para sancionar los delitos informáticos	No porque solo comprende conductas ya tipificadas	No es suficiente, se debe modificar o actualizar los tipos de delitos de la ciberdelincuencia	Considero que esta ley no es suficiente para mitigar los delitos informáticos
2	P2	Si lo considero porque si hubiera una tipificación más severa se reduciría estos delitos	Cuando no se tipifican todas las conductas delictivas, se abre la posibilidad de conductas que dañan bienes jurídicos	Si cuando no existe la tipicidad previamente establecidas	No, La tipificación está bien, pero se debe actualizar cada cierto tiempo de acuerdo a los nuevos tipos de ciberdelincuencia	Considero que si, porque conforme avanza la tecnología surge nuevas formas de cometer estos delitos
3	P3	SI, Considero que al ocupar el cargo los fiscales están en la capacidad	Es necesario fortalecer las capacidades y con ello mejorar las estrategias que aplican los fiscales	Si, En efecto los fiscales han demostrado deficiencia no solo en delitos informáticos	Sí, todos los operadores de justicia, deben tener una correcta capacitación	Sí, es necesario darle a los operadores de justicia las herramientas necesarias
4	P4	Si, presenta limitaciones porque cada vez van a mejorar los delitos informáticos	Considera que si presenta desafíos en la medida que no tenemos la debida preparación para su aplicación a nivel fiscal	Si existe una limitación en cuanto sigan habiendo adelantos tecnológicos	Sí, hay limitación debido a la escases en el presupuesto y a los avances de la delincuencia	Si presenta desafíos y limitaciones en cuanto a la capacitación y herramientas tecnológicas para los operadores de justicia.

5	P5	Considero que no existe una adecuada asignación de recursos necesarios a estas instituciones	Considero que no cuentan con los recursos económicos, logísticos y humanos suficientes para ello.	No, a nivel estado ninguna institución pública cuenta con los recursos necesarios	No, hay limitaciones en el presupuesto, falta de convenios internacionales, lo que limita a los operadores públicos tener información	Considero que los operadores de justicia no cuentan con los recursos necesarios.
6	P6	No asignan los recursos necesarios por una mala administración por parte de las autoridades	Considero que no existe una asignación adecuada de recursos por parte del Estado para este fin.	No porque no tienen soporte logístico y capital humano especializado	El presupuesto asignado por el estado no es suficiente, se debe invertir en tecnología para poder detectar a los autores	De acuerdo a mi experiencia el estado no asigna los recursos necesarios.
7	P7	Sí, Creo que deberíamos imitar lo bueno y ver qué países de la región está más avanzado en el tema	Considero que sí, es una necesidad global la cooperación internacional y para ello es obligatorio la adhesión del Perú en estos organismos internacionales.	Si se debería fortalecer la cooperación internacional para el intercambio de capacidades tecnológicas	Sí, es bueno fortalecer para tener una debida identificación ya que la ciberdelincuencia no es solo del Perú también proviene del extranjero.	Si, lo considero porque nos permite tener conocimiento de cómo otros países combaten estos delitos
8	P8	Si, Debe ponerse énfasis en cada una de ellas porque cada una tiene un modo de operar distinto	Si, Considero que es una obligación del legislador tipificar todas estas modalidades	Si de manera expresa, especifica conforme al principio de tipicidad	Sí, Es importante tipificar las nuevas formas de delitos informáticos.	Sí, es muy importante porque de esta forma ayuda a los operadores de justicia poder sancionar estos delitos
9	P9	Sí, porque es parte por la idiosincrasia que se ha creado al mesclar la delincuencia venezolana, colombiana y la peruana afectando a las personas	Si, Considero que estos delitos acrecientan la inseguridad ciudadana.	No porque la inseguridad ciudadana solo se debe a la delincuencia común	Sí, al robar los documentos de identidad, pueden vulnerar nuestros derechos, haciéndose pasar por uno.	Considero que si porque al sustraer un equipo electrónico pueden obtener nuestra información
10	P10	Si es la huella que deja al usar una máquina para cometer estos delitos	No, considero que a la evidencia digital se debe sumar otras evidencias	Se considera como un medio de prueba, no es suficiente	Sí, Es importante recabar la evidencia digital que vincule a la persona con el delito cometido.	Considero de que no porque existen otras pruebas que facilita saber quién cometió estos delitos
11	P11	Si hablamos tanto de publicas y privadas si aplican medidas de seguridad.	Considero que no.	Si tratan en la medida de cumplir para evitar el robo de información	No aplican adecuadamente, deben ser actualizadas ya que las entidades son vulneradas a través de su sistema	Si estas instituciones protegen los datos personales utilizando diferentes medios
12	P12	Afectar los activos de la nación y de las empresas	Se sustenta en la globalización de la información que no tiene fronteras físicas.	Que este grupo de personas no solo comete este delito en su país también lo hace en otros países.	Vulnerar las tecnologías de diferentes áreas, estatales o privadas a fin de obtener un beneficio económico	La delincuencia común no necesita una jerarquía mientras la organizada si

Tabla 6:

Tabla Sistematizada

P	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10
P1	SÍ • Implementación • Ley	• Sí • Necesidades • Combatir	• No • Conductas • Diversas	• No • Insuficiente • Evolucionan	• No • Corregir • Tipificación	• No • Insuficiente • Gaseosa	• Sí • Norma • Adecuada	• No • Conductas • Tipificadas	• No • Insuficiente • Modificar	• No • Suficiente • Mitigar
P2	• Proceso • Desarrollo	• Técnicamente • Diseñada • Sanciona	• Sí • Imposible • tipificar	• Inadecuada • Legislación	• Delitos • Fuera	• Tipificación • Severa • reduce	• Conductas • Dañan • Bien jurídico	• Sí • Tipicidad • Establecida	• No • Tipificación • Actualizar	• No • Tecnología • Nuevas
P3	• Tipificación • Crecimiento de delitos	• Ministerio Publico • Coordinación • Policía	• Sí • Capacitación	• Capacitación • Intervenir	• Herramientas • Necesarias	• Sí • Fiscales • Capacidad	• Necesidad • Fortalecer	• Fiscales • Deficiencia	• Sí • Operadores • Capacitación	• Si • Operadores • Herramientas
P4	• Desafíos • Limitaciones	• Estructura • Realidad	• Limitaciones • Nuevos delitos	• Desafíos • Actualización	• Desafíos • Evolución	• Limitaciones • Nuevos delitos	• Desafíos • Preparación	• Limitación • Adelantos Tecnológicos	• Sí • Limitación • Escases	• Si • Presenta • Capacitación
P5	• Contar • Recursos • Necesarios	• No • Incrementar • Unidades policiales	• No • Escases • Capacitación • Logístico	• Recursos • Herramientas • Necesarias	• Recursos • Necesarios	• No • Asignan • Recursos	• No • Ninguna • Institución • Recursos	• No • Ninguna • Institución • Recursos	• No • Limitaciones • Presupuesto	• No • Operadores • Cuentan
P6	• No • Enfoque directo • Recursos necesarios	• Insuficiente • Presupuesto	• Incremento	• Administración • Ineficiente	• Recursos • Distribución	• No • Inadecuada • Asignación de recursos	• Inadecuada • Asignación de recursos	• No • Soporte logístico • Capital humano	• No • Insuficiente • Invertir	• Experiencia • Estado • Asigna
P7	• Fortalecer • Cooperación	• Convenios • Internacionales	• Combatir • Delitos informáticos	• Estrategia • Implementar	• Necesario • Fortalecer	• Imitar • Países avanzados	• Necesidad • Cooperación • Internacional	• Fortalecer • Cooperación • Intercambio	• Si • Identificar • Delincuentes	• Si • Conocimiento • Países

P8	• Delito • Procedimiento	• Delitos • Adecuación	• Estudio • Tendencias	• Ordenamiento • Sanción	• Facilitar • Combatir	• Operar • Distinto	• Tipificar • Modalidades	• Expresa • Principio de tipicidad	• Sí • Importante • Tipificar	• Si • Importante • Conocimientos •
P9	• Delincuencia • Beneficios	• Transacciones • Virtuales	• Vulnerar • Tecnología	• Factores • Gestión inadecuada	• Delincuencia • Incremento	• Delincuencia • Internacional	• acrecientan • Inseguridad	• Inseguridad ciudadana • Delincuencia común	• Sí • Vulnerar • Derechos	• Si • Equipos • Electrónicos
P10	• Preservación de la prueba • Validez	• Evidencia	• Prueba • Sanción	• Capación	• Prueba	• Huella • Maquina	• Evidencia	• Prueba	• Sí • Recabar • Evidencia	• No • Pruebas
P11	• Importante • Seguridad	• Publico • Privado	• No • Incumplen • Empresas	• Publicas • Protección • Privado inadecuado	• Informalidad • Empresas	• Publicas • Privadas	• No	• Tratan de cumplir	• No • Aplican • Vulneradas	• Si • Instituciones • Protegen
P12	• Cooperación • Criminales	• Coordinan • Ataques cibernéticos	• Patrimonio • Ilícito	• Afectación • Fuera del país	• Delitos • Satisfacción	• Afecta • Activos	• Globalización • Sin fronteras	• Delitos • Dentro y fuera del país	• Vulnerar • Tecnologías	• Necesita • Jerarquía • Organización

Tabla 7: Cruce de información

Categorías Generales		Categorías Especificas			
Categorías General 1	Tipos de delitos informáticos en el Perú.	Aplicación de medidas legales.	Aplicación de medidas judiciales.	Recursos y capacidades de las instituciones.	Ámbito de aplicación.
		P1	P2	P3	P4
		• Implementación de la Ley de Delitos Informáticos (R1) • Necesidades de Combatir los delitos informáticos (R2) • Conductas Diversas (R3) • Los delitos informáticos evolucionan (R4) • Corregir la Tipificación (R5) • La ley es Insuficiente y Gaseosa (R6) • Norma Adecuada (R7) • Conductas no Tipificadas (R8) • Se necesita modificar la tipicidad de los delitos informáticos (R9) • Esta ley es insuficiente (R10)	• Esta ley está en proceso de desarrollo (R1) • Técnicamente la ley está bien diseñada (R2) • Imposible de tipificar las nuevas conductas (R3) • Inadecuada Legislación (R4) • Los delitos se cometen desde fuera del país (R5) • Se debe implementar la tipificación severa (R6) • Dañan el Bien jurídico (R7) • Tipicidad Establecida (R8) • La norma no está actualizada (R9) • Estos se cometen con nuevas tecnologías (R10)	• Crecimiento de delitos por falta de una inadecuada tipificación (R1) • Ministerio Publico en Coordinación Con la Policía (R2) • Capacitación al personal fiscales (R3) • Capacitación en el uso de la tecnología (R4) • Herramientas Necesarias (R5) • Fiscales con Capacidad de aplicar la ley (R6) • Necesidad de Fortalecer la ley de delitos informáticos (R7) • Fiscales son Deficientes por falta de preparación (R8) • Dar capacitación a los operadores de justicia (R9) • dar herramientas modernas a los fiscales (R10)	• Desafíos y Limitaciones en la aplicación de la ley (R1) • la ley debe tener una estructura de acuerdo a la Realidad (R2) • Limitaciones en los Nuevos delitos (R3) • Desafíos en la actualización de la ley (R4) • Desafíos en cuanto a la evolución de los delitos (R5) • Limitaciones en Nuevos delitos (R6) • Desafíos en la preparación de los operadores de justicia (R7) • Limitación en adelantos tecnológicos (R8) • Presenta una limitación por la escasa tipificación de los delitos (R9) • Limitación en cuanto preparar adecuadamente a los operadores de justicia (R10)
• Artículos de investigación científica (SS) • Tesis (PP) • Libros (PP)		• Hablar de los ciberdelitos es muy complejo porque existe una amplia variedad, los cuales evolucionan y no están tipificados en la ley de delitos informáticos (PP23) • Es una conducta típica la cual evoluciona a través del tiempo y nuestra norma necesita ser modificada de acuerdo a la evolución de los delitos informáticos (PP25)	• Nuestra noma esta desactualizada, no tipifica los delitos que actualmente se cometen, en comparación con Colombia que tiene sus nomas más adelantadas para combatir este tipo de delitos (PP4) • A medida que Colombia se vuelve un país dependiente de la informática, esto origina que los delitos que se cometen con esta tecnología no estén tipificados en nuestro ordenamiento (SS8)	• Para que se considere una evidencia, debe haber sido acopiada y examinada, de acuerdo a las normas legales tanto internacionales como del país (PP24) • En la actualidad el ciberespacio es una necesidad el cual brinda un amplio uso de poder operarlo, sin embargo, la ciberdelincuencia es parte de él, lo cual obliga a los operadores de justicia a tener una capacitación y se les brinde las herramientas necesarias para combatir estos delitos informáticos (SS17)	• existen dos clases de limitaciones: la primera en cuanto a cómo se califica la denuncia y la segunda en la tipificación de las nuevas formas de delitos informáticos (PP26) • La norma vigente es desactualizada, ya que no están de acuerdo con la tecnología actual; en cambio los delincuentes van evolucionando en su modo de cometer los delitos (PP19)

Categorías Generales		Categorías Especificas		
Categorías General 1	Tipos de delitos informáticos en el Perú.	Creación de autoridades y agencias específicas.	Asignación de recursos	Desarrollo de normativas y directrices.
		P5	P6	P7
		• Contar con recursos necesarios para combatir estos delitos informáticos (R1) • Incrementar las unidades policiales especializadas (R2) • Escases de capacitación y logística para los operadores de justicia (R3) • Recursos y herramientas necesarias para la policía (R4, R5 y R10)) • No asignan recursos para las instituciones que combaten estos delitos (R6, R7 Y R8) • Existe una limitación en el presupuesto para combatir estos delitos (R10)	• Inadecuada asignación de recursos (R1, R2, R3, R6, R7, R8 y R10) • Administración Ineficiente (R4) • Mala distribución de recursos (R5) • Insuficientes recursos asignados a las instituciones que combaten estos delitos (R9)	• Fortalecer la cooperación internacional (R1, R7 y R8) • Convenios Internacionales (R2) • Combatir delitos informáticos a través de convenios internacionales (R3) • Implementar Estrategia e identificar esos nuevos delitos (R4 y R9) • Necesario para fortalecer la lucha contra estos delitos (R5) • Imitar países avanzados en cuanto a la lucha contra delitos informáticos (R6 y R10)
• Artículos de investigación científica (SS) • Tesis (PP) • Libros (PP)		• Las fiscalías especializadas que combaten los delitos informáticos deben recibir Implementación en material tecnológico, capacitación del personal y los recursos necesarios para mitigar estos delitos (PP30) • Se debe establecer una estrategia y protocolos para que los recursos asignados por la administración pública, sean usados eficientemente en la lucha de estos delitos informáticos (SS29)	• Las Naciones Unidas y el Banco Interamericano de Desarrollo advierten que existe una falta de recursos asignados a las instituciones que combaten estos delitos (SS27) • Se ha creado una política nacional, formándose instituciones especializadas en Colombia, para mejorar la asignación de partidas presupuestales para fortalecer las medidas que combatan los delitos informáticos (SS28)	• El avance de la modernización ha fomentado los delitos informáticos, por tal razón, el estado debe fortalecer la cooperación entre países, para combatir estos delitos informáticos (PP6) • En el Perú los delitos informáticos van en aumento, debido a la constante modernización que usan los delincuentes, lo cual hace difícil identificarlos y más aún encontrarlos cuando se cometen desde fuera del país, en consecuencia, se debe implementar estrategias y convenios internacionales para luchar contra estos delitos (PP10)

Categorías Generales		Categorías Especificas				
Categorías General 2	Naturaleza de la delincuencia organizada transnacional	Tipificación de delitos informáticos en el Perú.	Tasa de delitos informáticos	Capacidad de investigación y procesamiento	Cumplimiento empresarial.	Naturaleza de la delincuencia organizada transnacional
		P1	P2	P3	P4	P5
		• tipificar las nuevas formas de delitos informáticos (R1, R4, R5, R8, R9 y R10) • Estos delitos se adecuan a lo establecido en la ley (R2) • Hacer un estudio de estas nuevas tendencias (R3) • Debe ponerse énfasis en cada una de ellas (R6) • Considero que es una obligación del legislador conocer y tipificar estas nuevas formas de delito (R7)	• Beneficios ilícitos obtenidos por la delincuencia (R1) • Transacciones virtuales ilícitas, vulnerando los derechos de las personas (R2 y R9) • Vulneración de la tecnología para obtener beneficios ilícitos (R3 y R10) • Factores de gestión inadecuada para combatir estos ilícitos (R4) • Incremento de la delincuencia (R5) • Delincuencia internacional que comete delitos informáticos (R6) • Inseguridad ciudadana por el tráfico de información ilícito (R7 Y R8)	• Sí, porque nos sirve como prueba fehaciente del ilícito cometido (R1, R4, R5, R6 y R9) • Sin esta evidencia no se podría sancionar (R2) • Es la carga de la prueba que va ayudar a poder sancionar (R3) • Implementar Estrategia para mejorar la calidad de las pruebas (R4) • Considero que a la evidencia digital se debe sumar otras evidencias (R7) • Se considera como un medio de prueba, no es suficiente (R8 y R10)	• Sí, es importante para promover la seguridad cibernética (R1, R2, R4, R6, R8 y R10) • No, porque existe mucha informalidad por parte de las empresas (R3, R5, R7 y R9)	• Coordinar entre ellos ataques cibernéticos a otros países y eludir a la justicia (R1, R2, R8 y R10) • Es la obtención del patrimonio de forma ilícita vulnerando los sistemas de protección por parte de bandas organizadas trasnacionales (R3, R4 Y R5) • Afectar los activos de la nación y de las empresas (R6) • Se sustenta en la globalización de la información que no tiene fronteras físicas, lo cual es aprovechado por la delincuencia organizada transnacional (R7)
• Artículos de investigación científica (SS) • Tesis (PP) • Libros (PP)		• La delincuencia organizada transnacional desestabiliza el orden legal y económico de las naciones, es por eso la necesidad de crear normas que tipifiquen ampliamente estos nuevos tipos de ilícitos, los cuales deben ser actualizados constantemente (PP5) • Es necesario la continua actualización de la tipificación de la Ley, tanto en la sección de delitos especiales como en la sección de delitos comunes, teniendo en cuenta el convenio de Budapest, con el fin de lograr mayor eficacia al combatir dichos delitos (PP13)	• Los delitos informáticos que son cometidos por delincuentes buscan dañar los bienes de las personas usando la tecnología como herramienta para cometer este ilícito. (SS1) • El Estado se ha visto superado, por la delincuencia organizada, este tipo de delitos tiene por finalidad de obtener beneficios ilícitos, cuenta con una estructura compleja, tiene tiempo de estar constituida por ende tiene funciones distribuidas para cometer sus delitos (PP2)	• La evidencia digital es la prueba fehaciente que permite saber quién o quienes cometieron el delito usando un equipo electrónico. • En nuestro país, no existe procedimiento normativo para obtener la evidencia digital, la policía solo cuenta con un manual de análisis digital forense (PP27)	• los mecanismos utilizados por las instituciones públicas y privadas para garantizar la seguridad de los datos personales, y estos no sean sustraídos desde cualquier parte del planeta (PP28) • es de suma importancia que las empresas incorporen un sistema de protección de datos, creando una cultura que fomente el cumplimiento empresarial (PP29)	• La delincuencia organizada transnacional es cada día más compleja cuentan con poder, recursos e influencias que provienen muchas veces de políticos involucrados en estas organizaciones. (SS24) • En la actualidad la delincuencia organizada transnacional comete los delitos informáticos afianzando el lavado de activos y tráfico de la nueva moneda virtual que son los Bitcoins y como esta moneda no está sujeta a un control por las autoridades (PP12)

4.2 **Discusión.**

Al respecto, se ha evidenciado que las modalidades de Delitos Informáticos van evolucionan junto con el avance tecnológico. Esta situación genera fallas en la aplicación de la Ley Nº 30096, “Ley de Delitos Informáticos”, toda vez que en ella aún no se consideran la formulación de nuevos supuestos típicos que han surgido durante los últimos años, evidenciando el desfase en el marco normativo peruano. Arellano y Galindo (2022), refieren que mencionado marco normativo contiene fallas legislativas en cuanto a la identificación de delitos en las que contemplan. En ese mismo orden de ideas, Vega y Arévalo (2022), señalan que en nuestra legislación no existe una ley que contemple de forma específica la descripción de la ciberdelincuencia ni la regulación de los delitos informativos cometidos en el ciberespacio. Por lo anteriormente señalado, se tiene a bien precisar que la constante evolución de las tecnologías ha conllevado al perfeccionamiento de las modalidades de delitos informáticos. Es por ello que con la finalidad de que se pueda combatir de forma íntegra aquellas modalidades, resulta imperiosamente necesario que se efectúe la actualización de la ley objeto de la presente investigación.

Por otra parte, se evidencia una inadecuada aplicación de las medidas judiciales que combaten los delitos informáticos, debido a que la Ley Nº 30096, “Ley de Delitos Informáticos”, se encuentra en proceso de reformulación y desarrollo, de tal manera que pueda considerar todas las conductas delictivas relacionadas a los delitos informáticos, que se han perfeccionado con el tiempo. Para Custodio (2020) ante las nuevas modalidades delictivas que surgen con el avance tecnológico, surge también la necesidad, de que las normas legales consideren la tipicidad específica, acorde con la evolución de los delitos que son cometidos en la actualidad, Por lo expuesto, con la finalidad de que referida Ley considere una óptima aplicación de medidas judiciales destinadas a combatir los delitos informáticos y sus nuevas modalidades, es necesario que esta sea actualizada de forma periódica.

En ese sentido, es necesario fortalecer la capacidad humana y del material tecnológico asignado al personal que interviene en la prevención y sanción de los Delitos Informáticos, con ello se podrá mejorar las estrategias destinadas a

combatir estos ilícitos, lo cual debe realizarse periódicamente, dado el avance de la tecnología. Para los autores Olivares y Ceras (2021), indican que, en la norma penal peruana, se establece el requerimiento de instrucción orientado a la capacitación del personal policial, fiscal y judicial, debido al incumplimiento de los principios penales de sanción. Olivares y ceras (2021) En la actualidad el ciberespacio es una necesidad el cual brinda un amplio uso de poder operarlo, sin embargo, la ciberdelincuencia es parte de él, lo cual obliga a los operadores de justicia a tener una capacitación y se les brinde las herramientas necesarias para combatir estos delitos informáticos. Por esta razón, se ha determinado que tanto el poder judicial, la fiscalía y la policía, no se encuentren debidamente capacitados para poder combatir estos delitos.

En consecuencia, resulta pertinente señalar que la inadecuada preparación y capacitación del personal involucrado en sancionar y prevenir los delitos informáticos, a nivel fiscal, policial y judicial, genera una actitud negativa que contribuye a su impunidad, en ese sentido se determina que mencionada situación representa ser un desafío para determinar su actualización, así como una limitación en cuanto a poderse determinar una correcta aplicación de las penas. Para Espinoza (2022), la ciberdelincuencia es un desafío de nuestra normativa legal en derecho penal, la cual representa nuevos retos tanto para la Policía Nacional como para la Fiscalía y el sistema judicial, es por ello que se determina que la aplicación de la normativa legal vigente es ineficiente para abarcar los nuevos delitos informáticos. Urpeque (2018), existen dos clases de limitaciones: la primera en cuanto a cómo se califica la denuncia y la segunda en la tipificación de las nuevas formas de delitos informáticos. En ese sentido su actualización representa desafíos y limitaciones en cuanto a la evolución de las nuevas modalidades de estos delitos.

En otro orden de ideas, los recursos que asigna el estado a las instituciones como el poder judicial, las fiscalías especializadas en delitos informáticos y la División de Investigación de Delitos de Alta Tecnología, es insuficiente debido al incremento de denuncias relacionadas a estos ilícitos. De acuerdo a la publicación Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina (2019), señalan que se debe establecer una estrategia y protocolos para que los recursos asignados por la administración pública, sean usados eficientemente

en la lucha de estos delitos informáticos. Hernández y Patricio (2022), Las fiscalías especializadas que combaten los delitos informáticos deben recibir Implementación en material tecnológico, capacitación del personal y los recursos necesarios para mitigar estos delitos. En ese sentido, la asignación de recursos no solo debe ser económico, también se debe asignar equipos tecnológicos modernos y establecer una capacitación periódica para el personal que labora en el poder judicial, las fiscalías especializadas y la división de la policía encargada de investigar estos delitos.

En ese sentido, no se cuentan con los recursos económicos, logísticos y humanos suficientes para combatir los Delitos Informáticos, por una inadecuada e ineficiente administración de los recursos asignados. Un informe sobre la ciberdelincuencia en el Perú: estrategias y retos de estado (2023), señala que la Organización de las Naciones Unidas (ONU) y el Banco Interamericano de Desarrollo (BID) se advierte sobre la baja asignación de recursos económicos como humanos que se asignan a las diferentes instituciones que combaten estos delitos. Cortez et al (2015), Se ha creado una política nacional, para mejorar la asignación de partidas presupuestales, para fortalecer las medidas que combatan los delitos informáticos Situación que conlleva a determinar que, es necesario que el Estado efectúe la asignación de partidas presupuestales destinadas a combatir los Delitos Informáticos, lo cual permita fortalecer la capacidad de las instituciones asignadas para tal fin.

Dicho de otro modo, es una necesidad global la cooperación internacional y para ello es obligatorio la adhesión del Perú en diferentes organismos internacionales, relacionados a la cooperación internacional para fomentar estrategias que permitan combatir estos Delitos Informáticos. Para los autores Tenorio (2001), Devia (2017) y Huamán (2020) definen que el ciberdelito es tratado por las autoridades de diversos países, así como también, por las organizaciones internacionales con el fin de reforzar el apoyo entre los países, así como la concordancia en la normatividad penal para combatir estos delitos. De modo que, existe una concordancia entre países que buscan fortalecer su normativa, para combatir estos delitos informáticos, en ese sentido, corresponde que nuestro país se adhiera a referido marco de cooperación internacional.

Al respecto, es una obligación del legislador efectuar un estudio para poder tipificar todas estas modalidades e inclusive dejar una clausula abierta que posibilite la persecución de nuevas formas delictivas no previstas hasta la fecha. Para Daza (2020), en la actualidad, el avanzado desarrollo tecnológico, en un mundo integrado y el desarrollo de diferentes tecnologías que crean nuevos riesgos, recientemente han brotado nuevos delitos cibernéticos que deben tipificarse. Pereyra y Turpo (2020), Es necesario la continua actualización de la tipificación de la Ley, tanto en la sección de delitos especiales como en la sección de delitos comunes, teniendo en cuenta el convenio de Budapest, con el fin de lograr mayor eficacia al combatir dichos delitos. Por lo expuesto, se debe actualizar la normativa y ponerse un énfasis a los nuevos delitos informáticos derivados del aprovechamiento del avance tecnológico.

Por otro lado, estos delitos informáticos acrecientan la inseguridad ciudadana, debido a que la delincuencia nacional como transnacional vulnera los diferentes sistemas de seguridad, para de esta forma obtener beneficios económicos ilícitos. Para Acosta, Benavides y García (2020) refieren que los delitos informáticos se configuran cuando se sustrae información de una o varias personas usando el ciberespacio, creando una problemática que atenta contra la tranquilidad de una sociedad. Chauca (2019), El Estado se ha visto superado, por la delincuencia organizada, este tipo de delitos tiene por finalidad de obtener beneficios ilícitos, cuenta con una estructura compleja, tiene tiempo de estar constituida por ende tiene funciones distribuidas para cometer sus delitos. En relación con lo mencionado, el perfeccionamiento y evolución de los delitos informáticos incrementan la inseguridad ciudadana, cada vez que se sustrae un equipo electrónico y se vulnera la información personal.

Además, en relación a la evidencia digital, es necesario que a esta se le sumen nuevas evidencias que contribuyan a que se efectúe una mejor valoración de la prueba, de tal manera que permita que las penalizaciones de estos delitos sean analizadas de forma conjunta. Para Prieto (2017) la evidencia digital tiene como función revisar los sistemas en busca de pruebas que permitan determinar quién o quienes cometieron estos ilícitos. Cadillo (2022), En nuestro país, no existe procedimiento normativo para obtener la evidencia digital, la policía solo cuenta con

un manual de análisis digital forense. En otras palabras, existe una discrepancia en el cruce de información debido a que esta no considerada como prueba única la evidencia digital.

Por consiguiente, es necesario que se efectue el cumplimiento de las estrategias de seguridad orientadas a la protección contra los Delitos Informáticos en las instituciones públicas y privadas, a fin de que estas se encuentren resguardadas ante cualquier amenaza relacionada con estos ilícitos. Por su parte, Rodríguez (2020) señala que los mecanismos utilizados por las instituciones públicas y privadas son efectivos para garantizar la seguridad de los datos personales, y estos no sean sustraídos desde cualquier parte del planeta. Trillo (2019), es de suma importancia que las empresas incorporen un sistema de protección de datos, creando una cultura que fomente el cumplimiento empresarial. Por lo expuesto, es necesario que se promueva la participación efectiva del sector privado y público, con la finalidad de contribuir con la protección de los datos personales y combatir los Delitos Informáticos.

Por lo tanto, la delincuencia organizada transnacional se sustenta en la globalización de la información que no tiene fronteras físicas. Situación que permite que se pueda lucrar de forma ilícita con una absoluta displicencia por los operadores de justicia. Para los autores Chauca (2019) y Paredes (2023) las organizaciones criminales se sustentan en obtener beneficio económico de forma ilícita, obteniendo estas ganancias de los mercados donde existe un flujo económico amplio. Al respecto, se determina que el principal fundamento para que los Delitos Informáticos se perfeccionen y evolucionen, es el nivel organizacional que estos poseen, toda vez que en la mayoría de los casos son transnacionales. Por lo tanto, es un ilícito que debe ser abarcado de forma conjunta con las diferentes organizaciones internacionales

V CONCLUSIONES

Se concluye que la Ley N° 30096 no ha tenido un efecto positivo en la reducción de los delitos informáticos. Actualmente, se han desarrollado nuevas modalidades de delitos informáticos que no están contempladas en nuestra legislación, lo que dificulta a los operadores de justicia abordar estos crímenes según las leyes vigentes.

La Ley N° 30096, conocida como Ley de Delitos Informáticos, se ha demostrado ineficaz en la reducción de las formas actuales de delitos informáticos, como el Phishing, Smishing, Vishing y las transferencias fraudulentas. Estos delitos no están contemplados en la ley, lo que genera vacíos legales que son aprovechados por la delincuencia organizada transnacional al no ser sancionados.

El principal desafío de la legislación de delitos informáticos radica en su falta de actualización frente a las nuevas modalidades de estos crímenes, ampliamente utilizadas por la delincuencia organizada transnacional. La limitación en su aplicación se debe a la carencia de una capacitación adecuada para los operadores de justicia, junto con la falta de herramientas tecnológicas modernas para combatir estos delitos.

Los factores principales que restringen la aplicación efectiva de la normativa para combatir los delitos informáticos perpetrados por la delincuencia organizada transnacional son: i) la necesidad de actualizar la ley objeto de esta investigación; ii) la asignación adecuada de recursos por parte del Estado a los operadores de justicia; iii) la capacitación continua de estos operadores para abordar las nuevas formas de delitos informáticos; y iv) el fortalecimiento de la cooperación internacional en la lucha contra la delincuencia organizada transnacional.

VI **RECOMENDACIONES**

Para potenciar el impacto positivo de la Ley N° 30096 en la mitigación de delitos informáticos, se recomienda: i) establecer Fiscalías Especializadas en Delitos de Ciberdelincuencia en los distintos departamentos del Perú; ii) asignar nuevos Fiscales provinciales y Fiscales Adjuntos Provinciales a estas Fiscalías Especializadas debido al incremento de los delitos informáticos en los últimos años, lo que ha generado una carga procesal considerable.

Es crucial realizar una reestructuración específica de la Ley N° 30096, Ley de Delitos Informáticos, que contemple: i) la inclusión de las nuevas modalidades como el Phishing, Smishing, Vishing y las transferencias fraudulentas en el capítulo V de la ley para permitir que los operadores de justicia apliquen penas tipificadas, eliminando vacíos legales; y, ii) la incorporación de agravantes en el artículo 11 para los delitos informáticos perpetrados desde el extranjero por la delincuencia organizada transnacional.

Para fortalecer la aplicación de la Ley N° 30096 en la prevención y persecución de delitos informáticos y la delincuencia organizada transnacional en el país, se sugiere: i). Se considere la actualización e incorporación de la Ley Nº 30096 en la cual se tipifiquen las nuevas modalidades de delitos informáticos. ii) ii) proveer equipos tecnológicos con sistemas de geolocalización para rastrear los dispositivos utilizados en los ilícitos; y, iii) que la Policía Nacional, a través de la División de Investigación de Delitos de Alta Tecnología (DIVIDAT), mejore los protocolos de investigación, preservación de pruebas digitales y persecución de los responsables.

Se recomienda que con la finalidad de que se efectúe una adecuada capacitación en temas relacionados a la ciberdelincuencia y se pueda asignar de una manera eficiente los recursos asignados, es necesario que se gestione una adecuada asignación presupuestal a la Unidad de Ciberdelincuencia (UCIBER) y la red de Fiscales de Ciberdelincuencia, la División de Investigación de Delitos de Alta Tecnología (DIVIDAT) de la Policía Nacional del Perú.

REFERENCIAS

Acosta, M.G., Benavides, M.M. & García, N.P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. Revista Venezolana de Gerencia, 25(89), 351–368. https://produccioncientificaluz.org/index.php/rvg/article/view/31534/32619

Abdullah et al., (2020) Comprehensiva Review of Cybercrime Detection Techniques. IEEE Access12 (8), 137296 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9146148

Akeem Olalekan AYUB y Linus AKOR. (2022). Tendencias, patrones y consecuencias del delito cibernético en Nigeria. Gusau International Journal of Management and Social Sciences , 5 (1), 22. https://gijmss.com.ng/index.php/gijmss/article/view/107

Aladro, E. (2011). La Teoría de la Información ante las nuevas tecnologías de la comunicación. :http://intra.uigv.edu.pe/bitstream/handle/20.500.11818/6461/TESIS_VITTERI%20MELGAR.pdf?sequence=1&isAllowed

Bullón Rocha, J. K. (2019). La importancia de la adhesión al Convenio sobre la Ciberdelincuencia para la legislación peruana de delitos informáticos [Tesis Bachiller, Universidad Andina de Cusco]. https://repositorio.ucv.edu.pe/handle/20.500.12692/83985

Callegari, N. (1985). Delitos informáticos y legislación. Revista De La Facultad De Derecho Y Ciencias Políticas, (70), 112–118. https://revistas.upb.edu.co/index.php/derecho/article/view/5140

Carnevali Rodríguez, Raúl. (2010) La criminalidad organizada. Una aproximación al derecho penal italiano, en particular la responsabilidad de las personas jurídicas y la confiscación. Revista Ius et Praxis, Año 16, Nº 2, 2010, pp. 273 – 330 https://www.corteidh.or.cr/tablas/r26012.pdf

Condori C. (2020). Implicancias Jurídicas del Fraude Informático y la Protección Penal del Delito Contra el Patrimonio Distrito Fiscal de Lima Norte 2020. https://repositorio.ucv.edu.pe/handle/20.500.12692/63158.

Cuervo, G. (2018) El crimen organizado transnacional como una amenaza híbrida para la Triple Frontera (Argentina, Paraguay y Brasil). Revista Científica General José María Córdova 16(23), phttps://revistacientificaesmic.com/index.php/esmic/article/view/304/231

Custodio, C. (2021). Las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/74797/Custodio_CY-SD.pdf.

Chávez Suárez, G. R., & Palomino Mendiolaza, A. E. (2019). Plan de negocio para combatir la obesidad en el distrito de Ate mediante un modelo de negocio “Crossfit”.

Chauca Oña, J. P. (2019). Delincuencia organizada: asociación Ilícita en la dogmática ecuatoriana [Tesis de Bachiller, Universidad Central Del Ecuador]. http://www.dspace.uce.edu.ec/bitstream/25000/18552/1/T-UCE-0013-JUR-181.pdf

Daza, D. (2020) crimen organizado transnacional: retos de la política criminal en México frente al tráfico de drogas [Tesis Doctoral, Universidad de Salamanca]. Repositorio Institucional - Universidad de Salamanca file:///C:/Users/canta/Downloads/PDEDGG_DazaG%C3%B3mezC_Crimenorganizado.pdf

Davina Shanti, S. (2020). A NEW STATE OF ORGANIZED CRIME: AN ANALYSIS OF ORGANIZED CYBERCRIME NETWORKS, ACTIVITIES, AND EMERGING THREATS. The Journal of Intelligence, Conflict, and Warfare, 3 (1), 1–11. https://doi.org/10.21810/jicw.v3i1.2359

Devia González, E. A. (2017). Estafa informática del artículo 248.2 del Código Penal [Tesis de Doctorado, Universidad de Sevilla]. https://idus.us.es/bitstream/handle/11441/75625/Tesis%20Edmundo%20Devia%20Completa%20Final%2031%20Mayo%202017.pdf?sequence=1&isAllowed=yquedan

Diario Oficial El Peruano (2023) Denuncias por delitos informáticos se incrementaron en más del 90% en el Perú. https://www.elperuano.pe/noticia/188048-denuncias-por-delitos-informaticos-se-incrementaron-en-mas-del-90-en-el-peru

Duarte, C. (2021). Ciberdelincuencia: análisis del Convenio No. 85 de Budapest y el compromiso del Estado de Guatemala. Revista Ciencia Multidisciplinaria CUNORI, 5(2). 111-118.DOI: https://doi.org/10.36314/cunori.v5i2.174

Espinoza Calderón, V. (2022). Delitos Informáticos y nuevas modalidades Delictivas. Instituto Pacifico S.A.C.

Fernández Osorio, A. y Lizarazo Ospina, Y. (2020) “Crimen organizado y derechos humanos en Colombia: enfoques en el marco de la implementación del

Acuerdo de Paz con las FARC-EP". NovumJus 16, núm. 2 pp. 215-250. https://doi.org/10.14718/NovumJus.2022.16.2.9

Giménez, A. (2020) delincuencia organizada trasnacional, Revista Española de Investigación Criminológica Volumen 21, p.2 https://reic.criminologia.net/index.php/journal/article/view/795/379

Gutiérrez Bonilla, R. L. (2020). La cooperación eficaz como técnica de investigación frente al delito de delincuencia organizada y su aplicación en el Ecuador. Período 2014-2018 [Tesis de Doctora, Universidad Técnica De Ambato – Ecuador]**.** https://repositorio.uta.edu.ec/jspui/bitstream/123456789/31099/1/FJCS-POSG-192.pdf

Gutiérrez, A. (2017) El delito de organización criminal: fundamentos de responsabilidad y sanciones jurídicas. Tesis Doctoral. Universidad de Sevilla https://idus.us.es/bitstream/handle/11441/61304/Tesis%20Alri%20ZURITA%20GUTI%C3%89RREZ.pdf?sequence=1

Guerrero, D., & Benavides, G. (2023). el estado ecuatoriano y el crimen organizado. revista de la academia del guerra del ejército ecuatoriano, 16(1), 12. https://doi.org/10.24133/AGE.VOL16.N01.2023.08

Huamán Cruz, M. Y. (2020]. Los delitos informáticos en Perú y la suscripción del Convenio de Budapest [Tesis de Bachiller, Universidad Andina del Cusco]. https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/4116/Marleny_Tesis_bachiller_2020.pdf?sequence=1&isAllowed=y

Huamán, C. (2018) Los delitos informáticos en Perú y la suscripción del convenio de Budapest, 2020. https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/4116/Marleny_Tesis_bachiller_2020.pdf?sequence=1&isAllowed=y

Lamas Suarez, G. (2019). Cibercrimen, bitcoins y lavado de activos. Licho & Arte S.A.C.

Mancebo, M. A. (2022). Organizaciones criminales: un talante para delinquir. Revista Honoris Causa, 14(1), 140–155. Recuperado a partir de https://revista.uny.edu.ve/ojs/index.php/honoris-causa/article/view/102

Ortiz Campos, N. J. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. Revista Científica Hallazgos21, 4(1), 100- 111. http://revistas.pucese.edu.ec/hallazgos21/

Ortiz, N. (2019). Normativa Legal sobre delitos informáticos en Ecuador. Rev.Hallazgos21,106.https://dialnet.unirioja.es/servlet/articulo?codigo=7148227.

Organización Internacional de Policía. (2022) informe resumido sobre las tendencias de la delincuencia a escala mundial - INTERPOL 2022. file:///C:/Users/canta/Downloads/Global%20Crime%20Trend%20Summary%20Report%20SP%20(3).pdf.

Prado Saldarriaga, V. (2019). Lavados de activos y organizaciones criminales en el Perú. Nuevas Políticas, estrategias y marco legal. Editorial Moreno S.A.

Paredes, R. (2023) crimen organizado transnacional en américa del siglo xxi: grupos criminales, estructura y funcionamiento, Revista de ciencias de investigación en defensa-CAEN, volumen 4, p. 38-54 http://recide.caen.edu.pe/index.php/recide/article/view/95/124

Payá Santos, C., Cremades Guisado, Álvaro, & Delgado Morán, J. J. (2017). El fenómeno de la ciberdelincuencia en España: La propuesta de la Universidad Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito. Revista Policía Y Seguridad Pública, *7*(1), 237–270. https://doi.org/10.5377/rpsp.v7i1.4312.

Peña, J. (2015). El fraude como delito informático. http://dspace.ucuenca.edu.ec/bitstream/123456789/21321/1/TESIS.pdf.

Pereira, P. (2015). Os Estados Unidos e a ameaça do crime organizado transnacional nos anos 1990. Revista Brasileira de Política Internacional, vol. 58, núm. 1. https://www.redalyc.org/articulo.oa?id=35842206005

Pereyra Maita, L. A. y Turpo Hinostroza, J. A. (2020). Instrumentos normativos que se deben adecuar en nuestra legislación según el marco del Convenio de Budapest como mecanismo legal de protección a la intimidad personal frente a las TICS [Tesis de Bachiller en Derecho, Universidad Tecnológica del Perú]. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/3579/Luz%20Pereyra_Jessy%20Turpo_Trabajo%20de%20Investigacion_Bachiller_2020.pdf?sequence=1&isAllowed=y

Peña Cabrera Freyre, A. (2020). Crimen Organizado, Aspectos Generales. Tópicos de la Parte General y Parte Especial. Gaceta Jurídica S.A.

Pierre Hauck and Sven Peterke (2010) Organized crime and gang violence in national and international law, Volume 92 Number 878 June 2010 https://www.corteidh.or.cr/tablas/r25263.pdf

Reátegui Sánchez, J. (2021). Lavado de Activos y compliance criminal. Gaceta Jurídica S.A.

Rodríguez Olave, G. Y. (2022). Sobre la organización criminal y la participación en la banda criminal: ¿Podemos distinguir entre ambos delitos? *IUS ET VERITAS*, (64), 216-227. https://doi.org/10.18800/iusetveritas.202201.012

Ruiz Barragán, S. (2017). Protección de datos y seguridad digital en Colombia: una propuesta sobre la necesidad de adhesión al Convenio de Budapest (2001). [Tesis de Bachiller, Universidad de los Andes]. https://repositorio.uniandes.edu.co/handle/1992/39748

Saín, G. (2018) Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet / compilado por Ricardo Antonio Parada; José Daniel Errecaborde. - 1a ed. - Ciudad Autónoma de Buenos Aires: Erreius, 2018. 192 p.; 26 x 19 cm.
https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Sequeiros Calderón, I. C. (2016). Vacíos legales que imposibilitan la sanción de los delitos informáticos en el nuevo código penal peruano – 2015 [Tesis de Bachiller, Universidad de Huánuco).
http://repositorio.udh.edu.pe/bitstream/handle/123456789/286/IVETT%20CLARITZA%20SEQUEIROS%20CALDERON.pdf?sequence=1&isAllowed=y

Somoza, R. (2022) Delincuencia organizada transnacional y su incidencia en las relaciones internacionales, Revista 593 Digital Publisher, volumen 7, p. 548-563https://dialnet.unirioja.es/servlet/articulo?codigo=8385853

Suárez J. (2022). vigencia ontológica de la ciberseguridad en el marco de la seguridad informática chilena. convenio de Budapest. aula virtual, 3(6), 132-148.
https://aulavirtual.web.ve/revista/ojs/index.php/aulavirtual/article/view/121

Torres, J. (2019). Zonas grises y delincuencia organizada transnacional: desafíos para la soberanía del Estado en América Latina. Via Iuris Libertadores Fundación Universitaria, 67. Recuperado desde: https://www.redalyc.org/journal/2739/273963960009/273963960009.pdf.

Torres, I. (2021) El impacto del cibercrimen en delitos de estafa en el Distrito de Lima, 2021. para optar el título profesional en derecho. universidad peruana de las américas
http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/1729/TRABAJO%20DE%20INVESTIGACI%C3%93N%20%281%29.pdf?sequence=1

Urpeque Tarazona, C. J. (2018). Análisis de la adecuación de la Ley N°30096, al marco del convenio internacional de Budapest 2001, y su incidencia en la reducción de los delitos informáticos [Tesis de Bachiller, Universidad Nacional José Faustino Sánchez Carrión]. https://repositorio.unjfsc.edu.pe/handle/20.500.14067/4632

Vega Aguilar, J. y Arévalo Minchola, M. (2022) Ciberdelitos, Análisis en el Sistema Penal, Editorial IUSTITIA

Villavicencio, F. (2014). Delitos Informáticos. IUS ET VERITAS, *24*(49), 284-304.https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view

ANEXOS

Matriz de categorización

"Perspectivas y Desafíos Legales en la Prevención de Delitos Informáticos y Delincuencia Organizada Transnacional en el Perú: Implicancias de la Ley N° 30096"

Expertos validadores del Instrumento de validación

Problema	**Hipótesis**	**Objetivos**	**Variable**	**Método**	**Participantes**
¿Cuál es el impacto de la Ley N° 30096 en la mitigación de delitos informáticos y la lucha contra la delincuencia organizada transnacional en el contexto peruano? **Problema Específicos** a) ¿De qué manera ha contribuido la Ley N° 30096 a la reducción de delitos informáticos en el Perú y a la desarticulación de grupos de delincuencia organizada transnacional? b) ¿Cuáles son los principales desafíos y limitaciones legales que enfrenta la aplicación de la Ley N° 30096 en la prevención y persecución de delitos informáticos y la delincuencia organizada transnacional en el país?	Determinar Cuál es el impacto de la Ley N° 30096 en la mitigación de delitos informáticos y la lucha contra la delincuencia organizada transnacional en el contexto peruano. **Hipótesis Específicos** a) la Ley N° 30096 contribuye a la reducción de delitos informáticos en el Perú y a la desarticulación de grupos de delincuencia organizada transnacional**.** b) los desafíos y limitaciones legales que enfrenta la aplicación de la Ley N° 30096, mejorara la prevención y persecución de delitos informáticos y la delincuencia organizada transnacional en el país.	Existe una mitigación de delitos informáticos y la lucha contra la delincuencia organizada transnacional en el contexto peruano, al aplicar la Ley N° 30096. **Objetivos Específicos** a) Analizar de qué manera ha contribuido la Ley N° 30096 a la reducción de delitos informáticos en el Perú y a la desarticulación de grupos de delincuencia organizada transnacional. b) Analizar cuáles son los principales desafíos y limitaciones legales que enfrenta la aplicación de la Ley N° 30096 en la prevención y persecución de delitos informáticos y la delincuencia organizada transnacional en el país.	**Independiente:** La implementación y aplicabilidad de la Ley N° 30096. **Dependiente:** La efectividad de la prevención de delitos informáticos y la lucha contra la delincuencia organizada transnacional en el Perú.	Enfoque cualitativo **Tipo** Básico **Diseño** Exploratorio	Está conformado por 10 especialista en derecho penal y derecho procesal penal **Escenario** Lima Metropolitana **Técnicas e Instrumentos** Revisión documental Entrevistas

Nombres y apellidos	**Especialidad**	**Ocupación**	**Grado Académico**	**Ámbito laboral**

Jennifer Lee Herrera Ñañez	Derecho Penal	Abogado	Magister	Estudio Jurídico
Luz Madeleyne Boza Quilca	Derecho Penal	Abogado	Magister	Estudio Jurídico
Carlos Jave Luyo	Maestro en Derecho Penal	Abogado	Doctor	SUNAFIL
Nataly Morón Salas		Abogado	Magister	Dirección de Telemática de la Marina
Edison Zegarra Escalante	Derecho Penal	Abogado	Magister	Estudio Jurídico
Evilyn Guere Rivera	Derecho Penal	Abogado	Magister	Estudio Jurídico

UCV
UNIVERSIDAD CÉSAR VALLEJO

GUÍA DE ENTREVISTA

Aplicación de medidas legales.

1. ¿Considera usted que la Ley 30096 de Delitos Informáticos es suficiente para sancionar adecuadamente los delitos informáticos?

Aplicación de medidas judiciales.

2 ¿Considera usted que la falta de una adecuada tipificación de los delitos informáticos en nuestra legislación contribuye al aumento de estos delitos por parte de la delincuencia organizada transnacional?

Recursos y capacidades de las instituciones.

3 ¿Cree usted que es necesario fortalecer las capacidades y estrategias de los fiscales para combatir los delitos informáticos?

Ámbito de aplicación.

4 ¿Opina usted que la Ley N° 30096 presenta desafíos y limitaciones en su aplicación?

Creación de autoridades y agencias específicas.

5 ¿Considera usted que el Poder Judicial, el Ministerio Público y la División de Investigación de Alta Tecnología (DIVINDAT) cuentan con los recursos necesarios para combatir los delitos informáticos transnacionales?

Asignación de recursos.

6 ¿Opina usted que el Estado peruano asigna los recursos necesarios para fortalecer las capacidades y la labor de los principales operadores de la administración de justicia?

Desarrollo de normativas y directrices.

7 ¿Considera usted que se debe fortalecer la cooperación internacional y promover la adhesión del Perú a los diferentes organismos internacionales en relación con los delitos informáticos?

Tipos de delitos informáticos en el Perú.

8 ¿Opina usted que deberían tipificarse en nuestro ordenamiento jurídico las nuevas formas de delitos informáticos, como el Phishing, Carding, SIM Swapping y Thief Transfer?

Tasa de delitos informáticos.

9 ¿Cree usted que la inseguridad ciudadana contribuye al crecimiento de los delitos informáticos?

UCV
UNIVERSIDAD CÉSAR VALLEJO

Capacidad de investigación y procesamiento.

10 ¿Cree usted que en nuestro país la evidencia digital es suficiente para respaldar la acusación y permitir una penalización adecuada de estos delitos?

Cumplimiento empresarial.

11 ¿Cree que las entidades, tanto públicas como privadas, aplican adecuadamente el cumplimiento empresarial en el Perú?

Naturaleza de la delincuencia organizada transnacional.

12 ¿Cuál es la naturaleza de la delincuencia organizada transnacional?

UCV
UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

DATOS GENERALES

Apellidos y Nombres: Jennifer Lee Herrera Ñañez
Cargo e institución donde labora: Abogado
Nombre del instrumento motivo de evaluación: Guía de Entrevista
Autores del Instrumento: Cordova Zapata, Francisco Arturo
Rosas Ramírez, Edith Elena

Experto 1

Criterios	Indicadores	Validación		Observancia
		Si	No	
Claridad	Está formado con el lenguaje claro y apropiado	X		
Objetividad	Está expresado en conductas observables	X		
Pertinencia	Adecuado al avance de la ciencia pedagógica	X		
Organización	Existe una organización lógica	X		
Suficiencia	Comprende los aspectos en calidad y cantidad		X	
Adecuación	adecuado para valorar el constructo o variable a medir	X		
Consistencia	Basado en aspectos teórico - científicos.	X		
Coherencia	Entre las definiciones, dimensiones e indicadores	X		
Metodología	La estrategia responde al propósito de la mediación.	X		
Significatividad	Es útil y adecuado para la investigación	X		

Opinión de aplicabilidad:

Aplicable [ ] **Aplicable después de corregir [ ]** **No aplicable [ ]**

Jennifer Lee Herrera Ñañez
ABOGADO
CAL N° 47713

Firma del Experto Informante

UCV
UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

DATOS GENERALES

Apellidos y Nombres: Luz Madeleyne Boza Quilca
Cargo e institución donde labora: Abogado
Nombre del instrumento motivo de evaluación: Guía de Entrevista
Autores del Instrumento: Cordova Zapata, Francisco Arturo
Rosas Ramírez, Edith Elena

Experto 2

Criterios	Indicadores	Validación		Observancia
		Si	No	
Claridad	Está formado con el lenguaje claro y apropiado	/		
Objetividad	Está expresado en conductas observables	/		
Pertinencia	Adecuado al avance de la ciencia pedagógica	/		
Organización	Existe una organización lógica	/		
Suficiencia	Comprende los aspectos en calidad y cantidad	/		
Adecuación	adecuado para valorar el constructo o variable a medir	/		
Consistencia	Basado en aspectos teórico - científicos.	/		
Coherencia	Entre las definiciones, dimensiones e indicadores	/		
Metodología	La estrategia responde al propósito de la mediación.	/		
Significatividad	Es útil y adecuado para la investigación	/		

Opinión de aplicabilidad:

Aplicable [X] **Aplicable después de corregir [ ]** **No aplicable [ ]**

CAL 65578

Firma del Experto Informante

UCV
UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

DATOS GENERALES

Apellidos y Nombres: Carlos Jave Luyo
Cargo e institución donde labora: Abogado
Nombre del instrumento motivo de evaluación: Guía de Entrevista
Autores del Instrumento: Cordova Zapata, Francisco Arturo
Rosas Ramírez, Edith Elena

Experto 3

Criterios	Indicadores	Validación		Observancia
		Si	No	
Claridad	Está formado con el lenguaje claro y apropiado	/		
Objetividad	Está expresado en conductas observables	/		
Pertinencia	Adecuado al avance de la ciencia pedagógica	/		
Organización	Existe una organización lógica	/		
Suficiencia	Comprende los aspectos en calidad y cantidad	/		
Adecuación	adecuado para valorar el constructo o variable a medir	/		
Consistencia	Basado en aspectos teórico - científicos.	/		
Coherencia	Entre las definiciones, dimensiones e indicadores	/		
Metodología	La estrategia responde al propósito de la mediación.	/		
Significatividad	Es útil y adecuado para la investigación	/		

Opinión de aplicabilidad:

Aplicable [X] **Aplicable después de corregir [ ]** **No aplicable [ ]**

CARLOS RICARDO JAVE LUYO
Abogado
Registro C.A.L. N° 68830

Firma del Experto Informante

UCV
UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

DATOS GENERALES

Apellidos y Nombres: Nataly Morón Salas
Cargo e institución donde labora: Abogado
Nombre del instrumento motivo de evaluación: Guía de Entrevista
Autores del Instrumento: Cordova Zapata, Francisco Arturo
Rosas Ramírez, Edith Elena

Experto 4

Criterios	Indicadores	Validación		Observancia
		Si	No	
Claridad	Está formado con el lenguaje claro y apropiado	/		
Objetividad	Está expresado en conductas observables	/		
Pertinencia	Adecuado al avance de la ciencia pedagógica	/		
Organización	Existe una organización lógica	/		
Suficiencia	Comprende los aspectos en calidad y cantidad	/		
Adecuación	adecuado para valorar el constructo o variable a medir	/		
Consistencia	Basado en aspectos teórico - científicos.	/		
Coherencia	Entre las definiciones, dimensiones e indicadores	/		
Metodología	La estrategia responde al propósito de la mediación.	/		
Significatividad	Es útil y adecuado para la investigación	/		

Opinión de aplicabilidad:

Aplicable [/] **Aplicable después de corregir [ ]** **No aplicable [ ]**

Jefe(e) (e) Primero C.J
Jefe de la Oficina de Asesoría Legal
Nataly MORÓN Salas
00216082

Firma del Experto Informante

UCV
UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

DATOS GENERALES

Apellidos y Nombres: Elson H. Zegarra Escalante.
Cargo e institución donde labora: Abogado
Nombre del instrumento motivo de evaluación: Guía de Entrevista
Autores del Instrumento: Cordova Zapata, Francisco Arturo
Rosas Ramírez, Edith Elena

Experto 5

Criterios	Indicadores	Validación		Observancia
		Si	No	
Claridad	Está formado con el lenguaje claro y apropiado	X		
Objetividad	Está expresado en conductas observables	X		
Pertinencia	Adecuado al avance de la ciencia pedagógica	X		
Organización	Existe una organización lógica	X		
Suficiencia	Comprende los aspectos en calidad y cantidad	X		
Adecuación	adecuado para valorar el constructo o variable a medir	X		
Consistencia	Basado en aspectos teórico - científicos.	X		
Coherencia	Entre las definiciones, dimensiones e indicadores	X		
Metodología	La estrategia responde al propósito de la mediación.	X		
Significatividad	Es útil y adecuado para la investigación	X		

Opinión de aplicabilidad:

Aplicable [X] **Aplicable después de corregir [ ]** **No aplicable [ ]**

Elson H. Zegarra Escalante
ABOGADO
Reg. C.A.L. 68975

Firma del Experto Informante

UCV
UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

DATOS GENERALES

Apellidos y Nombres: Evilyn Güere Rivera
Cargo e institución donde labora: Abogada
Nombre del instrumento motivo de evaluación: Guía de Entrevista
Autores del Instrumento: Cordova Zapata, Francisco Arturo
Rosas Ramírez, Edith Elena

Experto 6

Criterios	Indicadores	Validación		Observancia
		Si	No	
Claridad	Esta formulado con lenguaje comprensible.	X		
Objetividad	Esta adecuado a las leyes y principios científicos.	X		
Actualidad	Esta adecuado a los objetivos y las necesidades reales de la investigación.	X		
Pertinencia	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.	X		
Organización	Existe una organización lógica.	X		
Suficiencia	Toma en cuenta los aspectos metodológicos esenciales.	X		
Intencionalidad	Esta adecuado para valorar las categorías.	X		
Consistencia	Se respalda en fundamentos técnicos y/o científicos.	X		
Coherencia	Existe coherencia entre los problemas, objetivos, supuestos jurídicos	X		
Metodología	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos. .	X		

Opinión de aplicabilidad:

Aplicable [X] **Aplicable después de corregir [ ]** **No aplicable [ ]**

Evilyn E. Güere Rivera
Reg. CAH. N° 2327
ABOGADA

Firma del Experto Informante

Matriz de Consolidado de la Validez de un Instrumento de Investigación (Consolidado de Expertos) - Dicotómica

Criterios		Descripción	Expertos						Suma de acuerdos totales	V Aiken	Descripción
			1	2	3	4	5	6			
1	Claridad	Esta formulado con lenguaje comprensible.	1	1	1	1	1	1	6	1.00	Fuerte
2	Objetividad	Esta adecuado a las leyes y principios científicos.	1	1	1	1	1	1	6	1.00	Fuerte
3	Actualidad	Esta adecuado a los objetivos y las necesidades reales de la investigación.	1	1	1	1	1	1	6	1.00	Fuerte
4	Pertinencia	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.	1	1	1	1	1	1	6	1.00	Fuerte
5	Organización	Existe una organización lógica.	1	1	1	1	0	1	5	0.83	Aceptable
6	Suficiencia	Toma en cuenta los aspectos metodológicos esenciales.	1	1	1	1	1	1	6	1.00	Fuerte
7	Intencionalidad	Esta adecuado para valorar las categorías.	1	1	0	1	1	1	5	0.83	Aceptable
8	Consistencia	Se respalda en fundamentos técnicos y/o científicos.	1	1	1	1	1	1	6	1.00	Fuerte
9	Coherencia	Existe coherencia entre los problemas, objetivos, supuestos jurídicos	1	1	1	1	1	1	6	1.00	Fuerte
10	Metodología	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.	1	1	1	1	1	1	6	1.00	Fuerte
Números de expertos 6									**Media 58**	0.97	Fuerte

Matriz Consolidado de Evaluación de Contenido de la Valides de Ítems de Entrevistados

Ítems	Expertos						Suma de acuerdos Total (s)	V Aiken	Descripción
	1	2	3	4	5	6			
1	3	3	3	3	3	2	17	0.94	Fuerte
2	2	3	3	3	3	2	16	0.89	Aceptable
3	3	3	3	3	2	2	16	0.89	Aceptable
4	3	3	3	3	3	3	18	1.00	Fuerte
5	3	3	3	3	3	3	18	1.00	Fuerte
6	3	3	3	3	1	3	16	0.89	Aceptable
7	3	3	3	3	2	3	17	0.94	Fuerte
8	3	3	3	3	2	3	17	0.94	Fuerte
9	3	3	2	3	3	2	16	0.89	Aceptable
10	3	3	3	3	3	3	18	1.00	fuerte
11	2	3	3	3	3	3	17	0.94	Fuerte
12	3	3	3	3	3	3	18	1.00	fuerte
Numero de expertos 6							Media	0.94	Fuerte

UCV
UNIVERSIDAD CÉSAR VALLEJO

Matriz de Validez de ítems de Entrevista a profundidad por Expertos

Experto 2

Apellidos y Nombres del Experto:	Cargo o Institución donde labora:	Nombre del Instrumento
Luz Madeleyne Boza Quilca	Abogado	Valoración de los ítems del Instrumento

Ítems	Valoración				Descripción
	Deficiente (0)	Regular (1)	Bueno (2)	Excelente (3)	
1				/	
2				/	
3				/	
4				/	
5				/	
6				/	
7				/	
8				/	
9				/	
10				/	
11				/	
12				/	

CAL 65578

Firma del Experto Informante

UCV
UNIVERSIDAD CÉSAR VALLEJO

Matriz de Validez de ítems de Entrevista a profundidad por Expertos

Experto 3

Apellidos y Nombres del Experto:	Cargo o Institución donde labora:	Nombre del Instrumento
Carlos Jave Luyo	Abogado	Valoración de los ítems del Instrumento

Ítems	Valoración				Descripción
	Deficiente (0)	Regular (1)	Bueno (2)	Excelente (3)	
1				X	
2				X	
3				X	
4				X	
5				X	
6				X	
7				X	
8			X		
9				X	
10				X	
11				X	
12				X	

CARLOS RICARDO JAVE LUYO
Abogado
Registro C.A.L. N° 68830

Firma del Experto Informante

UCV
UNIVERSIDAD CÉSAR VALLEJO

Matriz de Validez de ítems de Entrevista a profundidad por Expertos

Experto 4

Apellidos y Nombres del Experto:	Cargo o Institución donde labora:	Nombre del Instrumento
Nataly Morón Salas	Abogado	Valoración de los ítems del Instrumento

Ítems	Valoración				Descripción
	Deficiente (0)	Regular (1)	Bueno (2)	Excelente (3)	
1				/	
2				/	
3				/	
4				/	
5				/	
6				/	
7				/	
8				/	
9				/	
10				/	
11				/	
12				/	

Jefa(e) Primero C.J
Jefe de la Oficina de Asesoría Legal
Nataly MORÓN Salas
00216082

Firma del Experto Informante