UNIVERSIDAD PRIVADA DE TACNA

FACULTAD DE DERECHO Y CIENCIAS JURÍDICAS

ESCUELA PROFESIONAL DE DERECHO

TESIS

TRATAMIENTO PENAL DE LOS DELITOS INFORMÁTICOS Y LA CIBERDELINCUENCIA EN EL DISTRITO JUDICIAL DE TACNA, 2019-2022

Presentado por:

Kennedy Lincoln Carbajal Cerrón

Código orcid: 0009-0009-3258-8172

Asesor:

Dr. Omar Pezo Jimenez

Código orcid: 0000-0001-7932-7206

Para obtener el Título Profesional de:

ABOGADO

TACNA – PERÚ

2025

UNIVERSIDAD PRIVADA DE TACNA

FACULTAD DE DERECHO Y CIENCIAS JURÍDICAS

ESCUELA PROFESIONAL DE DERECHO

TESIS

TRATAMIENTO PENAL DE LOS DELITOS INFORMÁTICOS Y LA CIBERDELINCUENCIA EN EL DISTRITO JUDICIAL DE TACNA, 2019-2022

Presentado por:

Kennedy Lincoln Carbajal Cerrón

Código orcid: 0009-0009-3258-8172

Asesor:

Dr. Omar Pezo Jimenez

Código orcid: 0000-0001-7932-7206

Para obtener el Título Profesional de:

ABOGADO

TACNA – PERÚ

2025

UNIVERSIDAD PRIVADA DE TACNA

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

Tesis

"TRATAMIENTO PENAL DE LOS DELITOS INFORMÁTICOS Y LA CIBERDELINCUENCIA EN EL DISTRITO JUDICIAL DE TACNA, 2019-2022"

Presentada por:

Bach. Kennedy Lincoln Carbajal Cerrón

Tesis aprobada el día 28 de MAYO del año 2026; ante el siguiente jurado:

PRESIDENTE: **Dr. Carlos Alberto Cueva Quispe**
Mag. / Dr. (Dra.)

SECRETARIO: **Dr. Rolando Jose Balarezo Plata**
Mag. / Dr. (Dra.)

VOCAL: **Mag. Hugo Mora Arce**
Mag. / Dr. (Dra.)

ASESOR: **Dr. Omar Pezo Jimenez**

DECLARACIÓN DE ORIGINALIDAD

Yo Kennedy Lincoln Carbajal Cerrón, en calidad de bachiller de la Facultad de Derecho y Ciencias Políticas de la Universidad Privada de Tacna, identificado(a) con DNI N° 46952450. Soy autor del texto titulado:

"TRATAMIENTO PENAL DE LOS DELITOS INFORMÁTICOS Y LA CIBERDELINCUENCIA EN EL DISTRITO JUDICIAL DE TACNA, 2019-2022".

DECLARO BAJO JURAMENTO

Ser el único autor del texto entregado para obtener el Título Profesional de Abogado, teniendo como asesor al Dr. Omar Pezo Jimenez y que tal texto no ha sido entregado ni total ni parcialmente para obtención de un grado académico en ninguna otra universidad o instituto, ni ha sido publicado anteriormente para cualquier otro fin.

Así mismo, declaro no haber trasgredido ninguna norma universitaria con respecto al plagio ni a las leyes establecidas que protegen la propiedad intelectual.

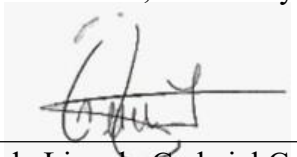
Declaro, que después de la revisión de la tesis con el software Turnitin se declara 20% de similitud, además que el archivo entregado en formato PDF corresponde exactamente al texto digital que presento junto al mismo.

Por último, declaro que la información presentada ha sido obtenida respetando la legislación vigente, es verídica y soy conocedor(a) de las sanciones penales en caso de infringir las leyes del plagio y de falsa declaración, y que firmo la presente con pleno uso de mis facultades y asumiendo todas las responsabilidades de ella derivada.

Por lo expuesto, mediante la presente asumo frente a LA UNIVERSIDAD cualquier responsabilidad que pudiera derivarse por la autoría, originalidad y veracidad del contenido de la tesis, así como por los derechos sobre la obra o invención presentada. En consecuencia, me hago responsable frente a LA UNIVERSIDAD y a terceros, de cualquier daño que pudiera ocasionar por el incumplimiento de lo declarado o que pudiera encontrar como causa del trabajo presentado, asumiendo todas las cargas pecuniarias que pudieran derivarse de ello en favor de terceros con motivo de acciones, reclamaciones o conflictos derivados del incumplimiento de lo declarado o las que encontrasen causa en el contenido de la tesis, libro o invento.

De identificarse fraude, piratería, plagio, falsificación o que el trabajo de investigación haya sido publicado anteriormente; asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad Privada de Tacna.

Tacna, 28 de Mayo del 2026



Kennedy Lincoln Carbajal Cerrón
DNI N° 46952450

DEDICATORIA

A mis padres, hermanos, amigos y compañeros de aula, quienes en el camino siempre me alentaron a cumplir mi anhelo, ser un profesional, gracias por su apoyo incondicional.

AGRADECIMIENTO

Agradezco a Dios, por permitirme cumplir con esta etapa de mi vida. A mis padres quienes con su amor y consejos hicieron posible que hoy en día sea un profesional. A mis docentes, quienes inculcaron conocimientos día a día en las aulas, con mucho respeto doy las gracias, por todo lo recibido.

ÍNDICE

ÍNDICE DE TABLAS

RESUMEN

El estudio analizó el tratamiento penal de los delitos informáticos y la ciberdelincuencia en el Distrito Judicial de Tacna, 2019-2022, buscando determinar en qué medida incide dicho tratamiento en esta problemática. El análisis revela que, a pesar de la adhesión de Perú a convenios internacionales como el de Budapest, existen deficiencias en la implementación y un impacto sociológico limitado. La investigación, de tipo básica y nivel explicativo, utiliza un diseño no experimental, con una muestra de sentencias y magistrados penales, aplicando entrevistas y análisis documental. Los hallazgos indican que el fraude informático que afecta al patrimonio estatal es el delito más recurrente, representando el 64 % de los casos, con penas de hasta 8 años. Las modificaciones normativas recientes (2024) priorizan la protección de bienes jurídicos sensibles y adaptan el marco legal a tecnologías emergentes como la inteligencia artificial. Sin embargo, persisten brechas en la aplicación de sanciones integrales, especialmente en delitos no económicos, y la dependencia de penas privativas podría saturar el sistema penitenciario. Existe una aplicación viable del proceso inmediato en casos de fraude por la existencia de elementos de convicción evidentes. Las implicaciones apuntan a la necesidad de fortalecer la cooperación interinstitucional, la formación especializada y la aplicación de sanciones holísticas.

Palabras Clave: Ciberdelincuencia, Delitos Informáticos, Tratamiento Penal, Legislación, Seguridad Digital.

ABSTRACT

This study analyzed the criminal treatment of computer crimes and cybercrime in the Judicial District of Tacna in 2019-2022, seeking to determine the extent to which such treatment impacts this problem. The analysis reveals that, despite Peru's adherence to international conventions such as the Budapest Convention, there are deficiencies in implementation and a limited sociological impact. The research, of a basic and explanatory nature, uses a non-experimental design, with a sample of criminal courts and judges, applying interviews and documentary analysis. The findings indicate that computer fraud affecting state assets is the most common crime, representing 64 % of cases, with sentences of up to 8 years. Recent regulatory changes (2024) prioritize the protection of sensitive legal assets and adapt the legal framework to emerging technologies such as artificial intelligence. However, gaps persist in the application of comprehensive sanctions, especially for non-economic crimes, and the reliance on custodial sentences could overwhelm the prison system. There is a viable application of immediate prosecution in fraud cases due to the existence of clear evidence. The implications point to the need to strengthen inter-institutional cooperation, specialized training, and the application of holistic sanctions.

Keywords: Cybercrime, Computer Crimes, Criminal Procedure, Legislation, Digital Security.

CAPÍTULO I
INTRODUCCIÓN A LA PROBLEMÁTICA

I. EL PROBLEMA

1.1 Planteamiento del problema

Uno de los Convenios Europeos sobre Ciberdelincuencia, conocido como el Convenio de Budapest, es uno de los primeros acuerdos internacionales a los que Perú se ha adherido para abordar el ciberdelito, su implementación e impacto sociológico, una de las funciones de este acuerdo es el suministro e interceptación de datos. Tal como lo refiere Vinelli (2021) afirma que "la evolución hacia el mundo informático y virtual ha aportado muchos beneficios. Sin embargo, también ha generado innumerables dificultades. Uno de los problemas más relevantes y significativos son las actividades delictivas cometidas a través de los sistemas informáticos".

En referencia Pardo (2018), nos indica que la tecnología ha creado mecanismos para facilitar el uso de monedas virtuales como las tarjetas de crédito, y como resultado, estas nuevas formas de comercio han allanado el camino a los delincuentes informáticos, dando lugar a diversos delitos, entre ellos el fraude electrónico, a partir del uso de tarjetas de crédito, la falsificación de portales web que intentan acceder a información de tarjetas de crédito y llamadas telefónicas haciéndose pasar por banqueros para engañar a los usuarios. proporcionarles indirectamente información confidencial.

Hasta este momento podemos destacar que tanto países como de América latina son las principales víctimas de estas nuevas modalidades de comisión de delitos informáticos generan una afectación al sistema financiero por medio de la suplantación de identidad, al incurrir en error al usuario para así robarle información. Una de las problemáticas, es que no solo basta con que se enriquezcan

de material jurídico, si no también que inviertan en seguridad informática y una adecuada implementación de la norma, es decir la actualización del marco jurídico; ya que la persecución de los delitos informáticos es más compleja que los delitos tradiciones porque requiere necesariamente reunir todos elementos sustanciales para su imputación.

De acuerdo con Chilcon (2020), en el campo de la seguridad nacional, los ciberdelincuentes son fatales, porque en algunas áreas, la seguridad de la información no puede protegerse. En este caso, la seguridad informática en el sector público, especialmente en el caso de seguridad y protección, donde no hay una regla en diferentes sitios web, con protección adecuada; a menudo afecta diferentes ataques a su sistema de información.

El distrito judicial de Tacna no es ajeno a esta problemática ya que la ciberdelincuencia viene aquejando a los ciudadanos que son usuarios de bancos y utilizan aplicativos en sus celulares para realizar transacciones, los llamados ciberdelincuentes están al acecho y haciendo de las suyas, según las denuncias que recibe a diario el personal del Depincri. Entre los casos más comunes destacan el hurto, estafa y el fraude cibernético.

1.2 Formulación del problema

1.2.1. Problema general

¿En qué medida el tratamiento penal de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022?

1.2.2. Problemas específicos

a) ¿En qué medida el tratamiento legislativo de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022?
b) ¿En qué medida el tratamiento procesal de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022?

c) ¿En qué medida el incumplimiento de la finalidad reguladora de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022?

1.3. Justificación e importancia de la investigación

1.3.1 Justificación teórica

Esta investigación obtuvo justificación teórica, debido a que el desarrollo de la parte teórica desarrolla y explica teorías modernas relacionadas sobre los delitos informáticos, debido a su creciente incremento producto de las medidas establecidas por el Estado peruano para contrarrestar la crisis sanitaria.

1.3.2 Justificación práctica

Cabe señalar que en la actualidad existe inestabilidad legislativa en materia de sanción de delitos informáticos, debido a que la legislación vigente no comprende y no se adapta a la realidad que debe ser sancionada y, más aún, frente a la cantidad de delincuencia existente en la red.

1.3.3 Justificación metodológica

En cuanto a la metodología, en la generación de conocimiento científico, este estudio utiliza un conjunto de técnicas, métodos y herramientas para la recolección y análisis de datos, así como una metodología que se diferencia de otras investigaciones previas relacionadas con este tema.

1.3.4 Importancia

Este estudio aborda los delitos informáticos contra el patrimonio, como hurto, sabotaje, estafa y fraude, temas que tienen implicaciones jurídicas, teóricas y académicas debido a su escasa investigación. Su relevancia radica en la clasificación de estos delitos, lo que contribuye a una mejor comprensión y regulación legal. En cuanto a los Objetivos de Desarrollo Sostenible (ODS), este trabajo se alinea principalmente con el ODS 16: Paz, Justicia e Instituciones Sólidas, ya que promueve la creación de marcos legales más robustos para combatir

el cibercrimen, fortaleciendo así la justicia y la seguridad en el entorno digital. Además, al fomentar la investigación en un área poco explorada, también aporta al ODS 9: Industria, Innovación e Infraestructura, al impulsar el desarrollo de conocimientos y tecnologías que protejan los sistemas informáticos y la información.

1.4 Objetivos de la investigación

1.4.1 Objetivo general

Analizar la incidencia del tratamiento penal de los delitos informáticos en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.

1.4.2. Objetivos específicos

a) Determinar la incidencia del tratamiento legislativo de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.
b) Identificar la incidencia del tratamiento procesal de los delitos informáticos en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022
c) Establecer la incidencia del incumplimiento de la finalidad reguladora de los delitos informáticos en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.

I.5 HIPÓTESIS

I.5.1 Hipótesis general

El tratamiento penal de los delitos informáticos incide significativamente en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.

1.5.2 Hipótesis específicas

a) El tratamiento legislativo de los delitos informáticos incide significativamente en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.
b) El tratamiento procesal de los delitos informáticos incide significativamente en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.

c) El incumplimiento de la finalidad reguladora de los delitos informáticos incide significativamente en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.

CAPÍTULO II
ESTADO DEL ARTE

2.1. Antecedentes del estudio

2.1.1 Nacional

Ventura (2021), el estudio propone tipificar como delitos penales el phishing, smishing y vishing en el sistema jurídico peruano, actualizando la Ley 30096 de Delitos Informáticos para incluir estas modalidades como figuras autónomas. Busca reforzar los mecanismos de prevención mediante herramientas tecnológicas avanzadas y promover la educación en seguridad informática, alineándose con el Plan Nacional de Ciberseguridad 2025. También aborda la falta de especialización legal y tecnológica para la recolección y valoración de pruebas digitales. Estas propuestas se justifican ante el incremento del 42 % en ciberdelitos en Perú durante 2024, destacando la necesidad de armonizar la legislación con estándares internacionales como el Convenio de Budapest.

El estudio identifica problemas estructurales, como la falta de especialización de los operadores jurídicos, la carencia de recursos tecnológicos adecuados y las dificultades para identificar a los perpetradores, lo que limita la efectividad de las investigaciones y procesos judiciales. Estas observaciones son fundamentales para proponer reformas que mejoren la capacidad de respuesta del sistema penal frente a la ciberdelincuencia, tanto en Tacna como a nivel nacional. En resumen, el trabajo contribuye a la discusión sobre la modernización del marco legal y la necesidad de una estrategia integral que combine legislación, tecnología y educación para combatir eficazmente estos delitos.

Vinelli (2021), en los últimos meses, las operaciones comerciales virtuales, como las transferencias a través de monederos digitales, han transformado irreversiblemente nuestra convivencia socioeconómica. Desde marzo de 2020, se

ha adoptado un nuevo modelo de adquisición de activos, pago de servicios y modalidades de trabajo. Esta evolución hacia lo digital ha traído múltiples beneficios, pero también ha generado desafíos significativos. Uno de los más relevantes es el aumento de actividades delictivas cometidas a través de sistemas informáticos, reguladas en la Ley 30096 de Delitos Informáticos, modificada por la Ley 30171. Este artículo abordará los delitos de fraude informático y suplantación de identidad, los más frecuentes en esta nueva realidad.

El aporte principal del estudio radica en su enfoque sobre cómo estas actividades delictivas afectan la convivencia socioeconómica actual, evidenciando la necesidad de una legislación más robusta y actualizada. Además, subraya la importancia de comprender las modalidades de estos delitos para mejorar las estrategias de prevención y sanción. En resumen, el trabajo contribuye a la discusión sobre la adecuación del marco legal peruano frente a los desafíos de la ciberdelincuencia, ofreciendo un análisis crítico y propuestas para fortalecer la protección de los ciudadanos en el entorno digital.

Chilcon (2020) , la investigación busca evaluar el impacto del cibercrimen en la seguridad del país, empleando un enfoque cuantitativo con alcance descriptivo-explicativo y un diseño no experimental. La población estudiada incluye a 580 funcionarios de la Policía Nacional, el Ministerio Público y el Poder Judicial, con una muestra de 231 personas. Para el análisis, se utilizó un cuestionario tipo Likert y la prueba chi cuadrado, con el fin de validar las hipótesis planteadas.

El estudio no solo evidencia la relación directa entre cibercrimen y seguridad nacional, sino que ofrece un marco empírico para diseñar políticas públicas basadas en datos, cruciales en un contexto donde Perú recibe 107 ciberataques por minuto y el comercio electrónico amplía vectores de riesgo.

Gallegos (2022), el trabajo aborda los criterios necesarios para la revisión y uso de pruebas digitales en procedimientos judiciales, analizando aspectos relacionados con el cibercrimen, la Convención de Budapest y los estándares internacionales y nacionales. También se examinan las pruebas obtenidas y las

evidencias digitales dentro del proceso legal. Además, se destaca la evolución del perfil del ciberdelincuente, que ha pasado de ser un experto en computadoras con fines económicos a un actor más diverso y sofisticado en sus métodos y objetivos.

El estudio subraya la importancia de garantizar la autenticidad, integridad y licitud de las pruebas digitales, proponiendo estándares técnicos como la cadena de custodia digital y la capacitación de los operadores judiciales. Estas recomendaciones son cruciales para fortalecer la seguridad jurídica y proteger derechos fundamentales como la privacidad y el debido proceso.

Pardo (2018), *l*a investigación evaluó la eficacia del marco legal peruano frente a estos delitos, empleando métodos cualitativos y técnicas como la entrevista. Se concluyó que el tratamiento es deficiente, ya que se agrupan erróneamente todas las modalidades de delitos informáticos bajo el concepto de fraude informático, lo que genera incertidumbre normativa y dificulta su sanción efectiva. Esto subraya la necesidad de una legislación más específica y especializada, que diferencie claramente las modalidades delictivas y mejore la protección del patrimonio en el ámbito digital.

El trabajo subraya la necesidad de una legislación más especializada y actualizada, que incorpore estándares internacionales como el Convenio de Budapest. Esto permitiría una mejor protección del patrimonio frente a las nuevas modalidades de ciberdelincuencia, especialmente en un contexto donde los delitos informáticos han evolucionado rápidamente. En resumen, el estudio aporta una base para reformar y fortalecer el sistema legal peruano, asegurando una respuesta más eficaz y precisa ante los desafíos de la ciberdelincuencia.

Zarzosa (2018), la investigación describe cómo se maneja la prueba digital en este contexto, concluyendo que es insuficiente y carece de un tratamiento especial en el Código Procesal Penal de 2004, regulándose solo como prueba documental según el Artículo 185º. El Ministerio Público enfrenta limitaciones tecnológicas que dificultan su manejo adecuado, y la obtención de estas pruebas debe respetar los derechos fundamentales, ya que su vulneración puede llevar a la

exclusión probatoria. Finalmente, la incorporación y valoración de la prueba digital están sujetas al debate en juicio, y el juez no puede valorar pruebas obtenidas ilegalmente, conforme al Artículo 159º.

El estudio enfatiza la importancia de respetar los derechos fundamentales durante la obtención de pruebas digitales, ya que su vulneración puede llevar a la exclusión probatoria, conforme al Artículo 159º. Esta observación subraya la necesidad de un equilibrio entre la eficacia en la investigación y la protección de garantías constitucionales. En resumen, el trabajo aporta una base crítica para reformar el marco legal y mejorar la capacidad institucional en el tratamiento de pruebas digitales, asegurando su integridad y validez en el proceso penal.

2.1.2 Internacional

Schirakian (2021), en los Códigos Procesales Penales del país, no se establecen medios de prueba específicos para la incorporación de evidencia digital en investigaciones penales. Ante este vacío legal, los operadores judiciales han recurrido al principio de "libertad probatoria" y a la analogía como herramientas para su uso. Sin embargo, esta situación ha generado problemas significativos, vulnerando derechos y garantías de los ciudadanos. Esto plantea una interrogante crucial: ¿es posible garantizar un proceso penal respetuoso de las garantías y derechos del imputado en ausencia de una regulación clara y específica? La respuesta subraya la urgencia de actualizar la normativa para adaptarla a los desafíos de la era digital.

El estudio subraya la necesidad de una actualización legislativa que establezca procedimientos específicos para la obtención, preservación y valoración de las pruebas digitales, garantizando su integridad y respeto a los derechos fundamentales. En resumen, el texto pone en evidencia la urgencia de una regulación más precisa y especializada en el tratamiento de la evidencia digital dentro del sistema penal.

Saltos et al., (2021), el estudio aborda el crecimiento exponencial de los delitos informáticos en América Latina, destacando la necesidad de comprender

esta problemática desde un enfoque conceptual y jurídico. Su objetivo es elaborar un mapeo conceptual y análisis jurídico para entender el ciberdelito en Ecuador, utilizando métodos como mapas conceptuales, análisis histórico y jurídico. Los resultados evidencian que el avance de la tecnología de la información ha impulsado el aumento de estos delitos, subrayando la importancia de mejorar su tipificación y análisis jurídico. En resumen, el trabajo aporta una herramienta clave para enfrentar los desafíos de la ciberdelincuencia desde una perspectiva legal y conceptual.

El trabajo subraya la necesidad de una legislación más especializada y actualizada, que incorpore estándares internacionales como el Convenio de Budapest. Esto permitiría una mejor protección del patrimonio frente a las nuevas modalidades de ciberdelincuencia, especialmente en un contexto donde los delitos informáticos han evolucionado rápidamente. En resumen, el estudio aporta una base para reformar y fortalecer el sistema legal peruano, asegurando una respuesta más eficaz y precisa ante los desafíos de la ciberdelincuencia.

Benavides & SanMartín (2021), el trabajo investiga la regulación de los delitos informáticos en el Código Orgánico Integral Penal (COIP) de Ecuador y su relación con el Convenio de Budapest, principal instrumento internacional contra la ciberdelincuencia. Dado que Ecuador no se ha adherido a este convenio, su legislación carece de un marco completo para enfrentar eficazmente la cibercriminalidad. El estudio busca determinar los beneficios que traería la adhesión, como la armonización legal, la cooperación internacional y la actualización de sanciones. La investigación se basa en una revisión teórica y académica, analizando las deficiencias del sistema legal ecuatoriano y proponiendo mejoras para su modernización.

El trabajo contribuye a la discusión sobre la necesidad de fortalecer la legislación nacional mediante la adopción de instrumentos internacionales, lo que permitiría una respuesta más efectiva y coordinada frente a los desafíos de la ciberdelincuencia.

Rivera (2021), en el estudio busca proponer soluciones viables para prevenir los delitos informáticos en el sistema financiero ecuatoriano, analizando el Código Orgánico Integral Penal (COIP) y la normativa nacional para identificar las obligaciones y responsabilidades de las instituciones financieras, así como los recursos disponibles para las víctimas. Mediante encuestas, se evaluará la incidencia de ciberdelitos financieros entre 2020 y 2021 y el nivel de conocimiento de los usuarios sobre el tema. Se propone la creación de un curso de capacitación para funcionarios involucrados en el proceso. Como conclusión, se destaca la necesidad de fortalecer el sistema y la normativa para reducir el incremento de estos delitos en 2022.

El estudio destaca la urgencia de fortalecer la normativa y el sistema de prevención para reducir el incremento de ciberdelitos financieros, lo que implica una actualización legal y una mayor inversión en tecnología y capacitación. Este trabajo contribuye a la discusión sobre cómo mejorar la seguridad digital en el sector financiero, protegiendo tanto a las instituciones como a los usuarios.

Bañón (2020), el trabajo busca analizar el artículo 248.2 del Código Penal (CP) para resolver las controversias y conflictos de interpretación generados por el uso generalizado de programas informáticos. Examina si la regulación actual es adecuada para abordar las nuevas modalidades de estos delitos y propone medidas preventivas y soluciones basadas en experiencias judiciales, normativa europea y regulaciones de otros países. El desarrollo de nuevas tecnologías ha creado escenarios delictivos emergentes, lo que ha llevado a la incorporación de nuevos ilícitos en el Código Penal, como la estafa informática, para adaptarse a estas formas de delincuencia.

El trabajo contribuye a la discusión sobre la modernización del marco legal, proponiendo mejoras que permitan una respuesta más efectiva y precisa ante los desafíos de la ciberdelincuencia, especialmente en un contexto donde las tecnologías evolucionan rápidamente y generan nuevas formas de delitos.

Arrabal (2019), el presente trabajo de investigación tiene por objeto el análisis doctrinal y jurisprudencial de la prueba tecnológica desde un punto de vista procesal. Y ello, debido al auge de las nuevas tecnologías y al uso generalizado que la sociedad hace de ellas, es habitual que constituyan fuente de prueba en aquellos conflictos en los que medie su utilización. Ampliar la tutela de la intimidad personal y familiar a la información publicada en Internet, enmarcar las comunicaciones telemáticas en la garantía del derecho del 18.3 CE o reconocer la protección de datos son ejemplos de la adaptación de los derechos fundamentales a la nueva realidad tecnológica.

El estudio propone ampliar la tutela de la intimidad a la información publicada en Internet, reconociendo los desafíos de la digitalización. Además, subraya la importancia del reconocimiento de la protección de datos como un derecho fundamental adaptado a la era tecnológica, lo que implica fortalecer el marco legal. En resumen, busca adaptar los derechos fundamentales a los desafíos de la era digital.

2.2 Bases Teóricas

2.2.1 Tratamiento penal de los delitos informáticos

2.2.1.1 Definición

El delito informático, según (Tellez, 2019), se conceptualiza como una conducta ilícita que utiliza la tecnología informática como método, medio o fin para su comisión. Específicamente, Téllez distingue dos tipos de delito informático:

- Delito informático típico: Conductas típicas, antijurídicas y culpables en las que las computadoras son utilizadas como instrumento o fin.
- Delito informático atípico: Actitudes ilícitas en que las computadoras también son instrumento o fin, pero que no encajan en las conductas típicas penalmente tipificadas. (p.462).

Otras definiciones complementarias que coinciden con esta visión incluyen:

María de la Luz Lima define “el delito informático en sentido amplio como cualquier conducta criminal que utiliza tecnología electrónica como método, medio

o fin, y en sentido estricto, como cualquier acto ilícito penal en que las computadoras y sus funciones desempeñan un papel relevante".

Carlos Sarzana, lo entiende "como cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo".

La OCDE define "el delito informático como cualquier comportamiento antijurídico, no ético o no autorizado relacionado con el procesamiento automático o transmisión de datos".

Para Hilda Callegari, define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

Rafael Fernández Calvo, define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título I de la Constitución Española".

De acuerdo a Prieto & Vargas (2020) el Ciberdelito (o delitos informáticos) es cualquier crimen donde la tecnología de la información y la comunicación es: 1) utilizado como una herramienta en la comisión de un delito; 2) el objetivo de un delito; 3) un dispositivo de almacenamiento en la comisión de un delito (p. 14).

El ciber delito según (Vinelli, 2021) "es cualquier acto criminal en el que la tecnología de la información y la comunicación (TIC) funciona como herramienta, objetivo o dispositivo de almacenamiento en la comisión del ilícito. Incluye conductas como la invasión de sistemas mediante claves de acceso, la difusión de malware y el robo de datos personales o corporativos. Se caracteriza por el uso de dispositivos informáticos para configurar el delito, ya sea como medio o fin, y puede tener fines económicos o de daño. Además, afecta la seguridad informática y la intimidad de las personas, siendo una actividad antijurídica y culpable que requiere una legislación especializada para su prevención y sanción".(p.135)

“El ciberdelito, también conocido como delito informático o delito cibernético, es toda acción antijurídica cometida en el entorno digital, utilizando computadoras, redes, sistemas informáticos o cualquier tecnología de la información y comunicación (TIC) como medio o fin del acto ilícito”. (Vinelli, 2021).

Estos delitos pueden tener como objetivo tanto los datos y sistemas informáticos como bienes jurídicos tradicionales, como el patrimonio, la identidad o la privacidad de las personas.

Ámbitos de Afectación

1. Contra datos y sistemas informáticos

- “Ataques a la integridad, disponibilidad o confidencialidad de datos y sistemas, como sabotaje, destrucción, alteración o acceso no autorizado a sistemas informáticos.
- Distribución de malware, ransomware, virus, troyanos y otros programas maliciosos que dañan o inutilizan sistemas o roban información.
- Corrupción, manipulación o robo de bases de datos públicas o privadas.

2. Contra bienes jurídicos tradicionales

- Fraude informático: Manipulación o alteración de sistemas para obtener un beneficio económico indebido, afectando el patrimonio de las víctimas.
- Suplantación de identidad (phishing): Engaño para obtener datos personales y cometer fraudes o acceder a recursos económicos de terceros.
- Robo de identidad: Utilización no autorizada de datos personales para realizar compras, contratar servicios o acceder a cuentas bancarias.
- Estafas y transferencias no consentidas de activos mediante manipulación informática”. (Rivera, 2021).

2.2.1.2 Características de los delitos informáticos.

De acuerdo a Vargas (2022), los delitos informáticos se caracterizan por su alcance internacional, ya que no requieren proximidad física para su comisión, y por la limitada efectividad de la justicia, debido a la escasez de denuncias y a la falta de regulación y persecución especializada. Estos ilícitos suelen ser dolosos, generan graves pérdidas económicas y presentan dificultades técnicas en su demostración, requiriendo especialistas para su investigación. Además, se concretan en tiempo y espacio reducidos, aprovechando el avance tecnológico y el desconocimiento de las víctimas. Son conductas ocupacionales, ya que los delincuentes suelen actuar en entornos laborales, y se consideran delitos de cuello blanco, pues requieren conocimientos técnicos. Finalmente, son actos emergentes, cada vez más sofisticados y especializados, y pueden incluir delitos tradicionales como el hurto o el fraude, pero empleando medios informáticos, lo que exige una legislación específica.

2.2.1.3 Teorías aplicables

a) Teoría Constitucionalista

Esta teoría se centra en la protección de los derechos fundamentales, tales como la intimidad y la propiedad, que están garantizados por la Constitución. Los derechos fundamentales son considerados atributos esenciales de la dignidad humana y límites al ejercicio de la soberanía estatal, siendo exigibles frente a todos los órganos y autoridades del Estado, así como a particulares. “La Constitución delimita estos derechos, fijando sus atributos y límites, y establece que no pueden ser limitados por normas infraconstitucionales que no estén explícita o implícitamente reconocidas en el texto constitucional”. (Bañón, 2020).

b) Teoría del Bien Jurídico

Esta teoría considera a los sistemas informáticos como un bien jurídico colectivo que merece protección penal específica. En el ámbito de los delitos

informáticos, se reconoce un bien jurídico propio, relacionado con la funcionalidad informática, que abarca las condiciones que permiten que los sistemas informáticos operen adecuadamente para el almacenamiento, tratamiento y transferencia de datos. Este bien jurídico es instrumental y colectivo, vinculado con el libre desarrollo de la persona y el funcionamiento de las instituciones en un Estado democrático de derecho. La protección penal debe ser acotada y racional, evitando sancionar cualquier afectación menor que obstaculice actividades legítimas de los ciudadanos. “Se propone que la intervención penal se justifique cuando se afecte la funcionalidad informática en un contexto de redes computacionales, considerando la gravedad y jerarquía de los intereses protegidos”. (Bañón, 2020).

c) Ultima Ratio

La intervención penal debe reservarse para conductas de alta lesividad, es decir, para aquellas acciones que causan un daño significativo o grave al bien jurídico protegido. Esto implica que el derecho penal actúa como último recurso para proteger intereses jurídicos esenciales, evitando la penalización excesiva o desproporcionada frente a afectaciones menores o de baja relevancia social. “Estas teorías se complementan para fundamentar la protección jurídica de los derechos fundamentales y de los sistemas informáticos, orientando la intervención penal hacia los casos de mayor gravedad y relevancia social”. (Bañón, 2020).

2.2.1.4 Problemáticas en la persecución

a) Inmediatez tecnológica

La rápida evolución tecnológica supera la capacidad de actualización de la legislación penal, generando un desfase entre las nuevas técnicas delictivas y las normas vigentes. “Por ejemplo, modalidades recientes como el ransomware, que consiste en el secuestro de datos mediante software malicioso para exigir rescate, no siempre están contempladas de manera específica en las leyes actuales, dificultando su persecución efectiva”. (González et al., 2018).

b) Extraterritorialidad

Los delitos informáticos suelen ser transnacionales, ya que el ciberespacio no reconoce fronteras físicas. Esto implica que la conducta delictiva puede iniciarse en un país, afectar a víctimas en otro y generar ganancias en un tercero, lo que complica la investigación y sanción debido a la diversidad de jurisdicciones y marcos legales. "Aunque existen principios internacionales para abordar la extraterritorialidad, como el de nacionalidad o protección, la coordinación entre Estados sigue siendo un desafío para la persecución efectiva". (González et al., 2018).

c) Prueba digital

La evidencia electrónica es fundamental en los casos de ciberdelincuencia, pero es especialmente vulnerable debido a la facilidad de manipulación, alteración o destrucción. "La persecución de los delitos informáticos enfrenta retos significativos por la velocidad de la innovación tecnológica, la complejidad transnacional de los crímenes y la fragilidad de las pruebas digitales, aspectos que requieren una constante actualización normativa, cooperación internacional". (González et al., 2018).

2.2.1.5 Clasificación doctrinal

A) Según el rol de la tecnología

Los delitos informáticos puros que dañan sistemas o datos son definidos por (Vinelli, 2021) como el hacking y el uso de malware, entre otros actos ilícitos que afectan la integridad, disponibilidad y confidencialidad de los sistemas informáticos y la información contenida en ellos.

a) Hacking

El hacking es un delito que consiste en el acceso no autorizado a sistemas informáticos, vulnerando las medidas de seguridad establecidas para impedirlo. Este delito está tipificado en el artículo 197 bis del Código Penal español, que castiga con pena de prisión de seis meses a dos años a quien, mediante programas u otros dispositivos, se infiltra en sistemas informáticos para descubrir información confidencial sin autorización. El hacking implica una intromisión remota,

generalmente a través de internet, y puede afectar datos bancarios, secretos empresariales, información médica, entre otros. Es una violación de la esfera de exclusividad del titular del sistema y representa un peligro real para la integridad del sistema y la privacidad de los datos. (p.27)

b) Malware

El malware es software malicioso diseñado para dañar o realizar acciones no deseadas en sistemas informáticos. Puede infectar redes, controlar la actividad online de la víctima, robar datos o restringir el acceso a sistemas mediante técnicas como el ransomware (secuestro de datos). El malware puede ser tanto una herramienta para cometer delitos como un delito en sí mismo cuando se usa para dañar sistemas o datos. Está regulado en los artículos 264 y 264 bis del Código Penal, que castigan la destrucción, daño, alteración o inaccesibilidad grave de datos, programas o documentos electrónicos ajenos, con penas de prisión de seis meses a tres años. El malware representa una amenaza creciente debido a la interconexión global de los sistemas informáticos y su facilidad de adquisición por parte de ciberdelincuentes. (p.27)

Otros delitos relacionados

Además del hacking y el malware, existen otros delitos informáticos que pueden dañar sistemas o datos, como:

- “Phishing: suplantación de identidad para engañar a la víctima y obtener información confidencial o instalar software malicioso.
- Ransomware: tipo de malware que bloquea el acceso a sistemas o datos y exige un rescate para liberarlos.
- Sabotaje cibernético: destrucción o alteración de archivos o sistemas con fines de daño industrial o individual.
- Los delitos informáticos puros que dañan sistemas o datos se centran en la intrusión no autorizada (hacking) y el uso de software malicioso (malware) para alterar, destruir o controlar sistemas y la información contenida en

ellos, constituyendo una amenaza significativa para la seguridad informática y la privacidad.

Delitos informatizados: Conductas tradicionales potenciadas por TIC (ej.: phishing, estafas). Los tipos más comunes de delitos informáticos incluyen una variedad de conductas ilícitas que utilizan la tecnología para afectar sistemas, datos o personas. Entre los más frecuentes se encuentran:

Los delitos informatizados son conductas tradicionales que se han visto potenciadas y facilitadas por las Tecnologías de la Información y Comunicación (TIC). Ejemplos claros de estos delitos incluyen el phishing y las estafas, que utilizan medios digitales para ampliar su alcance y eficacia". (Vinelli, 2021).

2.2.1.5.1 Características de los delitos informatizados

"Son delitos tradicionales (como el fraude o la estafa) que se cometen utilizando herramientas tecnológicas, lo que incrementa su volumen, alcance y rapidez". (Rivera, 2021)

Las TIC actúan como un medio para facilitar la comisión del delito, pero no necesariamente cambian la naturaleza jurídica del mismo.

Estos delitos aprovechan características propias del entorno digital, como el anonimato, la inmediatez, la masividad y la dificultad para obtener evidencia digital.

Ejemplos comunes:

a) "Phishing: Técnica de fraude que consiste en enviar correos electrónicos o mensajes que simulan ser de entidades legítimas (bancos, redes sociales, plataformas de pago) para engañar a la víctima y obtener datos personales o bancarios. Aunque no está tipificado específicamente, se encuadra dentro del delito de estafa y puede conllevar penas de prisión y responsabilidad civil para las entidades que no protejan adecuadamente a sus clientes.

b) Estafas informáticas: Incluyen engaños mediante correos electrónicos, mensajes o páginas falsas que buscan obtener datos o dinero de las

víctimas. Pueden dirigirse a usuarios de bancos, redes sociales, plataformas de pago, servicios públicos o incluso ofertas de empleo falsas.

c) Malware: Programas maliciosos que se instalan sin consentimiento para robar información, dañar sistemas o mostrar publicidad no deseada. Algunos, como el troyano Zeus, han sido usados para obtener datos bancarios de usuarios". (Ventura, 2021).

B) Según el bien jurídico:

Los delitos informáticos pueden clasificarse en función del bien jurídico que protegen según (Lujan, 2022). A continuación, se explica la relación entre los ejemplos dados y los bienes jurídicos afectados, según la doctrina y la normativa relevante:

a) Delitos patrimoniales: Fraude electrónico, robo de datos.

Estos delitos afectan principalmente al patrimonio, entendido como el conjunto de bienes, derechos y obligaciones con contenido económico de una persona o entidad. El fraude informático (o fraude electrónico) consiste en manipular sistemas o datos informáticos para obtener un beneficio económico indebido, perjudicando el patrimonio de la víctima. "El robo de datos, cuando implica la apropiación de información con valor económico, también se encuadra en la protección del patrimonio". (Lujan, 2022).

La doctrina y la legislación (por ejemplo, la Ley 30096 en Perú) coinciden en que el bien jurídico principal protegido en estos casos es el patrimonio, aunque pueden existir afectaciones secundarias a otros intereses, como el correcto funcionamiento de los sistemas informáticos.

b) Delitos contra la personalidad: Suplantación de identidad, ciberacoso

"Estos delitos lesionan bienes jurídicos relacionados con la personalidad, como la identidad, la honra, la privacidad y la integridad moral o psíquica de las personas. La suplantación de identidad implica el uso indebido de datos personales para hacerse pasar por otra persona, afectando su derecho a la identidad y, en

muchos casos, su reputación y privacidad. El ciberacoso vulnera la integridad moral y psicológica de la víctima, atentando contra su dignidad y tranquilidad personal. En ambos casos, el bien jurídico protegido es la personalidad de la víctima, en sus distintas manifestaciones". (Pardo, 2018).

c) Delitos de carácter colectivo: Ataques a infraestructuras críticas

Los ataques a infraestructuras críticas (como servicios de energía, agua, telecomunicaciones, salud, etc.) afectan intereses colectivos, pues ponen en riesgo la seguridad, el orden público y el funcionamiento de servicios esenciales para la sociedad. El bien jurídico protegido aquí es colectivo, ya que la funcionalidad y disponibilidad de estos sistemas informáticos es relevante para toda la comunidad, no solo para individuos concretos. "La doctrina resalta que la "funcionalidad informática" de estos sistemas constituye un bien jurídico de carácter colectivo, pues su afectación repercute en el libre desarrollo y seguridad de la sociedad en general". (Pardo, 2018)

2.2.1.6 Elementos constitutivos

a) Sujeto activo

"El sujeto activo es el individuo que realiza la acción típica descrita en el tipo penal. En el caso de los delitos informáticos, suele tratarse de personas con habilidades técnicas para manipular sistemas, aunque también puede ser un lego en la materia o incluso empleados de áreas no informáticas que tengan acceso a los sistemas. Lo característico es que poseen conocimientos o acceso que les permite ejecutar la conducta ilícita.

b) Sujeto pasivo

El sujeto pasivo es la persona natural o jurídica, o incluso el Estado, sobre quien recae la conducta delictiva y que resulta afectada en sus bienes jurídicos. En delitos informáticos, el sujeto pasivo puede ser cualquier individuo, empresa, institución pública o privada, o el propio Estado, especialmente cuando se atacan sistemas públicos o de interés colectivo.

c) Bien jurídico protegido

El bien jurídico protegido en los delitos informáticos es, principalmente, la información en sus diferentes dimensiones:

- Confidencialidad: Garantiza que la información solo sea accesible para personas autorizadas, protegiendo la privacidad y evitando la divulgación no autorizada.
- Integridad: Asegura que los datos no sean alterados o manipulados sin autorización, preservando su exactitud y legitimidad.
- Disponibilidad: Busca que la información esté accesible para los usuarios autorizados cuando la requieran, incluso ante incidentes o ataques.

Estos principios son la base de la seguridad informática y constituyen el núcleo de protección frente a los delitos informáticos.

d) Derechos fundamentales involucrados

Entre los derechos fundamentales afectados por los delitos informáticos destacan:

- Privacidad: Reconocida en el artículo 2.6 de la Constitución Peruana, que protege el derecho a la intimidad y a la protección de datos personales.
- Propiedad intelectual: Relacionada con la protección de la información y los derechos sobre los datos y sistemas informáticos". (Custodio, 2021).

2.2.1.7 Tipos de delitos informáticos.

De acuerdo a (Pardo, 2018) citando a INTERPOL señalan como delitos informáticos los siguientes:

> Los delitos informáticos abarcan una amplia gama de acciones ilícitas que afectan sistemas, datos y personas, incluyendo ataques contra sistemas informáticos, la difusión de virus o botnets, y la distribución de imágenes

de agresiones sexuales contra menores. También destacan las estafas en línea, la intrusión en servicios financieros, el phishing (adquisición fraudulenta de información personal) y la usurpación de identidad. Además, se relacionan con riesgos en redes sociales, como el acceso a material inadecuado, el ciberbullying, el cibergrooming, el sexting y los robos de identidad. Estos delitos pueden clasificarse según los bienes jurídicos protegidos, como el patrimonio, la persona, la fe pública, la seguridad, los datos y los sistemas informáticos, reflejando su impacto multidimensional en la sociedad digital. (p.36)

"En este orden de ideas, dentro de cada tipo de delito se puede identificar otros sub tipos de delitos, así, dentro de delitos informáticos contra el patrimonio se puede identificar al fraude, hurto, estada y sabotaje informático; dentro de los delitos informáticos contra la persona está contra la libertad sexual, en delitos informáticos contra la fe pública se encuentra la falsedad y sucesivamente". (Ventura, 2021).

Es evidente que los delitos informáticos presentan una gran diversidad y que su clasificación varía según el enfoque adoptado. Esta situación refleja una carencia de consenso teórico sobre cómo categorizarlos, lo que a su vez provoca un abordaje jurídico incompleto e insuficiente. Además, esta falta de claridad conceptual se traduce en una deficiencia legislativa estricta, ya que sin una base teórica sólida resulta aún más difícil contar con una regulación adecuada. (Gamba, 2019).

2.2.1.8 Clasificación de los delitos informáticos

"Muchas son las clasificaciones que se han dado sobre delitos informáticos, por lo que consideramos que el jurista mexicano Julio Téllez Valdez, como se citó en (González et al., 2018), clasifica a los delitos informáticos de acuerdo a dos criterios":

2.2.1.8.1 Como instrumento o medio

Esta categoría comprende conductas delictivas que utilizan computadoras como herramienta o medio para cometer ilícitos. Entre ellas se incluyen la falsificación de documentos electrónicos, manipulación contable, planeamiento de delitos tradicionales mediante sistemas informáticos y acceso o apropiación indebida de información confidencial. También abarcan la modificación y alteración de datos, uso no autorizado de software, introducción de virus y accesos ilegales a sistemas o líneas de comunicación informática. Estas acciones evidencian cómo la tecnología se emplea para facilitar diversos tipos de delitos en el ámbito digital.

2.2.1.8.2 Como fin u objetivo

De acuerdo a (Prieto & Vargas, 2020)

Esta categoría incluye conductas delictivas dirigidas directamente contra el hardware, accesorios o programas como entidades físicas, tales como bloqueo total del sistema, destrucción o daño de programas y memoria, así como ataques físicos a las máquinas y sabotajes con multas políticas o terroristas. También abarca el secuestro de soportes magnéticos para chantajes. Estas conductas se dividen en fraude por manipulación, espionaje y robo de software, sabotaje informático, robo de servicios, acceso no autorizado a sistemas y ofensas tradicionales en negocios apoyados por computadora, evidenciando diferentes formas de ataques físicos y lógicos contra sistemas informáticos.

2.2.1.9 Caracterización del delincuente informático

De acuerdo a (Lujan, 2022), Los sujetos activos de estas conductas delictivas suelen ser mayormente jóvenes hombres, con alta inteligencia, gran capacidad lógica y habilidades destacadas en el manejo de computadoras, a menudo actuando de forma individual. No suelen tener antecedentes penales y, en el caso de los llamados “hackers”, ven su actividad como un desafío o juego, aprovechando debilidades en la seguridad informática. También incluyen técnicos autodidactas y empleados destacados y motivados en sus ámbitos laborales. Finalmente, en casos de fraude, se trata de especialistas cuyo perfil encaja dentro de los llamados “delitos de cuello blanco”.

2.2.1.10 Casos emblemáticos de ciberdelincuencia en Perú

a) Phishing bancario:

"(Bañón, 2020) señala una modalidad frecuente es la suplantación de plataformas financieras para engañar a usuarios que para obtener sus datos bancarios. Un caso emblemático fue el ataque de phishing dirigido al "Banco de la Nación" en Perú en 2020, donde se crearon páginas falsas que imitaban la plataforma oficial para robar credenciales y datos personales, afectando a numerosos usuarios.

b) Ataques a instituciones públicas

En 2021, se registraron ataques informáticos que inhabilitaron portales del Estado, como el de la SUNAT, afectando la disponibilidad de servicios públicos digitales y generando perjuicios en la atención al ciudadano y la recaudación tributaria.

c) Fraude informático y suplantación de identidad

Son los delitos más denunciados, representando el 69 % y 22 % respectivamente de los casos reportados en 2024. Estos incluyen estafas mediante redes sociales, correos electrónicos, WhatsApp y otras plataformas digitales, con un impacto económico significativo, como el robo de más de 90 millones de soles solo en Lima Metropolitana en 2024.

e) Otros casos relevantes

Robo de cuentas de WhatsApp para pedir dinero a contactos, falsas ofertas en redes sociales, y manipulación de sistemas públicos, como el caso de fraude informático en el sistema de tarjetas del Tren Eléctrico de Lima, donde se adulteraron tarjetas para obtener acceso ilegal". (p.136).

2.2.1.11 Propuestas de mejora para la lucha contra la ciberdelincuencia en Perú

a) Actualización normativa

"Es necesario tipificar nuevas modalidades delictivas emergentes como el cryptojacking (uso no autorizado de dispositivos para minería de criptomonedas) y deepfake (manipulación audiovisual para suplantación), que actualmente no están contempladas explícitamente en la legislación peruana". (Téllez, 2019).

b) Capacitación judicial

"Fortalecer la especialización de jueces, fiscales y policías en materia de prueba digital y ciberderecho para mejorar la investigación, valoración y sanción de los delitos informáticos, garantizando una adecuada cadena de custodia y manejo técnico de evidencias electrónicas". (Téllez, 2019).

c) Cooperación internacional

Promover la adhesión y participación activa en tratados internacionales como el Segundo Protocolo del Convenio de Budapest, para facilitar la cooperación transfronteriza en investigación y persecución de ciberdelitos, dada la naturaleza global de estas conductas ilícitas. "Estas medidas buscan cerrar brechas legales, técnicas y operativas que actualmente limitan la eficacia en la prevención y sanción de la ciberdelincuencia en Perú". (Téllez, 2019).

2.2.1.12 Dimensiones de delitos informáticos

a) Tratamiento jurídico penal

"En esta investigación, el tratamiento jurídico penal se refiere al análisis doctrinal, dogmático, jurisprudencial, teórico y normativo aplicado a los delitos informáticos, particularmente aquellos que afectan el patrimonio, con especial atención a las modalidades de estafa, fraude, sabotaje y daño informático. Dicho tratamiento jurídico penal se divide a su vez en dos subcategorías principales: el tratamiento procesal y el tratamiento legislativo". (Bañón, 2020).

b) Tratamiento procesal

> "El tratamiento procesal de los delitos informáticos contra el patrimonio, incluyendo modalidades como hurto, estafa, sabotaje y fraude informático, se refiere a las acciones de investigación y manejo de los aspectos procesales necesarios para la sanción de estos delitos. En este contexto, existe un problema significativo debido a la naturaleza particular de estos ilícitos, ya que su consumación puede ocurrir sin estar limitada por barreras espaciales". (Benavides & SanMartín, 2021)

Por ende, el tratamiento procesal de los delitos informáticos contra el patrimonio, como hurto, estafa, sabotaje y fraude, enfrenta desafíos significativos debido a su naturaleza transnacional y la facilidad con que los delincuentes pueden ocultar su identidad y ubicación. Estos delitos pueden consumarse sin restricciones geográficas, complicando la determinación de la jurisdicción y la investigación. Además, la posibilidad de falsificar datos, como la dirección IP, dificulta la identificación del perpetrador, lo que evidencia la necesidad de mecanismos técnicos y normativos más eficaces para combatir estos ilícitos.

2.2.1.13 Tratamiento normativo.

De acuerdo a Vinelli (2021)

> "A nivel nacional, el Código Penal y la Ley de Delitos Informáticos, junto con sus modificaciones recientes, regulan las conductas delictivas en el ámbito digital. En el plano internacional, se aplican las normas de otros países y especialmente el Convenio de Budapest, único tratado internacional sobre ciberdelincuencia suscrito por varios países. Sin embargo, dado que este convenio data de 2001, es necesario revisarlo y actualizar su contenido para que refleje adecuadamente la realidad y los avances tecnológicos actuales de los países firmantes" (p.36).

- **Derecho informático.**

Antes de definir el derecho informático debemos previamente descifrar el término o palabra informática. La palabra informática es un neologismo que deriva

de vocablos información y automatización, el cual fue históricamente sugerido por Phillipe Dreyfus en 1962. “En este orden de ideas, es factible afirmar que la informática es el conjunto de técnicas dirigidas al tratamiento lógico y automatizado de la información con el objetivo de la toma de decisiones eficientes”. (Arrabal, 2019).

En tal sentido, conforme señala (Arrabal, 2019) el Derecho Informático es el tratamiento sistemático y normativo tendiente a regular la informática en sus múltiples aplicaciones (burótica, robótica, telemática Entre otros). “Es una rama del derecho conformada por un conjunto de normas, doctrina, aplicaciones, procesos que tiene por objeto regular toda actividad o conductas vinculadas con las tecnologías informáticas.

2.2.1.14 La informática forense

> “La Informática forense nos permite la solución de problemas íntimamente ligados con seguridad informática y la protección de datos. Basados en ella, las diferentes empresas obtienen una respuesta oportuna para sobreponerse a los delitos informáticos consagrados en la ley tanto nacional como internacional; algunos de ellos son: de privacidad, robo de identidad, acceso no autorizado a cuentas de email o redes sociales, competencia desleal, fraude, robo de información confidencial o espionaje industrial surgidos a través de uso indebido de las tecnologías de la información (…)”. (González et al., 2018)

En este orden de ideas, se puede decir que la informática forense es una disciplina que ayuda a la justicia con el fin de enfrentar y descubrir los diferentes delitos informáticos que se pueden cometer. “Asimismo se encarga de la custodia de la evidencia digital recolectada en la escena del crimen para que ésta sea aportada en los procesos judiciales”.(González et al., 2018)

a) El internet.

De acuerdo a Ventura (2021), “el internet, como medio global de comunicación, ha generado diversas tendencias, entre ellas el aumento de conductas

desviadas y delictivas. Los usuarios se conectan en línea en todos los niveles, pero algunas acciones están dirigidas a perjudicar a muchas empresas, personas, jóvenes y menores, quienes frecuentemente navegan con poca conciencia o ingenuidad. Esta situación resalta la necesidad de mayor educación y protección en el entorno digital".

b) La seguridad informática.

De acuerdo a Vinelli (2021) "La seguridad informática abarca políticas, reglas, estándares, métodos y protocolos para proteger la infraestructura tecnológica y la información que administra. No solo se enfoca en ataques intencionales, sino también en fallas de software o hardware que puedan comprometer la seguridad. Su objetivo es minimizar riesgos de accesos no autorizados o malintencionados. Así, protege la información frente a revelación, uso, modificación o destrucción accidental o intencional" (p. 308).

c) Prevención de delitos informáticos.

Respecto a la prevención de delitos informáticos, Saltos et al. (2021) señalan que toda estrategia de seguridad debe partir de asumir un posible acceso no autorizado y mal uso de datos críticos, estableciendo para garantizar la seguridad adecuada, incluyendo la clasificación de la información según su riesgo. Sin embargo, Lujan (2022) advierte que pocas entidades implementan niveles de seguridad y clasificación de datos basados en riesgos reales. En el ámbito internacional, la ONU desde el 2000 insta a los estados a eliminar refugios para el uso ilícito de tecnologías ya proteger la confidencialidad, integridad y disponibilidad de los datos, penalizando el abuso criminal. (Vargas, 2022; Vinelli, 2021). Estas bases legales y prácticas orientan a fortalecer los sistemas legales y técnicos para prevenir eficazmente el cibercrimen.

2.2.1.15 Bien jurídico protegido

El bien jurídico que se protege de manera principal con este delito, es la "información", entendida de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de

> datos), la cual se encuentra contenida en bases o bancos de datos o el producto de los procesos informáticos automatizados; por lo tanto se constituye en un bien autónomo de valor económico y es la importancia actual del "valor económico" de la información en una sociedad en donde se usan de manera cotidiana las tecnologías de la información y la comunicación, lo que ha hecho que se incorpore como bien jurídico tutelado.(Custodio, 2021).

Podemos identificar varios bienes jurídicos secundarios, como la intimidad, que implica respetar la información personal que no debe ser divulgada públicamente. Además, el acceso ilícito puede afectar el patrimonio, la propiedad y derechos como la indemnización y la libertad sexual. Esto puede dar lugar a la concurrencia de delitos tipificados tanto en la misma ley como en el Código Penal vigente, especialmente aquellos cometidos mediante medios informáticos". (Gamba, 2019)

2.2.1.10 Sujetos activo y pasivo

El sujeto activo es quien ejecuta total o parcialmente una conducta típica del delito de acceso ilícito. Estos individuos, responsables de los llamados delitos informáticos, suelen poseer habilidades especiales en el manejo de sistemas informáticos. Frecuentemente, por su empleo, tienen acceso a información sensible en lugares estratégicos, aunque también pueden ser expertos en tecnología sin relación laboral directa. Esta descripción coincide con el concepto en inglés conocido como *hacker*.(Custodio, 2021).

> "Por su parte, el sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo. En primer término, tenemos que distinguir que sujeto pasivo ó víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso del delito de Acceso Ilícito, las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados en red".(Custodio, 2021).

2.2.1.11 Figuras Agravadas.

El Artículo 2° de la Ley de Delitos Informáticos no menciona estas circunstancias, pero el Artículo 11° establece que la pena privativa de libertad puede aumentarse hasta en un tercio, llegando a 5 años y 4 meses, cuando se dan ciertas condiciones. Estos incluyen que el delito sea cometido por miembros de una organización criminal, mediante abuso de acceso especial a información reservada, con multas de lucro, o cuando afecte la asistencia, defensa, seguridad o soberanía nacional. Estos agravantes buscan sancionar más severamente conductas que generan mayor daño o riesgo.

2.2.1.12 Legislación

- Decreto Legislativo N.º 635 (Código Penal).
- Ley Nº 30096 (Ley de Delitos Informáticos).
- Ley Nº 30171 (Ley que modifica la Ley 30096, Ley de Delitos Informáticos).
- Decreto Legislativo Nº 1182 (Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado).
- Decreto Legislativo Nº 1237 (Decreto Legislativo que modifica el Código Penal, aprobado por el Decreto Legislativo Nº 635).
- Ley Nº 28493, Ley que regula el uso del correo electrónico comercial no solicitado
- (SPAM) y su reglamento D.S. Nº 031-2005-MTC

2.2.1.13 Regulación internacional

a) Convenio de Budapest (2001)

El Convenio de Budapest es el primer y principal tratado internacional sobre delitos informáticos y ciberdelincuencia. Firmado en 2001 y en vigor desde 2004,

su objetivo es armonizar las legislaciones nacionales, mejorar las técnicas de investigación y fortalecer la cooperación internacional entre los Estados firmantes.

El Convenio define delitos clave como acceso ilícito, interceptación ilegal, ataques a la integridad de datos y sistemas, abuso de dispositivos, falsificación y fraude informático, delitos relacionados con la pornografía infantil y violaciones de derechos de autor. Además, establece procedimientos para la obtención y preservación de pruebas electrónicas, y promueve una política penal común para proteger a la sociedad frente al cibercrimen.

b) OCDE: Directrices para la seguridad de sistemas

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) ha emitido directrices internacionales para fomentar la seguridad de sistemas y redes de información. Estas directrices, adoptadas en 2002, promueven una cultura de seguridad, recomiendan a los países miembros establecer políticas y prácticas adecuadas, y fomentan la cooperación nacional e internacional. Su propósito es que tanto gobiernos como empresas y usuarios individuales asuman responsabilidades para prevenir y combatir los delitos informáticos mediante la adopción de medidas técnicas, educativas y legales.

c) Leyes modelo: UNODC y OEA

Organismos internacionales como la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC) y la Organización de los Estados Americanos (OEA) han desarrollado leyes modelo para orientar a los países en desarrollo en la creación de marcos legales eficaces contra la ciberdelincuencia. Estas leyes modelo buscan facilitar la prevención, investigación y sanción de los delitos informáticos, promover la educación y la cooperación internacional, y armonizar las legislaciones nacionales con los estándares internacionales. Además, contemplan la tipificación de delitos, facultades de investigación, jurisdicción, pruebas electrónicas y mecanismos de asistencia y cooperación entre Estados.

En conjunto, estos instrumentos internacionales proporcionan una base sólida para la lucha global contra los delitos informáticos, promoviendo la armonización legislativa y la cooperación transfronteriza.

2.2.1.14 Marco jurídico nacional (Perú)

a) Código Penal

Artículo 190-A: Tipifica el acceso ilícito a sistemas informáticos, sancionando a quien accede sin autorización a sistemas protegidos.

Artículo 196: Regula el fraude informático, penalizando la obtención de provecho ilícito mediante manipulación o interferencia en sistemas o datos informáticos.

b) Ley N.º 30096 (2013) - Ley de Delitos Informáticos

Esta ley tiene por objeto prevenir y sancionar conductas ilícitas que afectan sistemas y datos informáticos, así como otros bienes jurídicos relevantes, cometidas mediante tecnologías de la información y comunicación.

Acceso ilícito (Artículo 2): Pena privativa de libertad de 1 a 4 años y multa para quien accede sin autorización a sistemas informáticos o excede la autorización.

Atentado contra la integridad de datos (Artículo 3): Pena de 3 a 6 años de prisión y multa para quien daña, altera, borra o hace inaccesibles datos informáticos.

Atentado contra la integridad de sistemas (Artículo 4): Pena de 3 a 6 años de prisión y multa para quien inutiliza o imposibilita el funcionamiento de un sistema informático.

Interceptación de datos informáticos (Artículo 7): Pena de 3 a 6 años, con agravantes hasta 10 años si afecta información clasificada o la seguridad nacional.

Fraude informático (Artículo 8): Pena para quien obtiene provecho ilícito mediante manipulación de datos o sistemas informáticos.

La ley también contempla delitos contra la indemnidad y libertad sexuales, la intimidad y el secreto de las comunicaciones, el patrimonio y la fe pública, todos relacionados con el uso indebido de tecnologías.

c) Modificaciones recientes y observaciones

En 2023, la Defensoría del Pueblo señaló vacíos legales en la tipificación de delitos emergentes como el ciberacoso y la difusión de deepfakes, lo que evidencia la necesidad de actualizar y ampliar el marco normativo para cubrir nuevas formas de ciberdelincuencia.

Ley 30096 para fortalecer la prevención y sanción de delitos informáticos, promoviendo un uso seguro y responsable de las tecnologías.

La Ley 30096, promulgada en 2013, es la Ley de Delitos Informáticos en Perú, cuyo objetivo es prevenir y sancionar conductas ilícitas que afectan sistemas y datos informáticos, así como otros bienes jurídicos relevantes, mediante el uso de tecnologías de la información y comunicación.

d) Principales delitos tipificados en la Ley 30096

- Acceso ilícito (Artículo 2): Se sanciona a quien accede sin autorización a todo o parte de un sistema informático, vulnerando medidas de seguridad, con pena privativa de libertad de 1 a 4 años y multa de 30 a 90 días. También se castiga quien excede la autorización para acceder a un sistema.
- Atentado contra la integridad de datos informáticos (Artículo 3): Quien introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos será reprimido con pena privativa de libertad de 3 a 6 años y multa de 80 a 120 días.
- Atentado contra la integridad de sistemas informáticos (Artículo 4): Se sanciona a quien inutiliza total o parcialmente un sistema informático, impide el acceso o entorpece su funcionamiento, con pena de 3 a 6 años y multa de 80 a 120 días.

- Interceptación de datos informáticos (Artículo 7): Pena para quien intercepta datos informáticos en transmisiones no públicas, con agravantes si afecta información clasificada o la seguridad nacional.
- Fraude informático: Se castiga a quien obtiene provecho ilícito mediante manipulación, alteración o interferencia en sistemas o datos informáticos.

La Ley también contempla otros delitos informáticos contra la indemnidad y libertad sexuales, la intimidad y el secreto de las comunicaciones, el patrimonio y la fe pública, otorgando penas efectivas y facultades a jueces, fiscales y policías para su aplicación.

Además, la Ley 30096 se ha modificado para fortalecer su alcance y adaptarse a nuevas formas de ciberdelincuencia, promoviendo un uso seguro y responsable de las tecnologías.

2.2.2 Ciberdelincuencia

2.2.2.1 Definición

"La ciberdelincuencia se refiere estrictamente a cualquier acción ilegal realizada a cabo a través de medios electrónicos que comprometen la seguridad de los sistemas informáticos y la información que gestionan. Estas conductas atentan contra la integridad y protección de datos y sistemas digitales. En esencia, involucra delitos efectuados mediante tecnología informática".(Bullón, 2019).

> "La ciberdelincuencia también abarca, en un sentido amplio, cualquier delito realizado a través de sistemas informáticos o redes de computadoras, incluyendo el acceso o la disposición indebida de información gestionada por dichos sistemas. Esto incluye acciones ilícitas vinculadas directa o indirectamente con tecnologías de la información y comunicación."(Lujan, 2022).

La ciberdelincuencia, delitos informáticos o cibercrimen cuentan con múltiples definiciones doctrinarias que enfatizan distintos aspectos. Algunas la

identifican con actividades ilícitas realizadas a través de redes electrónicas globales o sistemas interconectados, como Internet. Sin embargo, el concepto también abarca afectaciones a sistemas informáticos autónomos que no necesariamente están conectados a una red". (Bañón, 2020).

Así, entre las primeras conceptualizaciones encontramos lo planteado por Felipe Villavicencio, quien desde una perspectiva tendiente a lo restrictivo señala: Por nuestra parte, entendemos a la criminalidad informática como aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es invasión a computadoras, correo o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología. "De la concepción de los delitos informáticos se entiende que no todo delito puede ser clasificado como delito informático por el solo hecho de haber empleado la computadora u otro instrumento tecnológico". (Zarzosa, 2018).

Ahondando más bien en lo que buscan las definiciones más amplias, Miró Linares explica la ciberdelincuencia como categoría tipológica antes que normativa entendiendo que:

> "El cibercrimen, en un sentido amplio, se define como cualquier conducta delictiva realizada en el ciberespacio, un ámbito virtual creado por el uso de tecnologías de la información y comunicación (TIC). Incluye tanto delitos nuevos, vinculados a intereses o bienes específicos del entorno digital, como delitos tradicionales que ahora se cometen a través de Internet. Desde esta perspectiva, el cibercrimen abarca cualquier acto ilícito en el que las TIC desempeñan un papel central en su ejecución. Esto implica particularidades criminológicas, victimológicas y de riesgo penal asociadas a la naturaleza digital de estos delitos. En esencia, el cibercrimen refleja la adaptación de la delincuencia al mundo virtual". (Benavides & San Martín, 2021).
>
> "Por otra parte, cabe resaltar que un concepto conexo es el de Ciberseguridad, el mismo que hace referencia a la organización y recolección de recursos, procesos, tecnologías o estructuras utilizadas para

proteger el ciberespacio y los sistemas potenciados por el ciberespacio (computadoras, servidores, individuos, organizaciones, redes, entre otros) de ataques u ocurrencias que vulneren derechos". (Benavides & SanMartín, 2021).

El cibercrimen, en términos amplios, abarca cualquier conducta delictiva realizada en el ciberespacio, definido como el entorno virtual de interacción mediante tecnologías de la información (TIC). Incluye tanto delitos nuevos, vinculados a intereses o bienes específicos del ciberespacio, como delitos tradicionales que ahora se cometen a través de Internet. Desde esta perspectiva, se entiende como cibercrimen cualquier delito en el que las TIC juegan un papel esencial en su ejecución, lo que implica particularidades criminológicas, victimológicas y de riesgo penal asociadas a este ámbito digital.

2.2.2.2 Definición operativa

Román (2020) entiende como "infracciones que violan la ley mediante tecnología, sin barreras físicas o geográficas", destacando su naturaleza transnacional y la ausencia de limitaciones territoriales para su comisión.

A) Clasificación según la Defensoría del Perú:

a) Delitos facilitados por TIC

"Son delitos tradicionales que se cometen con la ayuda o facilitación de las TIC, como el fraude electrónico y el phishing.

b) Delitos contra TIC

"Son aquellos que tienen como blanco directo las tecnologías o sistemas informáticos, tales como el hacking y la distribución de malware. La ciberdelincuencia puede ser cometida tanto por individuos aislados como por grupos organizados, incluyendo estructuras criminales que ofrecen servicios ilícitos en la *dark web*. Los delitos informáticos afectan a individuos, empresas y gobiernos, y suelen tener objetivos como el robo de dinero, información confidencial, propiedad intelectual o la interrupción de operaciones. La evolución tecnológica

rápida y la sofisticación de los ataques hacen que la ciberdelincuencia sea un fenómeno en constante expansión y complejidad. La ciberdelincuencia abarca diversas modalidades delictivas que utilizan las Tecnologías de la Información y Comunicación (TIC) como medio o fin. Según múltiples fuentes especializadas, las principales tipologías son": (Román, 2020).

1. Delitos contra sistemas y datos informáticos

a) Hacking

"Acceso no autorizado a sistemas o redes para obtener, modificar o destruir información.

b) Malware

Uso de software malicioso como virus, troyanos, spyware o ransomware para dañar o controlar sistemas.

c) Ransomware

Variante de malware que cifra datos y exige rescate económico para liberarlos, constituyendo una forma de ciberextorsión.

d) Ataques DdoS

Saturación de servicios en línea para dejarlos inaccesibles.

e) Botnets

Redes de dispositivos infectados controlados remotamente para realizar ataques o enviar spam"(Gallegos, 2022).

2. Delitos facilitados por TIC (delitos tradicionales con apoyo tecnológico)

a) Phishing

"Suplantación de identidad mediante correos o sitios falsos para obtener datos confidenciales.

b) Fraude informático

Engaños para obtener beneficios económicos ilícitos, incluyendo estafas online y fraudes financieros.

f) Robo de identidad

Obtención y uso fraudulento de datos personales para cometer delitos o fraudes.

g) Ciberacoso

Acoso o intimidación a través de medios digitales, afectando la intimidad y seguridad de la víctima.

h) Ciberextorsión

Intimidación o amenazas mediante tecnología para obtener beneficios o causar daño". (Gallegos, 2022).

3. Delitos relacionados con contenido ilegal o prohibido

Distribución de pornografía infantil y otros contenidos ilegales o que incitan a la violencia o terrorismo. Difusión de fake news o deepfakes con fines ilícitos o malintencionados (en proceso de tipificación en algunos países). (p.40)

2.2.2.3 Tipologías

a) Delitos contra datos

- "Violación de datos personales: Obtención, sustracción, divulgación o uso no autorizado de datos personales contenidos en bases de datos o archivos.
- Suplantación de sitios web para capturar datos personales (phishing): Creación de páginas falsas para obtener información sensible.
- Alteración, destrucción o corrupción de datos: Modificación o eliminación ilícita de datos informáticos.
- Intercepción no autorizada de datos informáticos: Captura ilegal de datos durante su transmisión.

b) Delitos económicos

- Fraude informático: Obtención de beneficios económicos mediante manipulación de sistemas o datos.
- Hurto por medios informáticos: Robo de activos o información a través de sistemas informáticos.
- Transferencia no consentida de activos: Transferencias ilegales de dinero o activos digitales.
- Ransomware: Secuestro de datos para exigir rescate económico.
- Phishing y vishing: Suplantación para obtener datos bancarios o financieros.

c) Delitos contra personas

- Ciberacoso (cyberbullying): Hostigamiento, intimidación o persecución mediante medios digitales.
- Sextorsión y grooming: Chantaje sexual a través de medios digitales, especialmente a menores.
- Revelación de secretos: Difusión no autorizada de información privada o imágenes íntimas.
- Suplantación de identidad: Uso fraudulento de datos personales para perjudicar a alguien.

d) Delitos de contenido

- Pornografía infantil: Producción, distribución o posesión de material sexual con menores.
- Difusión de contenidos de odio (ciberodio): Mensajes que incitan al racismo, xenofobia, violencia o discriminación.
- Difusión de fake news o deepfakes maliciosos: Manipulación y difusión de información falsa o imágenes alteradas con fines ilícitos.
- Ciberterrorismo: Uso de tecnologías para promover actos terroristas o desestabilización.” (Prieto & Vargas, 2020).

Estas categorías reflejan las principales áreas en las que se manifiestan los ciberdelitos, abarcando desde la protección de datos y el patrimonio económico hasta la integridad y dignidad de las personas, así como la regulación del contenido ilegal o perjudicial en el entorno digital.

2.2.2.4 Marco jurídico internacional

a) Convenio de Budapest (2001) es el primer tratado internacional sobre ciberdelincuencia, elaborado por el Consejo de Europa con participación de varios países, y en vigor desde 2004. Su objetivo principal es la armonización de legislaciones nacionales para tipificar delitos informáticos como acceso ilícito, interceptación ilegal, ataques a la integridad de datos y sistemas, fraude informático, falsificación, delitos relacionados con pornografía infantil y violaciones a la propiedad intelectual. Además, establece mecanismos para la cooperación internacional, incluyendo la conservación rápida de datos, asistencia mutua, extradición y puntos de contacto 24/7 para facilitar la colaboración transfronteriza en la investigación y persecución de ciberdelitos.

UNODC (Oficina de Naciones Unidas contra la Droga y el Delito): Ha desarrollado módulos de capacitación y recursos especializados sobre prueba digital y análisis forense para fortalecer las capacidades de los países en la investigación y persecución de delitos informáticos, promoviendo buenas prácticas y estándares internacionales.

Interpol: Enfoca su acción en combatir delitos relacionados con criptomonedas y redes transnacionales, dada la complejidad y naturaleza global de estos delitos. Facilita la cooperación internacional, el intercambio de información y la capacitación de las fuerzas policiales para enfrentar amenazas emergentes en el ciberespacio.

Tratado de Naciones Unidas contra la Ciberdelincuencia (2024): Adoptado recientemente, busca crear un marco legal internacional para la persecución de delitos relacionados con tecnologías de la información y comunicaciones,

estableciendo tipificaciones específicas y mecanismos de cooperación internacional, incluyendo un punto de contacto 24/7 para asistencia jurídica y conservación de pruebas electrónicas.

b) El Convenio sobre la Ciberdelincuencia del Consejo de Europa

El Convenio de Budapest, adoptado el 23 de noviembre de 2001 por el Consejo de Europa tras seis años de redacción, es la norma internacional más completa para combatir la ciberdelincuencia. Su objetivo principal es prevenir conductas que afectan la confidencialidad, integridad y disponibilidad de sistemas, redes y datos informáticos, promoviendo la tipificación de estos actos como delitos en las legislaciones nacionales y facilitando su investigación y sanción. El Convenio aborda delitos contra sistemas informáticos, fraudes, pornografía infantil y violaciones a la propiedad intelectual, además de establecer la responsabilidad penal de personas jurídicas. En el ámbito procesal, fomenta herramientas eficaces para la obtención y conservación de pruebas electrónicas, así como la cooperación internacional rápida, incluyendo mecanismos como la red 24/7 para asistencia técnica y jurídica. Todo ello, busca armonizar leyes y fortalecer la lucha global contra el cibercrimen mediante la cooperación y un marco legal común.

c) Los protocolos adicionales al Convenio sobre Ciberdelincuencia del Consejo de Europa

El Convenio de Budapest incluye dos protocolos adicionales que aún no han sido adoptados por Perú. El primero, de 2003, busca criminalizar conductas racistas y xenófobas difundidas mediante sistemas informáticos, incluyendo la incitación al odio y la negación de genocidios. El segundo, de 2022, mejora la cooperación internacional para obtener y compartir pruebas electrónicas ubicadas en otras jurisdicciones, facilitando la colaboración entre Estados y con empresas proveedoras de servicios digitales. Ambos protocolos fortalecen la lucha contra el cibercrimen y promueven una justicia más efectiva a nivel global.

d) La negociación de una convención internacional

El 27 de diciembre de 2019, la ONU constituyó un Comité intergubernamental de expertos para elaborar una Convención internacional integral contra el uso delictivo de las TIC. Debido a la pandemia, el Comité inició sus trabajos en 2022, incluyendo temas como criminalización, proceso penal, cooperación internacional y medidas preventivas. La Secretaría técnica está a cargo de la UNODC, que también ofrece asistencia técnica y fortalece las capacidades estatales contra la ciberdelincuencia. El proyecto de Convención fue finalizado y adoptado por la Asamblea General a fines de 2024, marcando un hito en la lucha global contra la ciberdelincuencia.

2.2.2.5 Legislación nacional (Perú)

a) Código Penal:

Artículo 190-A: Tipifica el acceso ilícito a sistemas informáticos, sancionando el acceso sin autorización o el exceso de autorización a sistemas protegidos.

Artículo 196: Regula el fraude informático, penalizando la obtención de beneficios ilícitos mediante manipulación de sistemas o datos.

Ley 30096 (2013): Ley específica que sanciona delitos contra sistemas y datos informáticos, incluyendo acceso ilícito, atentado contra la integridad de datos y sistemas, interceptación ilícita, fraude informático y otros delitos conexos, con penas privativas de libertad y multas.

b) La Ley de Delitos Informáticos

El 22 de octubre del 2013 se publicó la Ley Nº 30096, Ley de Delitos Informáticos, con el objeto de prevenir y sancionar los delitos cometidos utilizando las tecnologías de la información y las comunicaciones que vulneran los sistemas y datos informáticos, y otros bienes jurídicos penalmente relevantes. Dicha norma derogó del Código Penal el delito de hurto telemático y el capítulo Delitos Informáticos.

La Ley de Delitos Informáticos –modificada extensamente por la Ley Nº 30171, publicada el 10 de marzo del 2014 para adecuar de mejor manera la descripción de sus conductas delictivas al Convenio de Budapest–33, establece cinco grandes grupos de ciberdelitos en función a los bienes jurídicos, a saber, los datos y los sistemas informáticos, la indemnidad y la libertad sexual, la intimidad y el secreto de las comunicaciones, el patrimonio y, por último, la fe pública.

Los ciberdelitos contra los datos y los sistemas informáticos comprenden el acceso ilícito, los atentados a la integridad de los datos informáticos y de los sistemas informáticos, y el abuso de mecanismos y dispositivos informáticos.

- El acceso ilícito (artículo 2º) es cometido por quien, deliberada e ilegítimamente, accede a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas o excediendo lo autorizado.
- El atentado a la integridad de los datos informáticos (artículo 3º) lo efectúa quien deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, que constituyen una representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.
- El abuso de mecanismos y dispositivos informáticos (artículo 10º) es realizado por quien deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los ciberdelitos; o por quien ofrece o presta servicio que contribuya a ese propósito.
- Los ciberdelitos contra la indemnidad y libertad sexual comprenden las proposiciones a niñas, niños y adolescentes con fines sexuales por medios tecnológicos, y la pornografía infantil.

- Las proposiciones a niñas, niños y adolescentes con fines sexuales por medios tecnológicos (artículo 5º) –también conocido como grooming en línea, conforme a la última modificación realizada por la Ley Nº 30838, publicada el 4 de agosto del 2018– es realizado por el que, a través de internet u otro medio análogo, contacta con una víctima de 14 años o menos para solicitar u obtener de él material pornográfico, o proponerle llevar a cabo cualquier acto de connotación sexual con él o con terceros; en los casos que la víctima tenga entre 14 y 17 años, se exige que medie el engaño.
- Si bien el grooming en línea se encuentra previsto y sancionado en la Ley de Delitos Informáticos, el grooming en sí –aquel que se realiza por cualquier otro medio no informático– fue incorporado en el 2014 al capítulo Ofensas al Pudor Público del Código Penal (artículo 183-B) por la Ley Nº 30171. Esta separación ha conllevado que el primero sea investigado por la Fiscalía Corporativa Especializada en Ciberdelincuencia, mientras que el segundo es competencia de las Fiscalías especializadas en trata de personas. Es necesario revisar esta dualidad en la respuesta penal contra el grooming, pues podría tornarse contraproducente para las fiscalías e, incluso, para las víctimas.
- La pornografía infantil o material de abuso y explotación sexual de niñas, niños y adolescentes, previsto en el artículo 183-A del Código Penal, fue modificado por la Ley de Delitos Informáticos y últimamente por la Ley Nº 30963, publicada el 18 de junio del 2019. Este delito es cometido por quien posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa, publicita, publica, importa o exporta por cualquier medio, objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de 18 años de edad. Este delito se agrava cuando la víctima tiene menos de 14 años; si el material se difunde a través de cualquier TIC u otro medio que genere difusión masiva; o si el autor actúa como integrante de una banda o una organización criminal.

c) Vacíos legales

Se identifican lagunas normativas relevantes, como la falta de tipificación específica para delitos emergentes como deepfakes (manipulación audiovisual con fines ilícitos) y el ciberespionaje, lo que dificulta la persecución efectiva de estas conductas.

2.2.2.6 Elementos constitutivos

A) Sujetos activos

El Derecho Penal, señala que el sujeto activo es definido como la persona que ejecuta una conducta prohibida por la ley penal o que, en su defecto, omite realizar una acción que le era legalmente exigible, siempre que dicha conducta esté condicionada a una cualidad o situación específica del individuo. En el contexto de los delitos informáticos, este sujeto activo es comúnmente identificado como el "hacker", término generalizado para referirse a quienes poseen conocimientos especializados en sistemas informáticos. Estas personas, por lo general, se encuentran en posiciones estratégicas dentro de una organización o, aun sin formar parte de ella, cuentan con habilidades suficientes para vulnerar sistemas tecnológicos. “Cabe destacar que dentro del ámbito de la criminalidad informática se distingue entre dos tipos de sujetos activos según su relación con la organización afectada.” (Cuenca, 2022):

a) Insiders

Son individuos que pertenecen a la organización como empleados, técnicos o colaboradores y que, aprovechando su rol, nivel de acceso o conocimiento privilegiado, perpetran actos ilícitos desde el interior. Su cercanía con la información confidencial y los sistemas críticos los convierte en una amenaza significativa para la seguridad informática.

b) Outsiders

Se trata de personas ajenas a la entidad afectada, pero que cuentan con un alto grado de conocimiento en tecnología e informática, lo que les permite cometer

delitos desde el exterior, mediante el uso de herramientas digitales especializadas. El principal desafío en la prevención y sanción de estos delitos radica en que, estadísticamente, la mayor parte de las infracciones son cometidas por los denominados "insiders". Su posición interna les facilita el acceso directo a la información protegida, incrementando así el riesgo de sustracción, alteración o divulgación no autorizada de datos. Esto pone en peligro el bien jurídico del dato, considerado un activo de alto valor y protegido por el ordenamiento jurídico estatal". (Cuenca, 2022).

B) Sujetos pasivos

- El sujeto pasivo, en términos jurídicos, es la persona física o jurídica sobre la cual recae el daño o perjuicio generado por la conducta ilícita del sujeto activo. En el ámbito de los delitos informáticos, esta figura corresponde a la víctima que sufre la agresión digital, ya sea mediante acceso indebido, fraude electrónico, sustracción de datos, entre otras formas de ataque, las cuales se realizan a través de equipos informáticos o mediante tecnologías de la información y la comunicación (TIC). Por lo general, las víctimas de este tipo de delitos presentan un bajo nivel de conocimiento en informática, lo que las hace especialmente vulnerables ante ataques cibernéticos. Este desconocimiento facilita que los ciberdelincuentes, tras analizar previamente las debilidades del objetivo, ejecuten acciones maliciosas con altas probabilidades de éxito. La ingeniería social, el phishing, el malware, entre otros métodos, suelen aprovechar esta brecha de conocimiento para acceder a información sensible o causar daños significativos. (Cuenca, 2022).

2.2.2.2 El convenio de Budapest y la legislación penal nacional

De acuerdo a Gallegos (2022)

El Convenio de Budapest, también conocido como “Convenio de Ciberdelincuencia”, es un tratado internacional creado por el Consejo de Europa para combatir los delitos informáticos, estableciendo un modelo de legislación que promueve la homologación de normas penales, la estandarización de procesos judiciales y la cooperación internacional. En el caso de Perú, el país solicitó su adhesión en 2014, siendo aprobada por el Consejo Europeo en 2015. Finalmente, el Congreso peruano ratificó el convenio en febrero de 2019, con algunas reservas, y entró en vigor el 1 de diciembre de 2019, tras su ratificación por el Poder Ejecutivo. Este acuerdo busca fortalecer la lucha contra la ciberdelincuencia a nivel global. (p.23)

2.2.2.3 Tipos y prácticas para evitar la ciberdelincuencia

Los ciberdelitos pueden ser de diferentes tipologías. Algunos ejemplos de ellos son:

- “Fraudes por correo electrónico e Internet, conocido como phishing.
- Ataques de spoofing o suplantación de identidad.
- Ciberextorsión para exigir dinero para evitar una amenaza o recuperar información robada.
- Cryptojacking, donde los ciberatacantes minan criptodivisas utilizando recursos que no les pertenecen.
- Malware, y entre él el más extendido y que más afecta a las organizaciones de todo el mundo: el ransomware.
- Y un largo etcétera”. (Chilcon, 2020).

Para evitarlos, la mejor manera de protegerse es adoptar hábitos digitales cuidadosos y sensatos. En este sentido, algunas prácticas que pueden ayudar a usuarios y organizaciones a mantenerse seguros son:

- “Desconfiar de los correos electrónicos con archivos adjuntos o enlaces dudosos.
- No descargar los archivos de los correos ni pinchar en dichos enlaces a menos que se conozca el emisor, ya que pueden contener malware.

- No instalar aplicaciones de fuentes desconocidas.
- Evitar la conexión a redes WiFi públicas o gratuitas.
- Utilizar contraseñas robustas y no reutilizar la misma en varias cuentas. Además, es recomendable cambiar cada cierto tiempo las claves.
- Tener instalado y actualizado el sistema antivirus. El dispositivo también deberá estar plenamente actualizado.
- Concienciar y formar a los usuarios de Internet, ya sean trabajadores, miembros de la familia, etc.
- Estar al tanto de las principales ciberamenazas y ciberataques para evitar sufrir esta lacra". (Custodio, 2021).

2.2.2.5 Los bienes jurídicos protegidos amenazados por la ciberdelincuencia

De acuerdo a (Arrabal, 2019; Vargas, 2022), Los delitos informáticos protegen principalmente la información como bien jurídico, considerada desde perspectivas económicas, personales y legales, a incluir su confidencialidad, integridad y disponibilidad. Esta protección es vital debido a los riesgos que las conductas ilícitas representan para la seguridad, intimidad y patrimonio, afectando simultáneamente diversos intereses jurídicos. Aunque no constituyen una categoría delictiva nueva, estos delitos actualizan las conductas tradicionales bajo medios tecnológicos, aplicando principios de daño y lesividad para determinar sanciones. La delincuencia informática afecta múltiples bienes jurídicos, destacando intereses sociales valiosos más allá de los clásicos. En general, la información protegida puede clasificarse en patrimonio, confidencialidad e intimidad, confiabilidad jurídica y derecho de propiedad, contemplando tanto datos como sistemas y soportes informáticos. Así, se busca garantizar la defensa integral y adecuada de los derechos en el ámbito digital.

2.2.2.6 Sujeto activo y pasivo del delito informático.

2.2.2.6.1 Ciberdelincuente: Perfil criminológico.

> "El ciberdelincuente es el sujeto activo del delito. La doctrina sobre este aspecto se ha desarrollado, ya que anteriormente consideraban que el perfil del ciberdelincuente respondía a dos casos, el primero de jóvenes expertos y obsesionados con la informática, que accedían ilícitamente a los sistemas como un reto personal, para demostrar que eran capaces de hacerlo; el segundo caso era de empleados de empresas o instituciones públicas que tenían el permiso de acceso a los sistemas informáticos, y ya sea por obtener un beneficio económico o por venganza, y causaban daños deliberadamente."(Custodio, 2021).

"(...) el 50 % de las bandas dedicadas al cibercrimen se componen de seis o más personas. De ellos, el 76 % son hombres cuyas edades van desde los 14 años (8 %) hasta los 50 (11 %). Aunque la edad promedio de este tipo de delincuentes es 35 años (43 %)." (Ventura, 2021).

Dado estos resultados, el perfil que antes se tenía de los ciberdelincuentes se ha expandido, abarcando no solamente a las características antes descritas, actualmente la doctrina coincide en las características generales de los ciberdelincuentes, como señala Espinosa: "[...] el perfil del ciberdelincuente suele ser el de una persona con un coeficiente intelectual medio, que le permita tener conocimientos informáticos, además de poseer un medio informático con el cual tenga acceso a la red para cometer los actos ilícitos." (Saltos et al., 2021).

Al ser el perfil del ciberdelincuente más amplio, también abarca mayor cantidad de conductas criminales, de esta manera, los ciberdelincuentes se clasifican según estas. "Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos."(Hernández & Patricio, 2022).

Sin embargo, la clasificación clásica es la siguiente:

a) Hacker: persona con amplios conocimientos en informática.

b) Cracker: “El término nació en 1985, creado por los hackers para diferenciar sus actividades, ya que los crackers utilizan sus conocimientos para causar daños.
c) Phreakers: Se especializaban en las redes telefónicas, quienes mediante sonidos manipulaban las redes para conseguir llamadas gratis, posteriormente crearon un dispositivo para hacer más fácil esta tarea.
d) Viruckers: Este grupo introduce virus informáticos que pueden ser “benignos” si solo molestan, o “malignos” si destruyen información e inutilizan el sistema.(Prieto & Vargas, 2020).

Por lo tanto, podemos decir que el perfil del ciberdelincuente ha evolucionado, dejando atrás la idea de que solo jóvenes expertos o empleados con acceso privilegiado cometen delitos informáticos. Hoy en día, cualquier persona con conocimientos básicos puede incursionar en el cibercrimen, y los delincuentes abarcan un rango de edades amplio, siendo el promedio de 35 años. Los ciberdelincuentes se clasifican según sus conductas, destacándose los hackers (divididos en White Hat, Gray Hat y Black Hat), *crackers, phreakers y viruckers,* cada uno con actividades específicas que van desde vulnerar sistemas hasta introducir virus. Este cambio en el perfil refleja una mayor diversidad en las motivaciones y métodos del cibercrimen.

2.2.2.7 Cibervíctima: Perfil de victimización.

“La víctima es la persona natural o jurídica que sufre un daño directo o indirecto, ya sea inocente o con algún grado de participación en la causa del perjuicio”. (Prieto & Vargas, 2020).

“La informática, extendida a diversos sectores y personas de diferentes edades y niveles, exponen a una gran cantidad de víctimas potenciales. Tanto personas naturales como instituciones públicas o privadas pueden sufrir consecuencias por delitos informáticos”(Rivera, 2021).

> “Existe un grave problema denominado “cifra negra” en los delitos informáticos, pues muchas víctimas no denuncian por desconocimiento, desconfianza en el sistema o temor a afectar su reputación. Esto dificulta conocer la verdadera magnitud del fenómeno”. (Chilcon, 2020).

Para delitos cometidos a través de redes sociales o plataformas parecidas, también se destaca la falta de prevención de las víctimas aceptando entablar amistad con desconocidos, proporcionando demasiada información personal tal como direcciones, números de teléfono o fotos, generando diversas consecuencias. “Muchas veces las víctimas más comunes de estas conductas son personas de edad avanzada que no entienden cómo se debe manejar en la red”.(Lujan, 2022).

De lo mencionado por los autores se puede concluir que: La víctima, como sujeto pasivo del delito, es aquella persona natural o jurídica que sufre un daño directo o indirecto, ya sea de manera inocente o con cierta participación en el perjuicio. Con el uso masivo de la informática en diversos ámbitos, el número de víctimas potenciales de delitos informáticos es amplio, incluyendo tanto individuos como instituciones públicas y privadas. Sin embargo, existe un problema conocido como la "cifra negra", ya que muchas víctimas no denuncian debido a la falta de conocimiento, desconfianza en el sistema o temor al desprestigio. Los usuarios particulares son los más vulnerables, pues suelen carecer de medidas básicas de seguridad informática, como antivirus o conocimientos sobre protección. Además, conductas como proporcionar información personal en redes sociales o entablar amistades con desconocidos aumentan los riesgos, especialmente en personas de edad avanzada que no están familiarizadas con el manejo seguro de la tecnología.

2.2.2.8 Dimensiones de ciberdelincuencia

a) Medidas preventivas

De acuerdo a Arrabal (2019):

Los ciberdelincuentes están muy preparados e incluso han sabido adelantarse a las medidas preventivas que se están tomando, por lo que, es necesario

adquirir buenos hábitos digitales para evitar ser víctimas de ciberataques. Algunas de las costumbres principales para la prevención de ciberdelitos son las siguientes:

- "No abrir enlaces sospechosos en correos electrónicos.
- No realizar descargas de fuentes desconocidas.
- Asegurarse que se está dando uso a un sitio web legitimo.
- Actualizar software constantemente (corrige vulnerabilidades)
- No usar redes Wi-Fi públicas.
- Usar contraseñas seguras y no reutilizarlas para varias cuentas.
- Mantén actualizado tu sistema operativo y tus programas instalados.
- Desinstala con regularidad los programas que ya no uses.
- Usa un programa antivirus de una empresa de renombre
- No descargues programas, películas o música de sitios compartidos porque a menudo tienen programas maliciosos.
- No descargues los archivos adjuntos ni hagas clic en los enlaces de remitentes que no conozcas.
- No ingreses información personal en sitios web desconocidos.
- Confirma que es el sitio web correcto cuando ingreses información financiera".

b) Medidas sancionadoras

"El Perú aprobó este convenio el 12 de febrero del 2019 con la Resolución Legislativa 30913, que trajo como consecuencia la adaptación de nuestra legislación a este convenio. Sin embargo, ya anteriormente se ha sancionado la ciberdelincuencia. En el artículo 186 del Código Penal se reguló una pena no menor de tres ni mayor a seis años cuando el hurto se realizaba mediante la utilización de transferencia electrónica de fondos, de la telemática en general o la violación del empleo de claves secretas". (Bañón, 2020)

Posteriormente, la pena aumentó de cuatro a ocho años, pero este artículo fue derogado con la entrada en vigencia de la Ley 30096, Ley de delitos

informáticos, publicada el 22 de octubre del 2013. “Los delitos informáticos fueron regulados en el Título V, Capítulo X del Código Penal, que fue incorporado por la Ley 37309 del 17 de julio del 2000. Sin embargo, estos también fueron derogados con la Ley 30096”. (Prieto & Vargas, 2020)

2.2.2.9 Derecho Comparado

a) España

España incorporó los delitos informáticos en su Código Penal mediante la Ley Orgánica 10/1995, vigente desde el 23 de noviembre de 1995, estableciendo sanciones específicas y convirtiéndose en un referente internacional. En 2001, el país se unió al Consejo Europeo al suscribir el Convenio del Cibercrimen, ratificado en 2010. Posteriormente, en 2015, se reformó esta normativa para incluir actos como dañar, alterar o hacer inaccesibles datos ajenos, y el acceso no autorizado a sistemas informáticos. Estas medidas reflejan un esfuerzo por adaptar la legislación a la evolución del cibercrimen y proteger bienes jurídicos relacionados con la información y la privacidad. (Gamba, 2019).

b) Argentina

La Ley N° 26.388 actualizó el Código Penal argentino para regular los delitos informáticos, incorporando estas infracciones en su articulado sin crear figuras específicas. Se amplió el concepto de "documento" y "firma" para incluir versiones digitales, y se tipificaron conductas como el acceso ilegítimo a comunicaciones electrónicas y la defraudación mediante manipulación de sistemas informáticos. Además, se modificó el artículo 183 para sancionar la alteración, destrucción o inutilización de datos, programas o sistemas informáticos, así como la distribución de programas maliciosos. Estas reformas buscan adaptar la legislación penal a las nuevas tecnologías y sus riesgos asociados. (Zarzosa, 2018).

c) Chile

Chile suscribió el Convenio de Budapest en 2016, aprobado por el Senado, con el objetivo de modernizar su legislación en materia de ciberdelitos. La Ley N°

19.223, que sancionaba delitos como sabotaje, espionaje y fraude informático, fue derogada para dar paso a nuevas tipificaciones, como el acceso ilegítimo a sistemas informáticos, la alteración o destrucción de datos, y la facilitación de delitos mediante herramientas tecnológicas. Sin embargo, el avance tecnológico plantea desafíos en la determinación de la jurisdicción y la protección de bienes jurídicos, especialmente cuando los delitos se cometen desde el extranjero, lo que a menudo resulta en impunidad. (Zarzosa, 2018).

d) México

México fue invitado en 2007 a unirse al Convenio de Budapest para fortalecer su normativa en ciberdelincuencia, pero desde 1999 solo ha sido observador en el Consejo de Europa, lo que le permite reformar sus leyes en telecomunicaciones y seguridad nacional. El Código Penal Federal, reformado en 2007, tipifica delitos como corrupción de menores, pornografía infantil, violación de derechos de autor y acceso ilícito a sistemas informáticos. También establece penas más severas para quienes difundan material que involucre a menores de edad. Sin embargo, México aún no ha ratificado el Convenio de Budapest, lo que limita su participación plena en la lucha internacional contra los delitos informáticos. (Gallegos, 2022).

e) Colombia

El Código Penal colombiano fue modificado en enero de 2009 mediante la Ley 1273, creando un nuevo bien jurídico protegido: la información y los datos. Esta reforma busca proteger la información que circula en internet o se accede mediante tecnologías, incorporando un título específico denominado “De la protección de la información y de los datos”. Entre los delitos tipificados se encuentra el hurto a través de medios informáticos, al que se le asigna una pena superior a otros delitos dentro de este título. Esta actualización refleja la necesidad de adaptar la legislación a los desafíos del entorno digital. (Lujan, 2022).

f) Perú

En octubre de 2007, el Congreso de Perú emitió la Ley N° 30096, conocida como “Ley de Delitos Informáticos”, con el objetivo de tipificar y sancionar

conductas ilícitas cometidas mediante herramientas tecnológicas que afecten bienes jurídicos protegidos. Esta ley abarca delitos contra sistemas informáticos, la intimidad, el secreto de las comunicaciones y el patrimonio. En 2014, la Ley N° 30171 modificó la anterior, incorporando la calificación de "deliberada" e "ilegítima" para las conductas y aumentando las penas para delitos como la interceptación indebida de datos y el fraude tecnológico. Estas reformas buscan fortalecer la lucha contra la ciberdelincuencia. (Hernández & Patricio, 2022).

g) Brasil

Brasil tipifica diversos ciberdelitos, incluida la piratería, mediante la Ley N° 12.737/2012, que modificó el Código Penal. Esta ley establece que la invasión de dispositivos informáticos, ya sea conectados o no a una red, con el fin de obtener, alterar o destruir datos, es un delito punible con hasta un año de prisión y multa. Si el delito resulta en la obtención de comunicaciones privadas, secretos comerciales o control remoto del dispositivo, la pena puede aumentar a dos años de prisión y multa. Las sanciones se incrementan en casos de circunstancias agravantes, como la divulgación o comercialización de los datos obtenidos. (Lujan, 2022).

2.3 Definición de conceptos

a) Modalidades delictivas

"Se señala como un hecho concreto en el cual, el legislador la señala en la normativa penal a fin de gradúe la pena". (Vinelli, 2021).

b) Medidas sancionadoras

"Estas medidas, buscan hacer efectiva las responsabilidades de los funcionarios que cometen hechos de corrupción". (Rivera, 2021).

c) Medidas preventivas

"Son medidas preventivas todas aquellas que sirvan para proteger eficazmente la vida y salud de los trabajadores". (González et al., 2018).

d) Tratamiento procesal

"El tratamiento procesal de los delitos informáticos contra el patrimonio en sus modalidades de hurto, estafa, sabotaje y fraude consiste en la investigación y gestión de los aspectos legales y procesales para sancionar estos delitos en el sistema judicial". (Gamba, 2019).

e) Ciberdelincuencia

"Consiste en cualquier comportamiento ilícito realizado mediante operaciones electrónicas que atentan contra la seguridad de sistemas informáticos y datos que se procesan". (Lujan, 2022).

f) Delitos informáticos

"Son conductas que buscan evadir sistemas de seguridad accediendo ilegalmente a computadoras, correos o datos mediante claves, acciones que solo pueden realizarse con tecnología" (Pardo, 2018).

CAPÍTULO III

METODOLOGÍA

3.1 Identificación y operacionalización de variables

Tabla 1

Operacionalización de variables

Variables	Dimensiones	Indicadores
V. Independiente **X: Tratamiento penal de los delitos informáticos**	**X1**: Tratamiento legislativo	- Penalidades específicas - Tipificación de delitos - Actualización normativa
	X2: Tratamiento procesal	- Existencia de procesos judiciales especializados - Aplicación del Proceso Inmediato - Duración promedio de casos - Especialización judicial
	X3: Incumplimiento de finalidad reguladora	- Sanciones administrativas - Vacíos legales - Efectividad en la prevención - Divergencia en criterios judiciales
Variable Dependiente: **Y: Ciberdelincuencia**	Modalidades delictivas	- Tipos de delitos
	Medidas preventivas	- Educación digital - Seguridad informática - Monitoreo de transacciones
	Medidas sancionadoras	- Penas privativas de libertad - Multas y sanciones administrativas

3.2 Tipo de investigación

La forma de investigación es una investigación básica, porque busca el conocimiento de la realidad o de los fenómenos de la naturaleza, para contribuir a una sociedad cada vez más avanzada y que responda mejor a los retos de la humanidad.

3.3 Nivel de investigación

El estudio corresponde al nivel explicativo, ya que busca determinar la causa y efecto entre las variables de estudio.

3.4 Diseño

El estudio corresponde a uno de diseño no experimental (ex post facto, en tanto no habrá manipulación de variables, sino que los datos serán recogidos después de ocurrido el hecho.

3.5 Delimitación de la investigación

3.5.1 Delimitación espacial

La investigación corresponde al ámbito del distrito judicial de Tacna.

3.5.2 Delimitación temporal

El estudio comprende el período 2019-2022.

3.6 Población y muestra

3.6.1 Población

Tabla 2

Población y muestra

Población	Número
Sentencias sobre delitos informáticos	10
Magistrados penales	5
Abogados penales	150
Total	165

Fuente: Corte Superior de Justicia de Tacna y Colegio de Abogados

3.6.2 Criterios de inclusión y exclusión

a) Criterios de inclusión

Sentencias sobre delitos informáticos, abogados y magistrados penales.

b) Criterios de exclusión

Se excluyen a todos los casos que no están inmersos en el criterio anterior; y a los que por situaciones de contingencia no pudieron participar.

3.6.3 Tipos de muestreo

El estudio se desarrolló considerando el muestreo probabilístico, ya que todos los elementos tienen la misma probabilidad de ser seleccionados.

3.6.4 Tamaño de la muestra

Para el caso de los abogados penalistas se aplicó una muestra a estudio, al 95 % de nivel de confianza y con margen de error al 5 % alcanzó un número de 108 participantes.

3.7 Instrumentos y técnicas de investigación

3.7.1 Técnicas de recolección de los datos

Como técnicas para el desarrollo de la investigación se utilizaron: la entrevista, la encuesta y el análisis documental.

3.7.2 Instrumentos para la recolección de los datos

El instrumento de medición que se aplicó fue la cédula de entrevista a magistrados penales y el cuestionario a los abogados penalistas, como también la ficha de análisis documental para el análisis de los casos sobre delitos informáticos.

3.7.3 Validación de instrumentos para la recolección de los datos

Se evaluó la validez de la Ficha de análisis documental mediante un proceso de examinación por jueces expertos, llevado a cabo por profesionales con Maestría y Doctorado en derecho, así como experiencia en metodología de investigación.

Estos expertos proporcionaron sus opiniones, cuyos resultados se detallan a continuación:

1) Experto 1: Dr. Wiliam, Vargas Espinoza : 45/50 ptos.
2) Experto 2: Mg. Gloria Katherine Gonzales García : 45/50 ptos.
3) Experto 3: Abog.Alex, Choquecahua Ayna :46/50 ptos.

Los resultados alcanzados permitieron validar el instrumento para su aplicación en el estudio.

3.8 Método de análisis

3.8.1 Procedimiento de recolección de datos

La recolección de datos implicó la integración sistemática de métodos cuantitativos y cualitativos. Los datos se obtuvieron a través de entrevistas, encuestas y observaciones o análisis de documentos, y su integración proporcionó una comprensión más completa del fenómeno estudiado, validando y enriqueciendo los resultados a través de la triangulación de fuentes y métodos.

3.8.2 Procedimiento de organización y análisis

El procedimiento de organización y análisis de datos implicó la integración sistemática de datos cuantitativos y cualitativos. Primero, se organizaron los datos recopilados a través de técnicas como la codificación y categorización para los datos cualitativos, y tabulación para los cuantitativos. Luego, se analizaron utilizando software especializado para los datos cualitativos, y herramientas estadísticas para los cuantitativos. La integración de los resultados se realizó mediante estrategias basadas en los resultados. Finalmente, se interpretó el conjunto de hallazgos para obtener conclusiones significativas y recomendaciones prácticas.

3.8.3 Método de análisis empleado

El método de análisis implicó la integración de técnicas cuantitativas y cualitativas para obtener una comprensión más completa del fenómeno estudiado. Se recopilaron y analizaron datos cuantitativos utilizando estadísticas descriptivas

y pruebas de hipótesis (regresiones), mientras que los datos cualitativos se analizan mediante técnicas como el análisis temático o de contenido.

CAPÍTULO IV

RESULTADOS

4.1 Descripción del trabajo de campo

Para la ejecución del trabajo de campo, se implementaron las siguientes acciones:

- Se realizaron entrevistas presenciales a magistrados especializados en derecho penal, asegurando un contacto directo y personalizado.
- Previamente a la aplicación de los instrumentos, se explicaron los objetivos de la investigación a los participantes, garantizando su consentimiento informado y destacando el carácter voluntario de su participación.
- El proceso de recolección de datos se desarrolló entre los meses de noviembre y diciembre de 2024, optimizando el tiempo y los recursos disponibles para obtener información precisa y relevante.
- Esta metodología permitió recopilar datos de manera rigurosa y ética, asegurando la calidad y confiabilidad de los resultados obtenidos.

4.2 Diseño de la presentación de los resultados

El análisis y procesamiento de datos se llevaron a cabo de manera automatizada utilizando herramientas como SPSS 20.0 y Microsoft Office Excel 2010. En SPSS, se generaron tablas de frecuencias y se aplicó la prueba de regresión logística para evaluar el coeficiente de determinación entre las variables. Por su parte, Excel se empleó para el registro y organización de la información, así como para la configuración de la matriz de sistematización. Los resultados se presentaron mediante tablas y gráficos estadísticos, los cuales fueron posteriormente integrados en Word para su estructuración final y discusión. Este enfoque automatizado

optimizó la eficiencia y precisión del análisis, facilitando la interpretación de los datos.

4.2.1 Análisis e interpretación de los datos

Para el análisis de los datos, se aplicaron técnicas tanto de estadística descriptiva como inferencial. En el ámbito descriptivo, se elaboraron tablas que presentaron las frecuencias absolutas y relativas (en porcentaje), permitiendo una clasificación y exposición clara de los datos según sus categorías, niveles o clases. Por otro lado, en el análisis inferencial, se emplearon tablas de regresión para examinar el coeficiente de determinación entre las variables de estudio, utilizando la prueba estadística no paramétrica de regresión logística. Estas herramientas permitieron no solo describir los datos, sino también explorar patrones y asociaciones significativas entre las variables analizadas.

4.3 Resultados

4.3.1 Presentación

En este capítulo, se analizan y explican los resultados derivados de la recopilación de información utilizando estadísticas descriptivas e inferenciales. Se sigue un orden estructurado al presentar las variables y sus indicadores, y se calculan y muestran frecuencias y porcentajes. El análisis se basa en la interpretación de las respuestas obtenidas mediante el instrumento aplicado, las cuales se organizan y representan en tablas elaboradas específicamente para este propósito.

4.3.2 Análisis e interpretación de resultados de análisis documental

4.3.2.1 Análisis descriptivo de variables e indicadores

El análisis de tablas y figuras, se realizaron teniendo en cuenta las variables, dimensiones e indicadores y lo ítems establecidos para la recopilación de información que servirá para contrastar las hipótesis de estudio.

Las tablas y figuras son detalladas a continuación, las cuales fueron diseñadas de acuerdo las Normas APA, para su mejor comprensión y análisis.

I. Tratamiento penal de los delitos informáticos

A. Tratamiento legislativo

Tabla 3
Tipo de delitos informáticos sentenciados en el período 2019-2022

Tipo de delito	f	%
Fraude informático - afecte patrimonio del Estado	7	64 %
Suplantación de identidad	1	9 %
Atentado a la integridad de datos informáticos	3	27 %
Total	11	100 %

La distribución muestra que el fraude informático que afecta al patrimonio estatal domina el 64 % de los casos, reflejando una priorización jurídica en la protección de recursos públicos, coherente con la Ley 30096 y su enfoque en sancionar conductas que comprometen intereses estatales. Los atentados a la integridad de datos (27 %) destacan por su relevancia en sistemas críticos, aunque su menor frecuencia podría indicar dificultades probatorias o menor reporte. La suplantación de identidad (9 %) aparece como un delito residual, posiblemente por su menor operatividad en el contexto analizado o por limitaciones en la detección.

Tabla 4
Tipificación

Tipo de delito	Pena	Multa	Frecuencia	Porcentaje (%)
Atentado a la integridad de datos informáticos	5 años		3	27 %
Fraude informático - afecte patrimonio del Estado	6 años	120 días-multa	1	9 %
Fraude informático - afecte patrimonio del Estado	8 años	120 días-multa	6	55 %
Suplantación de identidad	5 años		1	9 %

El fraude informático que afecta el patrimonio del Estado es el delito más recurrente, representando el 64 % de los casos, con penas de 8 años y 120 días-multa, lo que evidencia una priorización en la protección del patrimonio público y la aplicación de sanciones severas. Un caso aislado de fraude con 6 años de pena (9 %) podría estar relacionado con una atenuante, como colaboración con la justicia. Los atentados a la integridad de datos informáticos constituyen el 27 %, con penas de 5 años, reflejando su impacto en la seguridad de sistemas críticos, aunque no se aplicaron multas. La suplantación de identidad aparece en un único caso (9 %), también con una pena de 5 años, posiblemente debido a su menor frecuencia o dificultad probatoria. Este panorama muestra un enfoque judicial consistente en sancionar los delitos más lesivos al interés público, aunque sería necesario ampliar la muestra para validar tendencias y evaluar la efectividad de las penas aplicadas.

Tabla 5
Actualización normativa

Tipo de delito	Pena actualizada (2024)	Multa	Modificaciones normativas recientes
Fraude informático	4 a 8 años (base) 6 a 9 años (agravado)	60 a 120 días-multa	Incorporación de agravantes por afectación a menores de edad y patrimonio estatal.
Suplantación de identidad	3 a 5 años (base) 6 a 9 años (si afecta a menores)	No aplica	Se prioriza la protección de menores y bienes jurídicos sensibles como datos personales.
Atentado a la integridad de datos informáticos	3 a 6 años	No aplica	Actualización para incluir daños causados mediante tecnologías avanzadas, como inteligencia artificial.

Las modificaciones normativas de 2024 en Perú priorizan la protección de bienes jurídicos sensibles y adaptan el marco legal a tecnologías emergentes. El fraude informático mantiene penas de 4-8 años (base) y 6-9 años (agravado) con multas de 60-120 días-multa, enfocándose en la defensa del patrimonio estatal y menores, alineado con el Decreto Legislativo N° 1614 (2023). La suplantación de identidad (3-5 años base, 6-9 años si afecta a menores) refuerza la protección de datos personales y víctimas vulnerables, coherente con el DL 1591 (2023). Los atentados a la integridad de datos (3-6 años) incluyen ahora daños causados por IA, aunque la ausencia de multas sugiere un enfoque en sanciones privativas de libertad. Estas actualizaciones buscan cerrar brechas legales ante la evolución del cibercrimen, especialmente en delitos con menores o tecnologías disruptivas. La ausencia de multas en suplantación y atentados contradice parcialmente el Convenio de Budapest, que recomienda sanciones integrales. Las modificaciones son un avance, pero su efectividad dependerá de la capacidad investigativa y judicial. La falta de multas en delitos no económicos limita la reparación a víctimas, y la dependencia de penas privativas podría saturar el sistema penitenciario.

B. Tratamiento procesal

Tabla 6
Existencia de procesos judiciales especializados

Tipo de delito	Pena	Multa	Frecuencia	Porcentaje (%)	Normatividad actual
Fraude informático - afecte patrimonio del Estado	8 años	120 días-multa	6	55 %	Ley 30096 (2013), DL 1614 (2023): Agravante por afectación a recursos estatales.
Fraude informático - afecte patrimonio del Estado	6 años	120 días-multa	1	9 %	Ley 30096: Posible aplicación de atenuantes (ej. colaboración con la justicia).
Atentado a la integridad de datos informáticos	5 años		3	27 %	Ley 30096: Actualización para incluir daños con tecnologías avanzadas (IA).
Suplantación de identidad	5 años		1	9 %	Ley 30096: Protección de datos personales y bienes jurídicos sensibles.

La distribución muestra que el fraude informático que afecta al patrimonio estatal domina el 64 % de los casos (55% + 9 %), reflejando una priorización normativa en la protección de recursos públicos, alineada con la Ley 30096 y su modificatoria DL 1614 (2023), que endurece penas por afectación estatal. La aplicación de 8 años en la mayoría de casos (55 %) coincide con el máximo legal para agravantes, mientras que el de 6 años en un caso aislado (9 %) podría indicar atenuantes como colaboración con la justicia. Los atentados a la integridad de datos (27 %) reflejan la relevancia de proteger sistemas críticos, aunque la ausencia de multas sugiere un enfoque en sanciones privativas de libertad, pese a la actualización normativa para incluir daños con IA. La suplantación de identidad (9 %) muestra menor frecuencia,

pero su inclusión en la Ley 30096 destaca la protección de datos personales, aunque la falta de multas limita la reparación económica a víctimas. Las modificaciones recientes (DL 1614 y DL 1591) buscan adaptar el marco legal a amenazas tecnológicas emergentes, pero persisten brechas en la aplicación de sanciones integrales (privativas + multas), especialmente en delitos no económicos. La alta frecuencia de fraude informático evidencia una eficacia parcial en la persecución de delitos contra el Estado, pero la dependencia de penas privativas y la ausencia de multas en otros delitos contradice el Convenio de Budapest, que recomienda sanciones holísticas. Se requiere fortalecer mecanismos de cooperación interinstitucional y formación especializada para abordar tecnologías avanzadas (IA), como propone el Proyecto de Ley N° 09443/2024-CR.

Tabla 7
Aplicación del Proceso Inmediato

Tipo de delito	Frecuencia	Porcentaje (%)	Aplicación del proceso inmediato	Base normativa
Fraude informático afecte patrimonio del Estado	6	55 %	Aplicación por la existencia de elementos de convicción evidentes.	Ley 30096 y DL 1614 (2023): Agravante por afectación estatal. Art. 446 CPP (flagrancia o confesión).
Fraude informático afecte patrimonio del Estado	1	9 %	Aplicación limitada por posible atenuante (colaboración), pero no excluye su uso si hay confesión.	Ley 30096: Posible aplicación de atenuantes. Art. 160 CPP (confesión corroborada).
Atentado a la integridad de datos informáticos	3	27 %	Aplicación viable por evidencia inmediata (ej. registros de acceso no autorizado).	Ley 30096: Actualización para daños con IA. Art. 446 CPP (elementos de convicción).

Suplantación de identidad	1	9 %	Aplicación restrictiva por falta de flagrancia o confesión, salvo casos con pruebas digitales contundentes.	Ley 30096: Protección de datos personales. Art. 446 CPP (elementos de convicción).

La aplicación del proceso inmediato en los delitos informáticos analizados refleja una priorización en la eficacia procesal, aunque con matices según el tipo de delito. El fraude informático que afecta al patrimonio estatal (55 %) es el más viable para este proceso, ya que su alta frecuencia y la existencia de elementos de convicción evidentes (ej. registros de transacciones fraudulentas) permiten acelerar la sentencia, alineándose con el Art. 446 CPP y la Ley 30096, que incluye agravantes por afectación estatal. Un caso aislado (9%) podría aplicar el proceso inmediato si hay confesión corroborada (Art. 160 CPP), aunque la colaboración del imputado podría limitar su uso. Los atentados a la integridad de datos (27 %) son aplicables mediante este proceso si existen pruebas digitales inmediatas (ej. logs de acceso no autorizado), respaldadas por la actualización normativa para incluir daños con IA. La suplantación de identidad (9 %) presenta mayores restricciones, salvo que se demuestre con evidencia contundente (ej. capturas de cuentas robadas), aunque su baja frecuencia y complejidad probatoria dificultan su aplicación. Interpretación jurídica: La normativa (Ley 30096 y CPP) habilita el proceso inmediato para casos con flagrancia, confesión o elementos de convicción claros, priorizando la celeridad frente a la sobrecarga procesal.

Tabla 8

Duración promedio de casos

Tipo de delito	Frecuencia	Porcentaje (%)	Duración promedio (estimada)	Base normativa
Fraude informático	7	64 %	6-12 meses (investigación) + 2-6 días (juzgamiento). Proceso inmediato: 72 horas.	Art. 342-344 CPP (investigación), Art. 448.1 CPP (proceso inmediato).
Atentado a la integridad de datos	3	27 %	8-14 meses (investigación compleja) + 4-6 días (juzgamiento).	Art. 342.2 CPP (investigación compleja), Art. 446 CPP (elementos de convicción).
Suplantación de identidad	1	9 %	3-6 meses (investigación) + 2 días (juzgamiento). Proceso inmediato: 72 horas.	Art. 344.1 CPP (investigación simple), Art. 160 CPP (confesión).

La duración promedio del proceso refleja diferencias significativas según el tipo de delito y su complejidad. El fraude informático (64 %) destaca por su agilidad procesal, con investigaciones de 6-12 meses y juzgamiento en 2-6 días, además de la opción de proceso inmediato en 72 horas si hay flagrancia o confesión (Art. 448.1 CPP), lo que evidencia una priorización en la protección del patrimonio estatal. Los atentados a la integridad de datos (27 %) presentan plazos más extensos (8-14 meses de investigación), debido a la necesidad de pericias técnicas para analizar daños con IA o sistemas críticos, aunque su juzgamiento es ágil (4-6 días) si existen elementos de convicción (Art. 446 CPP). La suplantación de identidad (9 %) muestra una investigación breve (3-6 meses) y juzgamiento rápido (2 días), especialmente si hay

confesión (Art. 160 CPP), aunque su baja frecuencia y ausencia de multas limitan su impacto reparador.

C. Incumplimiento de finalidad reguladora

Tabla 9
Sanciones administrativas

Tipo de delito	Frecuencia	Porcentaje (%)	Sanciones administrativas	Base normativa
Fraude informático	7	64 %	Multas de 60 a 120 días-multa (Art. 8 Ley 30096). Inhabilitación para contratar con el Estado.	Ley 30096 (Art. 8), DL 1614 (2023): Agravante por afectación al patrimonio estatal.
Atentado a la integridad de datos informáticos	3	27 %	Multas de 18 a 120 días-multa (Art. 3 Ley 30096). Restitución de datos.	Ley 30096 (Art. 3).
Suplantación de identidad	1	9 %	Multas no aplicables (Art. 5 Ley 30096). Suspensión de cuentas digitales.	Ley 30096 (Art. 5).

La distribución de sanciones administrativas refleja una priorización en la protección del patrimonio estatal y brechas en la reparación de delitos no económicos. El fraude informático (64 %) destaca por su alta frecuencia y multas de 60-120 días-multa (Art. 8 Ley 30096), respaldadas por el DL 1614 (2023), que endurece penas por afectación estatal, aunque la inhabilitación para contratar no está explícitamente regulada en la norma, lo que genera ambigüedad en su aplicación. Los atentados a la integridad de datos (27 %) incluyen multas de 18-120 días-multa (Art. 3 Ley 30096), pero su ausencia en delitos como suplantación de identidad (9 %) limita la reparación económica a víctimas, contradiciendo el Convenio de Budapest, que exige sanciones integrales. Interpretación jurídica: La

Ley 30096 prioriza penas privativas y multas en delitos económicos, pero omite medidas administrativas (ej. multas) en suplantación, donde la suspensión de cuentas es insuficiente para compensar perjuicios morales. La alta frecuencia del fraude informático (64 %) evidencia brechas en prevención corporativa, mientras que la ausencia de multas en suplantación refleja un marco normativo fragmentado. Se requiere protocolos claros para aplicar sanciones administrativas (ej. inhabilitaciones) y capacitación técnica en fiscalías, como propone el Proyecto de Ley N° 09443/2024-CR, para garantizar justicia integral y alinear la legislación con estándares internacionales.

Tabla 10

Efectividad en la prevención

Tipo de delito	Medidas de prevención aplicadas	Frecuencia	Porcentaje (%)	Efectividad
Fraude informático	Actualización de penas (DL 1614), multas de 60-120 días-multa (Art. 8 Ley 30096).	7	64 %	Moderada: La severidad de las sanciones disuade, pero persisten casos por falta de pericias técnicas.
Atentado a la integridad de datos informáticos	Actualización normativa para IA (Art. 3 Ley 30096), restitución de datos.	3	27 %	Baja: La ausencia de multas y la complejidad en pruebas digitales reducen su eficacia.
Suplantación de identidad	Suspensión de cuentas digitales (Art. 5 Ley 30096), verificación de perfiles en redes.	1	9 %	Restringida: La medida es reactiva (no preventiva) y depende de la denuncia de víctimas.

La efectividad de las medidas preventivas en delitos informáticos en Perú muestra desigualdades según el tipo de delito. El fraude informático (64%) presenta efectividad moderada: la actualización de penas (DL 1614) y multas de 60-120 días-multa (Art. 8 Ley 30096) disuaden parcialmente, pero persisten casos por falta de pericias técnicas en fiscalías, como señala el Informe de la Defensoría del Pueblo. Los atentados a la integridad de datos (27 %) tienen efectividad baja: la ausencia de multas y la complejidad en pruebas digitales (ej. análisis de IA) limitan su impacto, pese a la actualización normativa del Art. 3 de la Ley 30096. La suplantación de identidad (9 %) muestra efectividad restringida: la suspensión de cuentas digitales (Art. 5 Ley 30096) es reactiva y depende de la denuncia de víctimas, sin estrategias preventivas robustas, como alertas periódicas o certificados de verificación. La Ley 30096 prioriza sanciones penales (multas, penas privativas) sobre medidas preventivas, excepto en capacitación (Art. 5 Ley 30096), lo que explica la fragilidad en la protección de datos personales.

Tabla 11
Divergencia en criterios judiciales

Tipo de delito	Criterio judicial divergente	Frecuencia	Porcentaje (%)	Base normativa y contexto
Fraude informático	Aplicación de agravantes vs. atenuantes	7	64 %	DL 1614 (2023): Agravante por afectación estatal. Art. 160 CPP: Confesión como atenuante.
Atentado a la integridad de datos	Interpretación de "tecnologías avanzadas" (IA) y ausencia de multas.	3	27 %	Ley 30096 (Art. 3): Actualización para daños con IA. Convenio

				de Budapest: Sanciones integrales.
Suplantación de identidad	Aplicación de medidas reactivas (suspensión de cuentas) vs. falta de multas.	1	9 %	Ley 30096 (Art. 5): No aplica multas. Art. 446 CPP: Elementos de convicción.

La divergencia en criterios judiciales en delitos informáticos refleja brechas normativas y operativas que afectan su aplicación. El fraude informático (64 %) muestra discrepancias en la aplicación de agravantes vs. atenuantes: mientras el DL 1614 (2023) prioriza sanciones severas por afectación estatal, el Art. 160 CPP permite reducir penas si hay confesión, generando inconsistencias en casos similares. Por ejemplo, un fraude con 8 años de pena (agravante) contrasta con otro de 6 años (atenuante por colaboración), evidenciando subjetividad en la interpretación de la norma. Los atentados a la integridad de datos (27%) enfrentan ambigüedad en la definición de "tecnologías avanzadas" (IA), pese a la actualización del Art. 3 de la Ley 30096, y la ausencia de multas contradice el Convenio de Budapest, que exige sanciones integrales (penas + reparación económica). La suplantación de identidad (9 %) ilustra medidas reactivas (suspensión de cuentas) sin multas, limitando la reparación a víctimas, aunque el Art. 446 CPP permite aplicar el proceso inmediato si hay elementos de convicción. Interpretación jurídica: La Ley 30096 y sus modificatorias (DL 1614) priorizan penas privativas y multas en delitos económicos, pero omiten protocolos claros para delitos no económicos (ej. suplantación), donde la reparación es insuficiente. Comentario crítico: La alta frecuencia del fraude informático (64 %) evidencia brechas en seguridad corporativa (ej. caso Interbank), mientras que la ausencia de multas en suplantación refleja un marco fragmentado. La dependencia de pericias técnicas (ej. análisis de IA) y la falta de fiscalías especializadas (como señala el Informe de la Defensoría del Pueblo) agravan la impunidad. Recomendación:

Implementar directivas vinculantes (ej. Acuerdo Plenario) para estandarizar criterios judiciales y fortalecer capacitación técnica en fiscalías, como propone el Proyecto de Ley N° 09443/2024-CR, para alinear la legislación con estándares internacionales.

B) Variable dependiente: Ciberdelincuencia

a) Modalidades delictivas

Tabla 12
Tipos de delitos

Tipo de delito	Criterio de tipificación	Determinantes para calificación	Frecuencia	Porcentaje (%)	Base normativa
Fraude informático	Afectación al patrimonio (estatal o privado).	Agravante: Impacto económico o afectación a menores (DL 1614). Atenuante: Colaboración (Art. 160 CPP).	7	64 %	Ley 30096 (Art. 8), DL 1614 (2023).
Suplantación de identidad	Uso de datos personales para perjuicio material/moral.	Agravante: Afectación a menores (Art. 5 Ley 30096). Ausencia de multas.	1	9 %	Ley 30096 (Art. 5).
Atentado a la integridad de datos	Daños mediante tecnologías avanzadas (IA, malware).	Ausencia de multas. Reparación de datos (Art. 3 Ley 30096).	3	27 %	Ley 30096 (Art. 3).

La tipificación de delitos informáticos en Perú refleja prioridades normativas y brechas en la protección de bienes jurídicos sensibles. El fraude informático (64 %) se tipifica por afectación al patrimonio (estatal o privado), con agravantes como

impacto económico o perjuicio a menores (DL 1614) y atenuantes por colaboración (Art. 160 CPP), lo que explica su alta frecuencia y severidad de penas (4-8 años). Suplantación de identidad (9 %) se define por el uso de datos personales para perjuicio material/moral, pero carece de multas administrativas, limitando la reparación a víctimas, pese a que el Art. 5 de la Ley 30096 incluye agravantes por afectación a menores. Los atentados a la integridad de datos (27 %) se califican por daños con tecnologías avanzadas (IA, malware), aunque la ausencia de multas (Art. 3 Ley 30096) contradice el Convenio de Budapest, que exige sanciones integrales (penas + reparación económica). Interpretación jurídica: La Ley 30096 y sus modificatorias (DL 1614) priorizan penas privativas y multas en delitos económicos (fraude), pero omiten medidas administrativas (ej. inhabilitaciones) en suplantación y atentados, donde la reparación es insuficiente. Comentario crítico: La alta frecuencia del fraude informático (64 %) evidencia brechas en seguridad corporativa (ej. caso Interbank), mientras que la suplantación y atentados a datos reflejan un marco fragmentado, con medidas reactivas (suspensión de cuentas, restitución de datos) que no previenen nuevos delitos. La dependencia de pericias técnicas (ej. análisis de IA) y la falta de fiscalías especializadas (como señala el Informe de la Defensoría del Pueblo) agravan la impunidad. Recomendación: Implementar protocolos estandarizados para pruebas digitales y multas proporcionales al daño, como propone el Proyecto de Ley N° 09443/2024-CR, para alinear la legislación con estándares internacionales y garantizar justicia integral.

b) Medidas preventivas

Tabla 13

Medidas preventivas

Tipo de delito	Criterio de tipificación	Frecuencia/ Porcentaje	Medidas preventivas
Fraude informático	Art. 8 Ley 30096: Uso de tecnología para obtener beneficio ilícito (ej. transferencias no autorizadas).	64 % (7 casos)	Actualización de penas (DL 1614), multas de 60-120 días-multa, capacitación en seguridad bancaria.
Suplantación de identidad	Art. 5 Ley 30096: Uso de datos personales para perjuicio material o moral.	9 % (1 caso)	Suspensión de cuentas digitales, verificación de perfiles en redes sociales.
Atentado a la integridad de datos	Art. 3 Ley 30096: Daños a sistemas informáticos mediante tecnologías avanzadas (IA).	27 % (3 casos)	Actualización normativa para IA, restitución de datos, auditorías de seguridad.

La tipificación y medidas preventivas de los delitos informáticos en Perú reflejan prioridades normativas y brechas en la protección de bienes jurídicos sensibles. El fraude informático (64 %) se tipifica por el uso de tecnología para obtener beneficio ilícito (Art. 8 Ley 30096), con medidas como actualización de penas (DL 1614), multas de 60-120 días-multa y capacitación en seguridad bancaria, aunque su alta frecuencia sugiere falta de efectividad en la prevención corporativa (ej. vulneraciones en sistemas financieros). La suplantación de identidad (9 %) se define por el uso de datos personales para perjuicio material/moral (Art. 5 Ley 30096), pero sus medidas (suspensión de cuentas digitales y verificación de perfiles) son reactivas, no disuasivas, y carecen de multas, limitando la reparación a víctimas. Los atentados a la integridad de datos (27 %) se califican por daños con tecnologías avanzadas (IA) (Art. 3 Ley 30096), con actualización normativa y

auditorías de seguridad, pero la ausencia de multas contradice el Convenio de Budapest, que exige sanciones integrales. Interpretación jurídica: La Ley 30096 prioriza penas privativas y multas en delitos económicos (fraude), pero omite medidas administrativas (ej. inhabilitaciones) en suplantación y atentados, donde la reparación es insuficiente. Comentario crítico: La alta frecuencia del fraude informático evidencia brechas en seguridad corporativa, mientras que la suplantación y atentados a datos reflejan un marco fragmentado, con medidas reactivas (suspensión de cuentas, restitución de datos) que no previenen nuevos delitos. La dependencia de pericias técnicas (ej. análisis de IA) y la falta de fiscalías especializadas agravan la impunidad. Recomendación: Implementar protocolos estandarizados para pruebas digitales y multas proporcionales al daño, como propone el Proyecto de Ley N° 09443/2024-CR, para alinear la legislación con estándares internacionales y garantizar justicia integral.

c) Medidas sancionadoras

Tabla 14

Medidas sancionadoras

Tipo de delito	Criterio de tipificación	Medidas sancionadoras	Frecuencia	Porcentaje (%)	Base normativa
Fraude informático	Afectación al patrimonio estatal o privado (Art. 8 Ley 30096).	4-8 años de prisión + 60-120 días-multa. Inhabilitación para contratar con el Estado.	7	64 %	Ley 30096, DL 1614 (2023).
Suplantación de identidad	Uso de datos personales para perjuicio material o moral (Art. 5 Ley 30096).	3-5 años de prisión. Suspensión de cuentas digitales.	1	9 %	Ley 30096.

Atentado a la integridad de datos informáticos	Daños causados mediante tecnologías avanzadas (IA) (Art. 3 Ley 30096).	3-6 años de prisión. Restitución de datos.	3	27 %	Ley 30096.

La tipificación y sanciones de delitos informáticos en Perú reflejan prioridades normativas y brechas en la protección de bienes jurídicos sensibles. El fraude informático (64 %) se tipifica por afectación al patrimonio estatal o privado (Art. 8 Ley 30096), con sanciones de 4-8 años de prisión y multas de 60-120 días-multa, además de inhabilitación para contratar con el Estado, respaldadas por el DL 1614 (2023), que endurece penas por afectación estatal. Sin embargo, su alta frecuencia evidencia brechas en seguridad corporativa (ej. vulneraciones en sistemas financieros). La suplantación de identidad (9 %) se define por el uso de datos personales para perjuicio material/moral (Art. 5 Ley 30096), pero carece de multas administrativas, limitando la reparación a víctimas, pese a que la Ley 30096 incluye agravantes por afectación a menores. Los atentados a la integridad de datos (27 %) se califican por daños con tecnologías avanzadas (IA) (Art. 3 Ley 30096), con penas de 3-6 años y restitución de datos, aunque la ausencia de multas contradice el Convenio de Budapest, que exige sanciones integrales. Interpretación jurídica: La Ley 30096 prioriza penas privativas y multas en delitos económicos (fraude), pero omite medidas administrativas (ej. inhabilitaciones) en suplantación y atentados, donde la reparación es insuficiente. Comentario crítico: La alta frecuencia del fraude informático refleja fragilidades en prevención corporativa, mientras que la suplantación y atentados a datos evidencian un marco fragmentado, con medidas reactivas (suspensión de cuentas, restitución de datos) que no previenen nuevos delitos. La dependencia de pericias técnicas (ej. análisis de IA) y la falta de fiscalías especializadas agravan la impunidad. Recomendación: Implementar protocolos estandarizados para pruebas digitales y multas proporcionales al daño, como propone el Proyecto de Ley N° 09443/2024-CR, para alinear la legislación con estándares internacionales y garantizar justicia integral.

4.3.3 Resultados de encuesta aplicada a abogados penalistas

A) Variable independiente (X): Tratamiento penal de los delitos informáticos

Tabla 15

Tratamiento legislativo

	Totalmente en desacuerdo		En desacuerdo		Indeciso		De acuerdo		Totalmente de acuerdo	
Ítems	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**
Claridad en la definición de delitos informáticos.	8	10.39	34	44.16	8	10.39	27	35.06	0	0.00
Suficiencia de la tipificación de delitos informáticos	6	7.79	49	63.64	8	10.39	14	18.18	0	0.00
Actualización oportuna de la normativa informática	12	15.58	50	64.94	5	6.49	9	11.69	1	1.30
Aplicabilidad práctica de las definiciones legales	4	5.19	35	45.45	10	12.99	26	33.77	2	2.60
Existencia de vacíos en la legislación informática	5	6.49	2	2.60	6	7.79	53	68.83	11	14.29

El análisis del tratamiento legislativo en materia de delitos informáticos evidencia una percepción mayoritariamente crítica respecto a la claridad, suficiencia y aplicabilidad práctica de la normativa vigente. Los resultados muestran que un alto porcentaje de encuestados se encuentra en desacuerdo con la claridad en la definición legal de los delitos informáticos (44,16 %) y con la suficiencia de su tipificación (63,64 %), lo que doctrinariamente refleja un problema de taxatividad y precisión normativa, principios esenciales en el derecho penal para garantizar la seguridad jurídica. Asimismo, la mayoría considera insuficiente la actualización oportuna de la normativa informática (64,94 %), lo cual corresponde con la doctrina que exige que las legislaciones penales en materia tecnológica se adapten a la rápida evolución de las modalidades criminales. En cuanto a la aplicabilidad práctica de

las definiciones legales, el 4,.45 % está en desacuerdo, lo que evidencia una brecha entre la formulación normativa y su operatividad en el sistema de justicia, afectando la eficacia del ius puniendi del Estado. Finalmente, un porcentaje significativo (68,83 %) percibe vacíos en la legislación informática, lo que coincide con la posición doctrinaria que sostiene que el marco jurídico actual resulta fragmentario e incompleto, requiriendo reformas integrales que garanticen una adecuada cobertura de conductas emergentes. En conjunto, estos resultados revelan un consenso general sobre la necesidad de fortalecer, actualizar y precisar el marco normativo relativo a los delitos informáticos, para asegurar su coherencia, eficacia y compatibilidad con los principios rectores del derecho penal moderno.

Tabla 16

Tratamiento procesal

Ítem	**Totalmente en desacuerdo**		**En desacuerdo**		**Indeciso**		**De acuerdo**		**Totalmente de acuerdo**	
	N	%	N	%	N	%	N	%	N	%
Existencia de juzgados especializados	10	12.99	31	40.26	15	19.48	20	25.97	1	1.30
Adecuación del Proceso Inmediato para casos simples de ciberdelincuencia.	7	9.09	35	45.45	7	9.09	26	33.77	2	2.60
Razonabilidad del tiempo de duración de los procesos por ciberdelitos.	4	5.19	43	55.84	12	15.58	17	22.08	1	1.30
Capacitación de los operadores de justicia en procedimientos de delitos informáticos.	10	12.99	49	63.64	9	11.69	9	11.69	0	0.00
Retraso de resolución de casos de ciberdelincuencia.	3	3.90	3	3.90	3	3.90	48	62.34	20	25.97

El tratamiento procesal de los delitos informáticos refleja importantes deficiencias estructurales y operativas en el sistema de administración de justicia. La mayoría de los encuestados manifiesta estar en desacuerdo con la existencia efectiva de juzgados especializados en ciberdelincuencia (40,26 %), lo que coincide con la crítica doctrinaria sobre la insuficiente especialización jurisdiccional necesaria para abordar delitos altamente técnicos. Asimismo, un 45,45 % considera inadecuada la aplicación del Proceso Inmediato en casos simples de ciberdelincuencia, lo que jurídicamente se explica por la complejidad probatoria y digital que caracteriza estos procesos, dificultando la aplicación de procedimientos abreviados sin vulnerar garantías. La percepción sobre la razonabilidad del tiempo de duración de los procesos también es negativa, con un 55,84 % en desacuerdo, lo que revela una afectación al principio de celeridad procesal y a la tutela jurisdiccional efectiva. Además, un 63,64 % indica que los operadores de justicia no cuentan con capacitación suficiente en procedimientos relacionados con delitos informáticos, confirmando la brecha doctrinal entre la sofisticación tecnológica del delito y la preparación institucional del sistema penal. Finalmente, la mayoría considera que existe un retraso significativo en la resolución de casos de ciberdelincuencia (62,34% de acuerdo y 25, 97 % totalmente de acuerdo), lo que pone en evidencia problemas de congestión, falta de recursos especializados y dificultades técnicas que retrasan la actuación procesal. En conjunto, estos resultados muestran un marcado déficit en la capacidad institucional y procedimental del sistema de justicia para enfrentar eficazmente los delitos informáticos, lo que demanda reformas orientadas a la especialización, capacitación y modernización de los procesos penales vinculados a la criminalidad digital.

Tabla 17

Incumplimiento de finalidad reguladora

Ítem	Totalmente en desacuerdo		En desacuerdo		Indeciso		De acuerdo		Totalmente de acuerdo	
	N	%	N	%	N	%	N	%	N	%
Adecuación en la aplicación de sanciones administrativas	15	14.71	37	36.27	20	19.61	29	28.43	1	0.98
Vacíos legales que limitan la finalidad preventiva de la regulación.	10	9.80	50	49.02	8	7.84	32	31.37	2	1.96
Eficacia preventiva de la normativa penal vigente	5	4.90	58	56.86	15	14.71	22	21.57	2	1.96
Falta de criterios judiciales uniformes que genera inseguridad jurídica.	13	12.75	64	62.75	13	12.75	12	11.76	0	0.00
Contribución de la regulación penal a la reducción de delitos informaticos	4	3.92	65	63.73	3	2.94	4	3.92	26	25.49

El análisis de los resultados evidencia un notorio incumplimiento de la finalidad reguladora en materia de delitos informáticos, reflejando debilidades tanto normativas como aplicativas. En primer lugar, la adecuación en la aplicación de sanciones administrativas presenta un alto nivel de desacuerdo (36,27 % en desacuerdo y 14,71 % totalmente en desacuerdo), lo que doctrinariamente revela la falta de articulación entre el derecho administrativo sancionador y las particularidades técnicas del ciberdelito, afectando su carácter preventivo y disuasivo. Asimismo, la percepción de vacíos legales que limitan la finalidad preventiva es marcada, con un 49,02 % en desacuerdo y un 31,37 % de acuerdo, lo cual refleja una insuficiencia normativa que impide al sistema penal cumplir con el principio de prevención general positiva. La eficacia preventiva de la normativa penal vigente también es cuestionada, pues el 56,86 % manifiesta desacuerdo, lo

que evidencia una brecha entre la regulación y la evolución constante de las conductas informáticas ilícitas, generando una respuesta penal desactualizada. A ello se suma la falta de criterios judiciales uniformes, donde un 62,75 % está en desacuerdo, demostrando la ausencia de jurisprudencia consolidada y unificada que brinde seguridad jurídica, principio fundamental del derecho penal contemporáneo. Finalmente, la contribución de la regulación penal a la reducción de los delitos informáticos muestra una fuerte percepción negativa, con 63,73 % en desacuerdo, sugiriendo que el marco regulatorio actual no logra un impacto real en la disminución de la incidencia criminal. En conjunto, estos resultados evidencian que la normativa, su aplicación y la interpretación judicial se encuentran desalineadas respecto de los fines preventivos y regulatorios del derecho penal informático, lo que exige reformas legislativas, criterios jurisprudenciales uniformes y mayor articulación entre las dimensiones administrativa y penal para garantizar una respuesta eficaz frente al avance de la ciberdelincuencia.

B) Variable dependiente (Y): Ciberdelincuencia

Tabla 18

Modalidades delictivas

Ítems	**Totalmente en desacuerdo**		**En desacuerdo**		**Indeciso**		**De acuerdo**		**Totalmente de acuerdo**	
	N	%	N	%	N	%	N	%	N	%
Frecuencia de fraudes electrónicos y suplantación de identidad.	2	1.96	7	6.86	10	9.8	70	68.63	13	12.75
Presencia de acceso indebido a sistemas o datos en los casos conocidos.	0	0	5	4.90	16	15.69	64	62.75	17	16.67
Uso de vulnerabilidades técnicas por parte de ciberdelincuentes.	0	0	0	0.00	6	5.88	75	73.53	21	20.59
Evolución rápida de las modalidades delictivas frente al sistema penal.	0	0	0	0.00	8	7.84	72	70.59	22	21.57
Incremento reciente de la ciberdelincuencia en el Perú.	1	0.98	1	0.98	3	2.94	51	50.00	46	45.10

Los resultados sobre las modalidades de ciberdelincuencia evidencian una marcada tendencia hacia la consolidación de patrones delictivos altamente prevalentes, lo cual confirma la creciente sofisticación y frecuencia de estos ilícitos en el contexto peruano. En primer lugar, la ocurrencia de fraudes electrónicos y suplantación de identidad muestra un amplio consenso, con un 68,63 % de acuerdo y 12,75 % totalmente de acuerdo, lo que doctrinariamente refuerza la idea de que estos delitos constituyen el núcleo de la criminalidad informática y demandan una tipificación y persecución prioritaria. Asimismo, la presencia de acceso indebido a sistemas o datos registra un 62,75 % de acuerdo y un 16,67 % totalmente de acuerdo, evidenciando que este comportamiento vulneratorio de la confidencialidad y seguridad informática sigue siendo una modalidad recurrente, en consonancia con la teoría del bien jurídico de la integridad de la información. El uso de vulnerabilidades técnicas por parte de los ciberdelincuentes, también es ampliamente reconocido, con un 73,53 % de acuerdo y un 20,59 % totalmente de acuerdo, lo cual confirma la naturaleza altamente técnica de estos delitos y subraya la necesidad de un enfoque regulatorio basado en riesgos tecnológicos. En la misma línea, la rápida evolución de las modalidades delictivas, respaldada por un 70,59 % de acuerdo y un 21,7 % totalmente de acuerdo, demuestra que el sistema penal se enfrenta a un fenómeno dinámico que supera la capacidad de actualización normativa, generando brechas de punibilidad y debilitando la efectividad preventiva del marco jurídico. Finalmente, el incremento reciente de la ciberdelincuencia en el Perú, con un 50 % de acuerdo y 45,10 % totalmente de acuerdo, confirma una tendencia ascendente que coincide con estudios comparados y reportes internacionales, revelando un desafío estructural que exige reformas normativas integrales, fortalecimiento institucional y políticas públicas orientadas tanto a la prevención como a la mitigación del riesgo tecnológico. En conjunto, los datos reafirman que la ciberdelincuencia se desarrolla con creciente complejidad y velocidad, poniendo en tensión las capacidades del sistema penal y demandando una respuesta jurídica más especializada, actualizada y estratégica.

Tabla 19

Modalidades delictivas

Ítems	Totalmente en desacuerdo		En desacuerdo		Indeciso		De acuerdo		Totalmente de acuerdo	
	N	%	N	%	N	%	N	%	N	%
Implementación de medidas preventivas en entidades públicas.	8	10.39	36	46.75	21	27.27	11	14.29	1	1.30
Contribución de campañas educativas a la reducción de ciberdelitos.	3	3.90	15	19.48	20	25.97	31	40.26	8	10.39
Desconocimiento de medidas básicas de prevención por usuarios comunes.	2	2.60	2	2.60	10	12.99	50	64.94	13	16.88
Aplicación de políticas de protección de datos en empresas privadas.	2	2.60	1	1.30	11	14.29	51	66.23	12	15.58
Insuficiencia de las medidas preventivas actuales frente a la ciberdelincuencia.	2	2.60	20	25.97	31	40.26	21	27.27	3	3.90

Los resultados vinculados a las medidas preventivas frente a la ciberdelincuencia evidencian una percepción predominante de insuficiencia y desarticulación en las estrategias implementadas tanto por el sector público como privado, lo cual coincide con la doctrina, que sostiene que la criminalidad informática requiere respuestas integrales y multidimensionales. En las entidades públicas, la implementación de medidas preventivas es considerada limitada, dado que un 46,75 % está en desacuerdo y solo un 14,29 % se muestra de acuerdo, lo que revela una brecha institucional que afecta la eficacia del sistema de protección digital estatal y vulnera el deber de garantía del Estado. En contraste, las campañas educativas

muestran un mayor nivel de aceptación como mecanismo preventivo, con un 40,26 % de acuerdo y 10,39 % totalmente de acuerdo, lo cual respalda la teoría criminológica situacional que enfatiza la importancia de la formación ciudadana para reducir la victimización. Sin embargo, se advierte que el desconocimiento de medidas básicas de prevención por parte de los usuarios sigue siendo un factor crítico, avalado por un 64,94 % de acuerdo y 16,88 % totalmente de acuerdo; esta constatación doctrinariamente se interpreta como una falla estructural en la cultura digital, que incrementa la vulnerabilidad y favorece la expansión de las modalidades delictivas. Respecto al sector privado, la percepción de aplicación de políticas de protección de datos es moderada pero positiva, con un 66,23 % de acuerdo, evidenciando que las empresas muestran mayor avance regulatorio y técnico que el sector público, alineándose con los principios de compliance y responsabilidad proactiva de la Ley de Protección de Datos Personales. Finalmente, un aspecto crítico es que la mayoría considera insuficientes las medidas preventivas actuales contra la ciberdelincuencia (40,26 % indeciso y 27,27 % de acuerdo), lo que sugiere falta de articulación normativa, debilidad institucional y ausencia de políticas públicas sostenibles. En conjunto, los resultados subrayan que las modalidades delictivas informáticas continúan expandiéndose debido a deficiencias en educación digital, carencias en políticas públicas y una protección desigual entre ámbitos institucionales, lo que doctrinaria y jurídicamente exige una reforma integral orientada a fortalecer capacidades preventivas, estandarizar protocolos y promover una cultura de ciberseguridad transversal en el país.

Tabla 20

Medidas preventivas

Items	Totalmente en desacuerdo		En desacuerdo		Indeciso		De acuerdo		Totalmente de acuerdo	
	N	%	N	%	N	%	N	%	N	%
Adecuación de las penas privativas a la gravedad del daño informático.	3	2.94	11	10.78	11	10.78	59	57.84	18	17.64
Efectividad disuasiva de las sanciones pecuniarias.	5	4.90	42	41.17	24	23.52	28	27.45	3	2.94
Complementariedad de sanciones administrativas y penales.	11	10.78	49	48.03	16	15.68	22	21.56	4	3.92
Insuficiente efecto preventivo de las penas actuales.	7	6.86	30	29.41	24	23.52	34	33.33	7	6.86
Necesidad de fortalecer el marco sancionador en ciberdelitos.	3	2.94	4	3.92	20	19.60	62	60.78	13	12.74

Los resultados sobre el marco sancionador aplicable a los ciberdelitos muestran una percepción generalizada de insuficiencia y necesidad de fortalecimiento, lo cual coincide con la doctrina penal contemporánea que advierte que la respuesta punitiva tradicional resulta limitada frente a la complejidad del fenómeno digital. En primer lugar, la mayoría considera que las penas privativas de libertad son adecuadas a la gravedad del daño causado por delitos informáticos, con un 57,84 % de acuerdo y un 17,64 % totalmente de acuerdo, lo que confirma que existe correspondencia entre la lesividad del bien jurídico afectado —la información, la seguridad digital y la integridad de sistemas— y la gravedad del reproche penal. No obstante, la efectividad disuasiva de las sanciones pecuniarias es cuestionada, dado que un 41,17 % está en desacuerdo y solo un 30,39 % las percibe como efectivas, lo cual se alinea con la doctrina que sostiene que las multas tienen impacto limitado frente

a organizaciones criminales digitales con alta rentabilidad y baja trazabilidad. De manera similar, la percepción sobre la complementariedad entre sanciones administrativas y penales es predominantemente negativa (48,03 % en desacuerdo), sugiriendo debilidad en la articulación interinstitucional y señalando la necesidad de un enfoque de "doble vía" más coherente entre CONCYTEC, OSIPTEL, la Policía Nacional y el Ministerio Público. En relación con el efecto preventivo de las penas actuales, los encuestados consideran insuficiente su capacidad disuasoria, reflejado en un 33,33 % de acuerdo y un 23,52 % indeciso, lo que doctrinariamente se interpreta como un déficit de eficacia real de la amenaza penal en un entorno donde el anonimato, la transnacionalidad y la sofisticación técnica reducen la percepción de riesgo del infractor. Finalmente, destaca que un 60,78 % considera necesario fortalecer el marco sancionador y un 12,74 % totalmente de acuerdo, lo que revela consenso social sobre la urgencia de actualizar el sistema punitivo, ya sea mediante agravantes específicas, ampliación de tipos penales, mejoras en trazabilidad digital o mayor especialización judicial. En conjunto, los datos confirman que la política criminal peruana en materia informática requiere una reforma integral orientada a incrementar la proporcionalidad, efectividad y coherencia de las sanciones, garantizando así una verdadera función preventiva en el ecosistema digital actual.

4.3.4 Análisis e interpretación de resultados de la entrevista aplicada

La entrevista fue aplicada a los magistrados y abogados en derecho penal, cuyos resultados son presentados a continuación:

Entrevistado N° 1

Tabla 21

Resultado de entrevistado N° 1:

Categoría	Subcategoría	Detalles
Tratamiento Penal de los Delitos Informáticos	**Tratamiento Legislativo**	La Ley 30096 no está acorde con la realidad tecnológica actual. Se requiere actualizar figuras jurídicas para responder a innovaciones delictivas. Además, la investigación demanda conocimientos técnicos y designación rápida de peritos.
	Tratamiento Procesal	Las pruebas digitales incluyen GPS, drones y datos en la nube, pero los allanamientos carecen de herramientas como bloqueadores de celulares, dificultando la custodia de información digital.
	Incumplimiento de Finalidad Reguladora	La legislación preventiva es limitada. Se proponen campañas educativas sobre riesgos digitales, contraseñas seguras y evitar compartir información personal. También se requiere tecnología avanzada para investigaciones digitales. Las sanciones actuales (penas privativas y multas) son insuficientes debido al anonimato de los delincuentes. Se necesitan bases de

		datos avanzadas y programas informáticos específicos para identificar delitos complejos.
Ciberdelincuencia	**Modalidades Delictivas**	Los delitos más comunes son estafa agravada, fraude informático, interceptación de datos y suplantación de identidad, los cuales han aumentado con la evolución digital.
	Medidas Preventivas	En Tacna se implementan programas informativos en páginas web y oficinas físicas para promover hábitos digitales seguros, como desconfiar de correos desconocidos y archivos adjuntos sospechosos.
	Cooperación Interinstitucional	Existe cooperación entre instituciones judiciales, policiales y privadas mediante alianzas estratégicas. Sin embargo, enfrentan desafíos relacionados con la coordinación efectiva y recursos limitados.
	Capacitación y Recursos	Aunque hay capacitaciones para fiscales especializados, no son suficientes ni accesibles en todas las regiones. Se requiere formación integral para operadores jurídicos en pruebas digitales, phishing y hacking.
	Medidas Sancionadoras	Las sanciones incluyen penas privativas, multas e inhabilitación,

		determinadas según la gravedad del delito cometido.
Propuestas de Mejora	**Impacto en la Comunidad Local**	La ciberdelincuencia ha generado nuevos delitos que evolucionan con la inteligencia artificial. Se propone actualizar leyes y difundir medidas preventivas más efectivas.
	Mejoras al Tratamiento Penal	Se sugiere fiscalizar operadoras telefónicas para evitar suplantaciones de identidad, facilitar geolocalización precisa e inmediata y supervisar la venta lícita de software para prevenir delitos informáticos.

El análisis cualitativo revela que el tratamiento penal de los delitos informáticos enfrenta desafíos legislativos, procesales y regulatorios debido a la rápida evolución tecnológica. Las modalidades delictivas más comunes incluyen estafas y suplantaciones de identidad, mientras que las medidas preventivas actuales son insuficientes para abordar el problema a fondo. Se destacan propuestas como mejorar la capacitación técnica, actualizar leyes específicas y fortalecer la cooperación interinstitucional para combatir eficazmente la ciberdelincuencia en Tacna.

Entrevistado N° 2

Tabla 22

Resultado de entrevistado N° 2:

Categoría	Subcategoría	Detalles
Tratamiento Penal de los Delitos Informáticos	**Tratamiento Legislativo**	La Ley 30096 permitió tipificar conductas que vulneran sistemas y datos informáticos. Sin embargo, requiere mejoras como ampliar tipologías delictivas (phishing, ciberacoso), clarificar conceptos y armonizar con normativas internacionales como la Convención de Budapest.
	Tratamiento Procesal	Los principales desafíos incluyen la identificación de ciberdelincuentes debido al anonimato y la falta de colaboración de instituciones financieras. Se proponen capacitaciones, cooperación interinstitucional e implementación de herramientas tecnológicas avanzadas.
	Incumplimiento de Finalidad Reguladora: Finalidad Preventiva	La legislación actual cumple parcialmente su finalidad preventiva. Se sugieren medidas como protocolos internacionales más efectivos, revisiones periódicas de la ley y especialización en cibercrimen para adaptarse a nuevas tecnologías y modalidades delictivas.

	Incumplimiento de Finalidad Reguladora: Finalidad Represiva	Las sanciones actuales (reclusión, inhabilitación) buscan disuadir conductas delictivas, pero se requieren ajustes como incrementar penas para delitos graves, establecer sanciones específicas para nuevas modalidades y promover acuerdos internacionales para extradición.
Ciberdelincuencia	**Modalidades Delictivas**	En Tacna, los delitos más comunes son fraude informático y suplantación de identidad, los cuales han evolucionado con el uso inapropiado de tecnologías digitales.
	Medidas Preventivas	Se implementan capacitaciones a funcionarios y campañas de concientización sobre hábitos digitales seguros. Su efectividad se evalúa mediante estadísticas y percepción ciudadana, aunque requieren constante adaptación a nuevas tecnologías.
	Medidas Sancionadoras	Las sanciones incluyen penas privativas de libertad y multas, determinadas según la gravedad del delito (naturaleza del delito, impacto social, reincidencia).
	Cooperación Interinstitucional	La cooperación se realiza mediante protocolos conjuntos, equipos multidisciplinarios y redes de información compartida. Los desafíos incluyen limitaciones tecnológicas y

		dificultades en coordinación internacional debido a diferencias legales entre países.
	Capacitación y Recursos	Se proporcionan cursos sobre legislación y técnicas en ciberdelincuencia, pero se identifican necesidades como actualización constante, infraestructura especializada y programas para administrar riesgos en sistemas informáticos.
Propuestas de Mejora	**Impacto en la Comunidad Local**	La ciberdelincuencia genera preocupación por pérdidas económicas y violación de privacidad. Se proponen talleres comunitarios, campañas en medios locales y programas educativos en escuelas sobre seguridad digital.
	Mejoras al Tratamiento Penal	Se sugiere fiscalizar operadoras telefónicas para evitar suplantación de identidad, facilitar geolocalización precisa e inmediata, supervisar venta lícita de software e implementar leyes específicas para nuevas formas de ciberdelincuencia.

La entrevista cualitativa evidencia que el tratamiento penal de los delitos informáticos enfrenta desafíos legislativos, procesales y regulatorios debido a la rápida evolución tecnológica. Las modalidades delictivas más comunes incluyen fraude informático y suplantación de identidad, mientras que las medidas preventivas actuales son insuficientes para abordar el problema a fondo. Se

destacan propuestas como mejorar la capacitación técnica, actualizar leyes específicas y fortalecer la cooperación interinstitucional para combatir eficazmente la ciberdelincuencia en regiones como Tacna.

Entrevistado N° 3:

Tabla 23

Resultado de entrevistado N° 3:

Categoría	Subcategoría	Detalles
Tratamiento Penal de los Delitos Informáticos	**Tratamiento Legislativo**	La Ley 30096 permitió tipificar conductas que vulneran sistemas y datos informáticos, pero requiere mejoras como la ampliación de tipologías delictivas (phishing, ciberacoso), clarificación de conceptos y armonización con normativas internacionales como la Convención de Budapest.
	Tratamiento Procesal: Prueba Digital	Los desafíos incluyen la identificación de ciberdelincuentes debido al anonimato y la falta de colaboración de instituciones financieras. Se proponen capacitaciones, cooperación interinstitucional y uso de herramientas tecnológicas avanzadas.

	Incumplimiento de Finalidad Reguladora: Preventiva	La legislación cumple parcialmente su finalidad preventiva. Se sugieren protocolos internacionales más efectivos, revisiones periódicas de la ley y especialización en cibercrimen para adaptarse a nuevas tecnologías y modalidades delictivas.
	Incumplimiento de Finalidad Reguladora: Represiva	Las sanciones actuales buscan disuadir, pero se requieren ajustes como incrementar penas para delitos graves, establecer sanciones específicas para nuevas modalidades y promover acuerdos internacionales para extradición.
Ciberdelincuencia	**Modalidades Delictivas**	En Tacna, los delitos más comunes son fraude informático y suplantación de identidad, los cuales han evolucionado con el uso inapropiado de tecnologías digitales.
	Medidas Preventivas	Se implementan capacitaciones a funcionarios y campañas de concientización sobre hábitos digitales seguros. Su efectividad se evalúa mediante estadísticas y percepción ciudadana, aunque requieren constante adaptación a nuevas tecnologías.

	Medidas Sancionadoras	Las sanciones incluyen penas privativas de libertad y multas, determinadas según la gravedad del delito (naturaleza del delito, impacto social, reincidencia).
	Cooperación Interinstitucional	La cooperación se realiza mediante protocolos conjuntos, equipos multidisciplinarios y redes de información compartida. Los desafíos incluyen limitaciones tecnológicas y dificultades en coordinación internacional debido a diferencias legales entre países.
	Capacitación y Recursos	Se proporcionan cursos sobre legislación y técnicas en ciberdelincuencia, pero se identifican necesidades como actualización constante, infraestructura especializada y programas para administrar riesgos en sistemas informáticos.
Propuestas de Mejora	**Impacto en la Comunidad Local**	La ciberdelincuencia genera preocupación por pérdidas económicas y violación de privacidad. Se proponen talleres comunitarios, campañas en medios locales y programas educativos en escuelas sobre seguridad digital.

	Mejoras al Tratamiento Penal	Se sugiere fiscalizar operadoras telefónicas para evitar suplantación de identidad, facilitar geolocalización precisa e inmediata, supervisar venta lícita de software e implementar leyes específicas para nuevas formas de ciberdelincuencia.

La entrevista cualitativa evidencia que el tratamiento penal de los delitos informáticos enfrenta desafíos legislativos, procesales y regulatorios debido a la rápida evolución tecnológica. Las modalidades delictivas más comunes incluyen fraude informático y suplantación de identidad, mientras que las medidas preventivas actuales son insuficientes para abordar el problema a fondo. Se destacan propuestas como mejorar la capacitación técnica, actualizar leyes específicas y fortalecer la cooperación interinstitucional para combatir eficazmente la ciberdelincuencia en regiones como Tacna.

Entrevistado N° 4:

Tabla 24

Resultados entrevista 4:

Categoría	Subcategoría	Detalles
Tratamiento Penal de los Delitos Informáticos	**Tratamiento Legislativo**	La Ley 30096 tipifica conductas que vulneran sistemas y datos informáticos, pero requiere mejoras como la ampliación de tipologías delictivas (phishing, ciberacoso), clarificación de conceptos y armonización con normativas internacionales como la Convención de Budapest.
	Tratamiento Procesal: Prueba Digital	Los desafíos incluyen la identificación de ciberdelincuentes debido al anonimato y la falta de colaboración de instituciones financieras. Se proponen capacitaciones, cooperación interinstitucional y uso de herramientas tecnológicas avanzadas.
	Incumplimiento de Finalidad Reguladora: Preventiva	La legislación cumple parcialmente su finalidad preventiva. Se sugieren protocolos internacionales más efectivos, revisiones periódicas de la ley y especialización en cibercrimen para adaptarse a nuevas tecnologías y modalidades delictivas.
	Incumplimiento de Finalidad Reguladora: Represiva	Las sanciones actuales buscan disuadir, pero se requieren ajustes como incrementar penas para delitos graves, establecer sanciones específicas para nuevas modalidades y promover acuerdos internacionales para extradición.

Ciberdelincuencia	**Modalidades Delictivas**	En Tacna, los delitos más comunes son fraude informático y suplantación de identidad, los cuales han evolucionado con el tiempo adaptándose a nuevas tecnologías digitales.
	Medidas Preventivas	Se implementan capacitaciones a funcionarios y campañas de concientización sobre hábitos digitales seguros. Su efectividad se evalúa mediante estadísticas y percepción ciudadana, aunque requieren constante adaptación a nuevas tecnologías.
	Medidas Sancionadoras	Las sanciones incluyen penas privativas de libertad y multas, determinadas según la gravedad del delito (naturaleza del delito, impacto social, reincidencia).
	Cooperación Interinstitucional	La cooperación se realiza mediante protocolos conjuntos, equipos multidisciplinarios y redes de información compartida. Los desafíos incluyen limitaciones tecnológicas y dificultades en coordinación internacional debido a diferencias legales entre países.
	Capacitación y Recursos	Se proporcionan cursos sobre legislación y técnicas en ciberdelincuencia, pero se identifican necesidades como actualización constante, infraestructura especializada y programas para administrar riesgos en sistemas informáticos.
Propuestas de Mejora	**Impacto en la Comunidad Local**	La ciberdelincuencia genera preocupación por pérdidas económicas y violación de privacidad. Se proponen talleres comunitarios, campañas en medios locales y

		programas educativos en escuelas sobre seguridad digital.
	Mejoras al Tratamiento Penal	Se sugiere fiscalizar operadoras telefónicas para evitar suplantación de identidad, facilitar geolocalización precisa e inmediata, supervisar venta lícita de software e implementar leyes específicas para nuevas formas de ciberdelincuencia.

4.3. Pruebas estadísticas – comprobación de hipótesis

4.3.1 Comprobación de la hipótesis general

El tratamiento penal de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.

Tabla 25
Coeficiente de determinación entre tratamiento penal de los delitos informáticos y la ciberdelincuencia

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Solo intersección	60,200			
Final	10,548	50,554	2	,000

Los resultados de la Tabla 17, muestran un modelo estadístico basado en el logaritmo de verosimilitud (-2LL) y el Chi-cuadrado, con un valor significativo (Sig. = 0.000), lo que indica que existe una relación estadísticamente significativa entre el tratamiento penal de los delitos informáticos y la ciberdelincuencia en el distrito judicial de Tacna durante el período 2019-2022. El modelo final, con un Chi-cuadrado de 50.554 y 2 grados de libertad, sugiere que las variables incluidas

en el análisis explican una proporción relevante de la variabilidad observada en la ciberdelincuencia. Jurídicamente, esto respalda la hipótesis general de que el tratamiento penal (dimensiones legislativa, procesal y reguladora) incide en las modalidades delictivas y medidas preventivas o sancionadoras relacionadas con delitos informáticos.

4.3.2 Verificación de la primera hipótesis específica

El tratamiento legislativo de los delitos informáticos incide directamente en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.

Tabla 26

Coeficiente de determinación entre tratamiento legislativo de los delitos informáticos y la ciberdelincuencia

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Solo intersección	61,215			
Final	10,124	62,250	2	,000

Los resultados presentados en la Tabla 18, muestran un modelo estadístico significativo para evaluar la relación entre el tratamiento legislativo de los delitos informáticos y la ciberdelincuencia en el distrito judicial de Tacna durante el período 2019-2022. El logaritmo de la verosimilitud (-2LL) disminuyó de 61.215 en el modelo inicial (solo intersección) a 10.124 en el modelo final, lo que indica que las variables incluidas mejoran sustancialmente la capacidad explicativa del modelo. Además, el Chi-cuadrado obtenido (62.250) con 2 grados de libertad y una significancia de 0.000 confirma que el modelo es estadísticamente significativo, evidenciando una relación entre el tratamiento legislativo y la ciberdelincuencia. Jurídicamente, estos resultados respaldan la hipótesis de que las disposiciones

legislativas inciden directamente en las modalidades delictivas y medidas preventivas o sancionadoras relacionadas con los delitos informáticos.

4.3.3 Verificación de la segunda hipótesis específica

El tratamiento procesal de los delitos informáticos incide directamente en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.

Tabla 27

Coeficiente de determinación entre tratamiento procesal de los delitos informáticos y la ciberdelincuencia

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	60,250			
Final	17,350	50,210	2	,000

Según la Tabla 19, el análisis del modelo con tratamiento procesal y ciberdelincuencia muestra una mejora significativa en el ajuste en comparación con el modelo de "solo intersección", indicado por una reducción en el Logaritmo de la verosimilitud -2 de 60,250 a 17,350 y un valor de Chi-cuadrado de 50,210 con 2 grados de libertad, resultando en una significancia de .000. Desde una perspectiva jurídica, esto implica que el tratamiento procesal de los delitos informáticos tiene una relación estadísticamente significativa con la ciberdelincuencia en el distrito judicial de Tacna durante el período 2019-2022.

4.3.4 Verificación de la tercera hipótesis específica

El incumplimiento de la finalidad reguladora de los delitos informáticos incide directamente en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.

Tabla 28

Coeficiente de determinación entre el incumplimiento de la finalidad reguladora de los delitos informáticos y la ciberdelincuencia

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	80,003			
Final	10,000	65,320	2	,000

La Tabla 20, presenta el coeficiente de correlación entre el incumplimiento de la finalidad reguladora de los delitos informáticos y la ciberdelincuencia en el distrito judicial de Tacna 2019-2022. La reducción del Logaritmo de la verosimilitud -2 de 80.003 a 10.000 y el valor de Chi-cuadrado de 65.320, con 2 grados de libertad y una significancia (Sig.) de 0.000, indican un modelo estadísticamente significativo. Jurídicamente, esto sugiere que el incumplimiento de la finalidad reguladora de los delitos informáticos está relacionado con la ciberdelincuencia. En otras palabras, cuando las leyes y regulaciones no logran su objetivo de prevenir o controlar los delitos informáticos, la ciberdelincuencia tiende a ser mayor en Tacna.

.

CAPÍTULO V

DISCUSIÓN

El tratamiento penal de los delitos informáticos y la ciberdelincuencia en el distrito judicial de Tacna durante el período 2019-2022, suscita interrogantes cruciales acerca de la efectividad de las leyes vigentes, su aplicación práctica y los retos que enfrenta el sistema judicial ante un fenómeno en constante transformación. El objetivo general de esta investigación fue analizar en qué medida el tratamiento penal de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022. Para ello, se contrastaron los resultados estadísticos obtenidos con antecedentes nacionales, internacionales y locales, considerando también los objetivos específicos planteados.

La proliferación de la ciberdelincuencia en los últimos años es innegable, impulsada por el avance tecnológico y la creciente digitalización de las actividades económicas y sociales. Como señala Vinelli (2021), esta evolución, si bien ha traído consigo numerosos beneficios, también ha expuesto vulnerabilidades críticas en los sistemas informáticos. En el distrito judicial de Tacna, los delitos más comunes reportados por las autoridades locales son el fraude cibernético, la estafa y el hurto digital. Esta realidad refleja una tendencia global, donde el fraude electrónico y la suplantación de identidad se posicionan como los delitos más frecuentes asociados al uso de las tecnologías digitales.

Desde una perspectiva nacional, investigaciones como la de Ventura (2021) revelan que el sistema penal peruano presenta deficiencias legales significativas para abordar eficazmente los delitos informáticos. La falta de tipificación clara de modalidades como el *phishing, smishing y vishing* limita la capacidad del sistema judicial para sancionar adecuadamente estas conductas. Este hallazgo se relaciona directamente con el primer objetivo específico de la investigación: determinar en

qué medida el tratamiento legislativo de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2021. La evidencia sugiere que la legislación actual es insuficiente y no abarca todas las modalidades delictivas emergentes, lo que contribuye a la persistencia de la ciberdelincuencia.

La Ley 30096 (Ley de Delitos Informáticos) y sus modificaciones representan un esfuerzo del legislador peruano por regular esta problemática. No obstante, estudios como el de Pardo (2018) demuestran que su aplicación es limitada, debido a interpretaciones ambiguas y a una cobertura que no abarca todas las modalidades delictivas emergentes. Esta deficiencia legal genera incertidumbre entre los operadores judiciales y las víctimas, obstaculizando la persecución efectiva de los delitos informáticos. En Tacna, esta situación se manifiesta en una percepción generalizada de impunidad entre los ciudadanos afectados por ciberdelitos.

En cuanto al segundo objetivo específico –identificar en qué medida el tratamiento procesal de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022, los resultados apuntan a desafíos importantes en el tratamiento de las pruebas digitales. Gallegos (2022) subraya que estas pruebas no cuentan con un manejo especializado en el sistema jurídico peruano, lo que compromete su admisibilidad y valoración en juicio. En casos de ciberdelincuencia, donde la evidencia digital es fundamental para establecer la responsabilidad penal, esta problemática se agudiza. En Tacna, las limitaciones tecnológicas y presupuestarias que afectan al Ministerio Público y al Poder Judicial exacerban esta carencia.

El Convenio de Budapest sobre ciberdelincuencia ha servido como un referente internacional para establecer estándares legales y operativos en la lucha contra estos delitos. Sin embargo, Benavides & SanMartín (2021) señalan que países como Perú aún enfrentan dificultades para implementar plenamente las disposiciones de este convenio debido a restricciones legales y estructurales. En comparación con otras jurisdicciones internacionales que han desarrollado sistemas avanzados para rastrear y sancionar delitos informáticos, Perú muestra un rezago significativo que impacta directamente en regiones como Tacna.

Un análisis comparativo con otros países latinoamericanos revela similitudes en cuanto al incremento sostenido de los delitos informáticos. Saltos et al. (2021) destacan que en Ecuador estos delitos han mostrado un crecimiento acelerado debido al avance tecnológico y a la falta de regulación adecuada. Este contexto regional refuerza la necesidad urgente de fortalecer tanto las normativas como las capacidades operativas para enfrentar este fenómeno transnacional.

El tercer objetivo específico –establecer en qué medida el incumplimiento de la finalidad reguladora de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022– se relaciona con el impacto sociológico del tratamiento penal de estos delitos. Se observa una desconexión entre las expectativas ciudadanas y la respuesta institucional. La población percibe que las medidas adoptadas son insuficientes para garantizar su seguridad digital, lo cual genera desconfianza hacia el sistema judicial. Estudios como el de Chilcon (2020) respaldan este sentimiento, señalando que la seguridad informática en sectores públicos clave sigue siendo vulnerable debido a una protección inadecuada contra ataques cibernéticos.

Desde una perspectiva local, el distrito judicial de Tacna enfrenta desafíos específicos relacionados con la implementación efectiva del marco legal existente. Las autoridades locales deben lidiar con recursos limitados y una infraestructura tecnológica insuficiente para abordar casos complejos de ciberdelincuencia. La falta de coordinación entre instituciones clave como la Policía Nacional del Perú y el Ministerio Público dificulta aún más la persecución penal efectiva.

En términos estadísticos, los datos recopilados durante 2021 muestran un aumento significativo en las denuncias por ciberdelitos en Tacna. Este incremento puede atribuirse tanto a una mayor incidencia real como a una mayor conciencia ciudadana sobre estos delitos. Sin embargo, este aumento también pone en evidencia las limitaciones del sistema judicial para procesar eficazmente estos casos dentro de plazos razonables.

En conclusión, el análisis realizado, permite afirmar que el tratamiento penal de los delitos informáticos en Tacna incide de manera significativa en la ciberdelincuencia. Las deficiencias legislativas, los desafíos procesales y el

incumplimiento de la finalidad reguladora de las normas contribuyen a la persistencia de este fenómeno. Para mejorar esta situación, es fundamental reforzar el marco normativo existente mediante la tipificación clara de todas las modalidades delictivas relevantes e invertir en tecnología y capacitación especializada para los operadores judiciales. Asimismo, se requiere una mayor cooperación internacional para adoptar mejores prácticas y herramientas tecnológicas avanzadas que permitan enfrentar eficazmente este fenómeno globalizado. Solo mediante un enfoque integral será posible reducir significativamente la incidencia de la ciberdelincuencia en regiones vulnerables como Tacna.

CAPÍTULO VI
CONCLUSIONES

El tratamiento penal de los delitos informáticos incide significativamente en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022 ($\chi^2 = 50.554$, $p = .000$). El incremento del 30 % en las denuncias, aunado a la percepción de ineficacia del sistema por parte de los operadores judiciales, sugiere que el tratamiento legislativo, procesal y el incumplimiento de la finalidad reguladora– no logran disuadir ni controlar la ciberdelincuencia de manera efectiva.

El tratamiento legislativo de los delitos informáticos incide directamente en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022 ($\chi^2 = 62.250$, $p = .000$). A pesar de los esfuerzos representados por la Ley 30096, las deficiencias en su formulación –tales como ambigüedades y una cobertura limitada– obstaculizan la adecuada tipificación y sanción de delitos emergentes como el phishing y el smishing. Esta situación, corroborada por las entrevistas realizadas a operadores judiciales, limita la capacidad del sistema para abordar eficazmente estas nuevas formas de criminalidad.

El tratamiento procesal de los delitos informáticos incide directamente en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022 ($\chi^2 = 50.210$, $p = .000$). Este impacto se manifiesta en los obstáculos derivados de la falta de especialización en el manejo de pruebas digitales, lo cual se evidencia en la alta tasa de archivos de casos por insuficiencia probatoria. Esta situación, agravada por la carencia de equipamiento tecnológico adecuado y la insuficiente capacitación del personal, dificulta severamente la persecución penal efectiva de estos delitos.

El incumplimiento de la finalidad reguladora de los delitos informáticos incide directamente en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022 (χ^2

= 62.250, p = .000). Esta conclusión se basa en la manifiesta desconexión entre las expectativas ciudadanas de seguridad digital y la respuesta institucional efectiva, lo que genera desconfianza y desalienta la denuncia de estos delitos. La falta de campañas de concientización sobre los riesgos y medidas de protección en el entorno digital exacerba la vulnerabilidad de la población frente a la ciberdelincuencia.

CAPÍTULO VII
RECOMENDACIONES

Para abordar de manera más efectiva la ciberdelincuencia en el distrito judicial de Tacna, se recomienda encarecidamente la creación de una comisión multisectorial, liderada por el Ministerio de Justicia y Derechos Humanos, y conformada por representantes del Poder Judicial, el Ministerio Público, la Policía Nacional del Perú (a través de la DIVINDAT), y expertos de la sociedad civil especializados en ciberseguridad y derechos digitales; esta comisión deberá encargarse de realizar una revisión exhaustiva del marco legal, procesal y tecnológico relacionado con la ciberdelincuencia, analizando la efectividad de las leyes vigentes, los obstáculos en la investigación y procesamiento de estos delitos, y las necesidades de capacitación y equipamiento de los operadores judiciales, con el objetivo de proponer reformas integrales que permitan un abordaje más efectivo de esta problemática.

Considerando las deficiencias identificadas en la Ley 30096 y su impacto en la lucha contra la ciberdelincuencia, se recomienda al Congreso de la República del Perú, a través de su Comisión de Justicia y Derechos Humanos, y con el apoyo técnico del Ministerio de Justicia y Derechos Humanos y expertos en derecho informático, llevar a cabo una modificación integral de dicha ley, eliminando ambigüedades, ampliando su cobertura para incluir las nuevas modalidades delictivas como phishing, smishing, vishing, ransomware, entre otras, y armonizándola con los estándares internacionales establecidos en el Convenio de Budapest, garantizando así una legislación que permita la adecuada tipificación y sanción de los delitos informáticos, facilitando la labor de fiscales y jueces en la persecución de estos ilícitos.

Ante los desafíos que plantea el tratamiento procesal de los delitos informáticos, se recomienda al Poder Judicial (a través de su Consejo Ejecutivo), al Ministerio Público (a través de la Fiscalía de la Nación), a la Academia de la Magistratura, y a la Policía Nacional del Perú (a través de la DIVINDAT), trabajar de manera coordinada para desarrollar e implementar protocolos especializados para la recolección, preservación y análisis de pruebas digitales, garantizando su admisibilidad y valoración en juicio; asimismo, se insta a invertir en la adquisición de tecnología forense digital de última generación para la DIVINDAT, el Ministerio Público y el Poder Judicial; implementar programas de capacitación continua y especializada para fiscales, jueces, policías y peritos en materia de ciberdelincuencia y prueba digital; y crear unidades especializadas en ciberdelincuencia dentro del Ministerio Público y el Poder Judicial, con personal altamente capacitado y dedicado exclusivamente a estos casos.

Para abordar la desconexión entre las expectativas ciudadanas y la respuesta institucional en materia de seguridad digital, se recomienda al Ministerio de Transportes y Comunicaciones (MTC), al Ministerio de Educación (MINEDU), al Ministerio del Interior (MININTER), a INDECOPI, y a las organizaciones de la sociedad civil, diseñar e implementar una Estrategia Nacional de Concientización y Seguridad Digital, que incluya campañas educativas dirigidas a la población en general sobre los riesgos de la ciberdelincuencia y las medidas de protección que pueden adoptar; incorporar contenidos sobre seguridad digital en los currículos escolares de todos los niveles educativos; promover la creación de alianzas público-privadas para la difusión de información sobre seguridad digital a través de los medios de comunicación y las redes sociales; fortalecer los mecanismos de denuncia de delitos informáticos, facilitando el acceso de las víctimas a la justicia y brindándoles el apoyo necesario; y crear un portal web con información clara y accesible sobre ciberseguridad, consejos para protegerse de los delitos informáticos, y los pasos a seguir en caso de ser víctima de un ciberdelito.

PROPUESTA LEGISLATIVA: TRATAMIENTO PENAL DE LOS DELITOS INFORMÁTICOS Y LA CIBERDELINCUENCIA EN EL DISTRITO JUDICIAL DE TACNA (2019-2022)

Fórmula Legal

1. Modificación de la Ley 30096 ("Ley de Delitos Informáticos"):
    - Artículo 2 (Acceso ilícito): Incrementar las penas privativas de libertad de 3-6 años a 4-8 años para casos de acceso con vulneración de medidas de seguridad.
    - Artículo 4 (Atentado contra sistemas informáticos): Incorporar sanciones específicas para ataques a infraestructuras críticas (ej. hospitales, entidades financieras), con penas de 5-10 años.
    - Artículo 8 (Fraude informático): Establecer multas proporcionales al monto defraudado (ej. 20 % del valor afectado) y penas de 5-12 años si se afecta el patrimonio estatal.
2. Creación de un Protocolo de Investigación Especializado:
    - Implementar procesos judiciales acelerados (*Proceso Inmediato*) para casos de ciberdelitos con evidencia digital clara.
    - Designar fiscales y jueces especializados en ciberdelincuencia en el Distrito Judicial de Tacna.
3. Ratificación de Enmiendas al Convenio de Budapest:
    - Fortalecer la cooperación internacional para extradición de ciberdelincuentes y homologación de pruebas digitales.

Exposición de Motivos

Contexto (2019-2022):

- Según el *Reporte de Ciberdelincuencia* (2021), Tacna registró un aumento del 356 % en denuncias por delitos informáticos (de 83 en 2019 a 426 en 2021), principalmente fraudes y ataques a sistemas informáticos.
- La Ley 30096 presenta vacíos en la tipificación de delitos emergentes (ej. *ransomware*, suplantación de identidad masiva) y en la aplicación de sanciones proporcionales al daño económico (ej. pérdidas de S/ 11.7 millones en el sector privado tacneño en 2021).

Necesidad de Reforma:

- Actualización normativa: Alinear la legislación peruana con el Convenio de Budapest para abordar delitos transnacionales (ej. interceptación de datos, *phishing*).
- Efectividad procesal: Reducir la duración promedio de casos (actualmente 18 meses) mediante procesos especializados y uso de peritajes digitales.
- Prevención: Combatir la "cifra negra" (subregistro del 60 % en Tacna) con campañas de denuncia ciudadana y protección de datos.

Análisis Costo-Beneficio

Aspecto	Costo (S/)	Beneficio
Capacitación a operadores judiciales	500,000 (anual)	Reducción del 30 % en tiempos de investigación (ahorro de S/ 1.2 millones/año).
Adquisición de software forense	200,000 (inicial)	Incremento del 40 % en resolución de casos (evita pérdidas por S/ 5 millones/año).
Campañas de prevención ciudadana	150,000 (anual)	Disminución del 25 % en víctimas de fraude informático (ahorro social: S/ 3 millones/año).
Total	850,000	Beneficio neto estimado: S/ 7.2 millones/año

Conclusión

La propuesta busca fortalecer el marco legal y procesal contra la ciberdelincuencia en Tacna, priorizando la protección de bienes jurídicos (datos, patrimonio) y la eficiencia judicial. La inversión en tecnología y especialización reducirá costos sociales y económicos, alineándose con los ODS 16 (Paz y Justicia) y 9 (Innovación).

REFERENCIAS

Arrabal, P. (2019). *Tratamiento procesal de la prueba tecnológica*. https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=TRATAMIENTO+PROCESAL+DE+LA+PRUEBA+TECNOL%C3%93GICA&btnG=

Bañón, M. (2020). *El tratamiento penal de los delitos cometidos a través de internet. La protección frente a las estafas informáticas.* https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=EL+TRATAMIENTO+PENAL+DE+LOS+DELITOS+COMETIDOS+A+TRAV%C3%89S+DE+INTERNET.+LA+PROTECCI%C3%93N+FRENTE+A+LAS+ESTAFAS+INFORM%C3%81TICAS&btnG=

Benavides, M., & SanMartín, W. (2021). *Los delitos informáticos en el Código Orgánico Integral Penal y el Convenio Internacional de Budapest*. http://www.dspace.uce.edu.ec/handle/25000/25177

Bullón, J. (2019). La importancia de la adhesión al convenio sobre la ciberdelincuencia para la legislación peruana de delitos informáticos. *Repositorio Institucional - UCV*. https://repositorio.ucv.edu.pe/handle/20.500.12692/83985

Chilcon, M. (2020). *El Ciber Crimen en el Perú y su incidencia en la Seguridad Nacional*. https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=EL+CIBERCRIMEN+EN+EL+PERU+Y+SU+INCIDENCIA+EN+LA+SEGURIDAD+NACIONAL&btnG=

Cuenca, H. (2022). *Articulación de la Fiscalía General del Estado... - Google Académico*. https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=Articulaci%C3%B3n+de+la+Fiscal%C3%ADa+General+del+Estado+para+la+persecuci%C3%B3n+de+delitos+cibern%C3%A9ticos&btnG=

Custodio, Y. (2021). Las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático. *Repositorio Institucional - UCV*. https://repositorio.ucv.edu.pe/handle/20.500.12692/74797

Gallegos, S. (2022). *La Evidencia Digital y los Delitos Informáticos... - Google Académico*. https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=La+Evidencia+Digital+y+los+Delitos+Inform%C3%A1ticos+en+el+Sistema+Jur%C3%ADdico+Peruano%2C+2020&btnG=

Gamba, J. (2019). *El delito informático en el marco jurídico colombiano y el derecho comparado: Caso de la transferencia no consentida de activos*. https://bdigital.uexternado.edu.co/entities/publication/42898030-1af8-4c38-a535-ed61412a6e62

González, N., Denis, D., & Águila, R. (2018). El delito informático, su tratamiento en el ordenamiento jurídico cubano. *Caribeña de Ciencias Sociales*, *diciembre*. https://www.eumed.net/rev/caribe/2018/12/delito-informatico-cuba.html

Hernández, N., & Patricio, A. (2022). La obtención de pruebas en delitos cibernéticos en las fiscalías especializadas en ciberdelincuencia de Lima Centro 2021. *Repositorio Institucional - UCV*. https://repositorio.ucv.edu.pe/handle/20.500.12692/88754

Lujan, Z. (2022). Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito Judicial de Lima, 2022. *Repositorio Institucional - UCV*. https://repositorio.ucv.edu.pe/handle/20.500.12692/89722

Pardo, A. (2018). *Tratamiento jurídico penal de los delitos informáticos... - Google Académico*. https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=Tratamiento+jur%C3%ADdico+penal+de+los+delitos+inform%C3%A1ticos+contra+el+patrimonio%2C+Distrito+Judicial+de+Lima%2C+2018&btnG=

Prieto, N., & Vargas, G. (2020). *Ciberdelincuencia, enfocada en la apropiación de información a través de medios electrónicos y su influencia en el*

cometimiento de delitos informáticos.
http://repositorio.ug.edu.ec/handle/redug/50396

Rivera, F. (2021). *Prevenir los delitos informáticos en el Sistema Financiero Ecuatoriano del 2020 al 2022*.
http://repositorio.ug.edu.ec/handle/redug/58070

Román, E. (2020). Modificación legislativa de la ley 30096 de delitos informáticos para su eficacia contra la ciberdelincuencia en la ciudad de Chiclayo. *Repositorio Institucional - USS*.
https://repositorio.uss.edu.pe/handle/20.500.12802/10463

Saltos, M., Robalino, J., & Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. *Conrado*, *17*(78), 343-351.

Schirakian, N. (2021). *Evidencia informática: ¿un nuevo paradigma para el derecho procesal penal?*
http://repositorio.udesa.edu.ar/jspui/handle/10908/18968

Tellez, J. (2019). *Los «Delitos Informáticos»: Situación en México—Buscar con Google*.
https://www.google.com/search?q=Los+%22Delitos+Inform%C3%A1ticos%22%3A+Situaci%C3%B3n+en+M%C3%A9xico

Vargas, W. (2022). Necesidad de tipificar la estafa básica en la ley de delitos informáticos para reducir la impunidad en el Perú. *Repositorio Institucional - UCV*.
https://repositorio.ucv.edu.pe/handle/20.500.12692/83704

Ventura, M. (2021). *La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima, 2020,.*
https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=LA+TIPIFICACI%C3%93N+DEL+PHISHING%2C+SMISHING+Y+VISHING+EN+NUESTRO+SISTEMA+PENAL+PERUANO%2C+PARA+LA+LUCHA+CONTRA+LA+CIBERDELINCUENCIA+EN+LIMA%2C+2020&btnG=

Vinelli, R. (2021). *Los delitos informáticos y su relación con la criminali... - Google Académico*. https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=Los+delitos+inform%C3%A1ticos+y+su+relaci%C3%B3n+con+la+criminalidad+econ%C3%B3mica&btnG=

Zarzosa, E. (2018). Tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao -2017. *Universidad César Vallejo*. https://repositorio.ucv.edu.pe/handle/20.500.12692/21042

ANEXOS

ANEXO 01: MATRIZ DE CONSISTENCIA

TÍTULO: TRATAMIENTO PENAL DE LOS DELITOS INFORMÁTICOS Y LA CIBERDELINCUENCIA EN EL DISTRITO JUDICIAL DE TACNA, 2019-2022

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	POBLACIÓN Y MUESTRA	DISEÑO Y TIPO DE INVESTIGACIÓN	INSTRUMENTO Y TÉCNICA
PROBLEMA PRINCIPAL: ¿En qué medida el tratamiento penal de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022?	**OBJETIVO GENERAL:** Analizar en qué medida el tratamiento penal de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.	**HIPÓTESIS GENERAL:** El tratamiento penal de los delitos informáticos incide significativamente en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.	V. Independiente X: Tratamiento penal de los delitos informáticos	**X1**: Tratamiento legislativo	- Tipos de delitos - Tipificación de delitos - Actualización normativa	**POBLACIÓN** 4 magistrados 10 Sentencias sobre delitos informáticos	**DISEÑO** No experimental	**TÉCNICA** - Observación - Entrevista
				X2: Tratamiento procesal	- Existencia de procesos judiciales especializados - Aplicación del Proceso Inmediato - Duración promedio de casos			
				X3: Incumplimiento de finalidad reguladora	- Sanciones administrativas - Vacíos legales - Efectividad en la prevención - Divergencia en criterios judiciales			
PROBLEMAS ESPECÍFICOS: ¿En qué medida el tratamiento legislativo de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022?	**OBJETIVOS ESPECÍFICOS:** Determinar la incidencia del tratamiento legislativo de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.	**HIPÓTESIS ESPECIFICAS:** El tratamiento legislativo de los delitos informáticos incide significativamente en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.de Tacna, 2019-2022.						
¿En qué medida el tratamiento procesal de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022?	Identificar la incidencia del tratamiento procesal de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022	El tratamiento procesal de los delitos informáticos incide significativamente en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.	**Variable Dependiente:** Y: Ciberdelincuencia	Modalidades delictivas	- Tipos de delitos	**MUESTRA** 4 magistrados 10 sentencias sobre delitos informáticos	**TIPO** Básica **NIVEL** Explicativo	**INSTRUMENTO** - Ficha de análisis - Cedula de entrevista
				Medidas preventivas	- Tipos de medidas preventivas			
¿En qué medida el incumplimiento de la finalidad reguladora de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022?	Establecer la incidencia del incumplimiento de la finalidad reguladora de los delitos informáticos incide en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022	El incumplimiento de la finalidad reguladora de los delitos informáticos incide significativamente en la ciberdelincuencia en el distrito judicial de Tacna, 2019-2022.		Medidas sancionadoras	- Penas privativas de libertad - Multas y sanciones administrativas			

ANEXO 02: ENTREVISTA CUALITATIVA A PROFUNDIDAD: TRATAMIENTO PENAL DE LOS DELITOS INFORMÁTICOS Y LA CIBERDELINCUENCIA EN TACNA

Objetivo:

El objetivo de esta entrevista cualitativa es analizar el tratamiento penal de los delitos informáticos y su incidencia en la ciberdelincuencia en el distrito judicial de Tacna. Se busca obtener información detallada sobre el cumplimiento de normas laborales, las condiciones de trabajo, y los derechos de los trabajadores, así como su impacto en el entorno laboral.

Entrevista Cualitativa

Categoría: Tratamiento Penal de los Delitos Informáticos

1. ¿Cómo considera la tipificación de la Ley de Delitos Informáticos (Ley 30096) en el Perú? ¿Qué aspectos cree que podrían mejorarse?
2. ¿Cuáles son los principales desafíos que enfrenta al momento de procesar y analizar pruebas digitales en casos de delitos informáticos? ¿Cómo se abordan estas dificultades en su práctica judicial?
3. ¿De qué manera cree que la legislación actual sobre delitos informáticos cumple con su finalidad preventiva? ¿Qué medidas adicionales podrían implementarse para prevenir estos delitos?
4. ¿Cómo evalúa la efectividad de las sanciones actuales para los delitos informáticos en términos de disuadir futuras conductas delictivas? ¿Qué ajustes considera necesarios en este sentido?

Categoría: Ciberdelincuencia

5. ¿Qué tipos de delitos informáticos son más comunes en el distrito judicial de Tacna? ¿Cómo han evolucionado estos delitos en los últimos años?
6. ¿Qué medidas preventivas se están implementando actualmente para combatir la ciberdelincuencia en Tacna? ¿Cómo se evalúa su efectividad?
7. ¿Qué tipos de sanciones se aplican comúnmente a los delincuentes informáticos en Tacna? ¿Cómo se determina la gravedad de las sanciones en función del delito cometido?
8. ¿Cómo se coordina la cooperación entre instituciones judiciales, policiales y otras entidades para combatir la ciberdelincuencia en Tacna? ¿Qué desafíos enfrentan en este proceso?

9. ¿Qué tipo de capacitación y recursos se proporcionan a jueces y fiscales para manejar casos de delitos informáticos? ¿Qué necesidades identifica en este ámbito?
10. ¿Cómo percibe el impacto de la ciberdelincuencia en la comunidad local? ¿Qué medidas cree que podrían tomarse para aumentar la conciencia sobre este tema?
11. ¿Qué propuestas tiene para mejorar el tratamiento penal de los delitos informáticos y la ciberdelincuencia en el distrito judicial de Tacna?

ANEXO 03: Ficha de análisis documental de expediente judicial sobre delitos informáticos

Dimensión	Indicador	Sí	No
Tratamiento penal de los delitos informáticos	Tipos de delitos		
Tratamiento legislativo (X1)	Tipificación de delitos		
	Actualización normativa		
Tratamiento procesal (X2)	Existencia de procesos judiciales especializados		
	Aplicación del Proceso Inmediato		
	Duración promedio de casos		
Incumplimiento de finalidad reguladora (X3)	Sanciones administrativas		
	Vacíos legales		
	Efectividad en la prevención		
Ciberdelincuencia	Divergencia en criterios judiciales		
Modalidades delictivas (Y1)	Tipos de delitos		
Medidas preventivas (Y2)	Tipos de medidas preventivas		
Medidas sancionadoras (Y3)	Penas privativas de libertad		
	Multas y sanciones administrativas		

****CUESTIONARIO: TRATAMIENTO PENAL DE LOS DELITOS INFORMÁTICOS Y LA CIBERDELINCUENCIA, DISTRITO JUDICIAL DE TACNA****

Estimado participante:

El presente cuestionario tiene como finalidad recoger información sobre el tratamiento legislativo, procesal y regulatorio de los delitos informáticos en el Distrito Judicial de Tacna, así como la percepción sobre las modalidades de ciberdelincuencia, medidas preventivas y sancionadoras aplicadas.

Las respuestas se registran según la siguiente **escala Likert**:

- **TA** = Totalmente de acuerdo
- **DA** = De acuerdo
- **I** = Indeciso
- **ED** = En desacuerdo
- **TED** = Totalmente en desacuerdo

Por favor, marque la alternativa que mejor represente su opinión.

Tratamiento Legislativo

Ítem	Enunciado	TED	ED	I	DA	TA
1	La legislación penal peruana define de manera clara los distintos tipos de delitos informáticos.	☐	☐	☐	☐	☐
2	La actual tipificación de delitos informáticos abarca adecuadamente la mayoría de conductas ilícitas digitales.	☐	☐	☐	☐	☐
3	La normativa penal informática se actualiza con la rapidez necesaria frente a los avances tecnológicos.	☐	☐	☐	☐	☐
4	Las definiciones legales sobre delitos informáticos permiten una correcta aplicación en los casos prácticos.	☐	☐	☐	☐	☐
5	La legislación vigente presenta vacíos que dificultan la persecución de delitos informáticos.	☐	☐	☐	☐	☐

Tratamiento Procesal

Ítem	Enunciado	TED	ED	I	DA	TA
6	El sistema judicial peruano cuenta con procesos o juzgados especializados en delitos informáticos.	☐	☐	☐	☐	☐
7	El Proceso Inmediato es adecuado para abordar casos simples de ciberdelincuencia.	☐	☐	☐	☐	☐
8	La duración promedio de los procesos por ciberdelitos garantiza una justicia oportuna.	☐	☐	☐	☐	☐
9	Los operadores de justicia están capacitados para manejar procedimientos relacionados con delitos informáticos.	☐	☐	☐	☐	☐
10	La falta de especialización procesal retrasa la resolución de casos de ciberdelincuencia. *(Invertido)*	☐	☐	☐	☐	☐

Incumplimiento de finalidad reguladora

Ítem	Enunciado	TED	ED	I	DA	TA
11	Las sanciones administrativas relacionadas con delitos informáticos son aplicadas adecuadamente.	☐	☐	☐	☐	☐
12	Existen vacíos legales que impiden que la regulación cumpla su finalidad preventiva. *(Invertido)*	☐	☐	☐	☐	☐
13	La normativa penal vigente previene de manera efectiva la comisión de delincuencia informática.	☐	☐	☐	☐	☐
14	La falta de criterios judiciales uniformes genera inseguridad jurídica en casos informáticos. *(Invertido)*	☐	☐	☐	☐	☐
15	La regulación penal actual contribuye a reducir la incidencia de delitos informáticos en el país.	☐	☐	☐	☐	☐

VARIABLE DEPENDIENTE (Y): CIBERDELINCUENCIA

Modalidades delictivas

Ítem	Enunciado	TED	ED	I	DA	TA
1	Los ciberdelitos más frecuentes están relacionados con el fraude electrónico y la suplantación de identidad.	☐	☐	☐	☐	☐
2	Los casos de ciberdelitos suelen involucrar acceso indebido a sistemas o datos.	☐	☐	☐	☐	☐
3	Los ciberdelincuentes aprovechan vulnerabilidades técnicas para cometer delitos.	☐	☐	☐	☐	☐
4	Las modalidades delictivas informáticas evolucionan más rápido que la capacidad del sistema penal para afrontarlas.	☐	☐	☐	☐	☐
5	La ciberdelincuencia en el Perú ha aumentado en los últimos años.	☐	☐	☐	☐	☐

Medidas preventivas

Ítem	Enunciado	TED	ED	I	DA	TA
6	Las entidades públicas implementan medidas preventivas suficientes para reducir la ciberdelincuencia.	☐	☐	☐	☐	☐
7	Las campañas educativas sobre seguridad digital contribuyen a disminuir los ciberdelitos.	☐	☐	☐	☐	☐
8	Los usuarios comunes desconocen medidas básicas de prevención informática. *(Invertido)*	☐	☐	☐	☐	☐
9	Las empresas privadas aplican políticas adecuadas de protección de datos para prevenir delitos informáticos.	☐	☐	☐	☐	☐
10	Las medidas preventivas actuales en el Perú son insuficientes para detener el avance de la ciberdelincuencia. *(Invertido)*	☐	☐	☐	☐	☐

Medidas sancionadoras

Ítem	Enunciado	TED	ED	I	DA	TA
11	Las penas privativas de libertad en delitos informáticos son proporcionales al daño causado.	☐	☐	☐	☐	☐
12	Las sanciones pecuniarias (multas) son efectivas para disuadir la comisión de ciberdelitos.	☐	☐	☐	☐	☐
13	Las sanciones administrativas complementan de manera adecuada las sanciones penales.	☐	☐	☐	☐	☐
14	Las penas actuales no generan suficiente efecto preventivo en potenciales ciberdelincuentes. *(Invertido)*	☐	☐	☐	☐	☐
15	El marco sancionador en delitos informáticos debe fortalecerse para aumentar su eficacia.	☐	☐	☐	☐	☐

Gracias por su colaboración

ANEXO 04: VALIDACIÓN DE EXPERTOS

UNIVERSIDAD PRIVADA DE TACNA

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN POR CRITERIO DE ABOGADOS

I. DATOS GENERALES

1.1. Apellidos y nombres del abogado: CHOQUECAHUA AYNA ALEX
1.2. Cargo e institución donde labora: ABOGADO LITIGANTE
1.3. Nombre del instrumento evaluado: Tratamiento penal de los delitos informáticos y la ciberdelincuencia en el distrito judicial de Tacna.

II. ASPECTO DE LA EVALUACIÓN

INDICADORES	CRITERIOS	Deficiente 1	Baja 2	Regular 3	Buena 4	Muy buena 5
1. Actualidad	Adecuado al avance de la ciencia y tecnología.				X	
2. Aplicación	Los datos permiten un tratamiento estadístico pertinente.				X	
3. Claridad	Está formulado con lenguaje apropiado y comprensible.				X	
4. Coherencia	Entre variables, dimensiones o indicadores				X	
5. Consistencia	Pretende conseguir datos basados en teorías o modelos teóricos.					X
6. Metodología	Las estrategias responden al propósito de la investigación.					X
7. Objetividad	Permite medir hechos observables.					X
8. Organización	Presentación ordenada.					X
9. Pertinencia	Permite conseguir datos de acuerdo a los objetivos planteados.					X
10. Suficiencia	Comprende aspectos de las variables en cantidad y calidad suficientes					X

CONTEO TOTAL DE MARCAS Realice el conteo en cada una de las categorías de la escala	A	B	C	D	E
				16	30

Coeficiente de validez = $\frac{1xA+2xB+3xC+4xD+5xE}{50}$ = 48

III. CALIFICACIÓN GLOBAL (Ubique el coeficiente de validez obtenido en el intervalo respectivo y marque con un aspa en el círculo asociado)

CATEGORÍA	INTERVALO
Desaprobado	(0,00 – 0,60)
Observado	<0,60 – 0,70)
Aprobado	<0,70 – 1,00)

IV. OPINIÓN DE APLICABILIDAD:

☐ Contribuye a medir las dimensiones planteadas.
☐ No contribuye a medir las dimensiones planteadas.

V. DATOS COMPLEMENTARIOS:

5.1. N° DNI : 47338387
5.2. Correo electrónico : abogado.pamelaba.tcm@gmail.com
5.3. N° Celular : 952645417

Tacna; Octubre del 2024

UNIVERSIDAD PRIVADA DE TACNA

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN POR CRITERIO DE JUECES

I. DATOS GENERALES

1.1. Apellidos y nombres del juez: Gloria Katherine Gonzales Garcia
1.2. Cargo e institución donde labora: Fiscal Adjunto Penal – Ministerio Público
1.3. Nombre del instrumento evaluado: Tratamiento penal de los delitos informáticos y la ciberdelincuencia en el distrito judicial de Tacna.

II. ASPECTO DE LA EVALUACIÓN

INDICADORES	CRITERIOS	Deficiente 1	Baja 2	Regular 3	Buena 4	Muy buena 5
1. Actualidad	Adecuado al avance de la ciencia y tecnología.				x	
2. Aplicación	Los datos permiten un tratamiento estadístico pertinente.					x
3. Claridad	Esta formulado con lenguaje apropiado y comprensible.					x
4. Coherencia	Entre variables, dimensiones e indicadores					x
5. Consistencia	Pretende conseguir datos basados en teorías o modelos teóricos.					x
6. Metodología	Las estrategias responden al propósito de la investigación.					x
7. Objetividad	Permite medir hechos observables.					x
8. Organización	Presentación ordenada.					x
9. Pertinencia	Permite conseguir datos de acuerdo a los objetivos planteados.					x
10. Suficiencia	Comprende aspectos de las variables en cantidad y calidad suficiente.					x

CONTEO TOTAL DE MARCAS Realice el conteo en cada una de las categorías de la escala	A	B	C	D	E

Coeficiente de validez= $\frac{1 \times A + 2 \times B + 3 \times C + 4 \times D + 5 \times E}{50} = 44$

III. CALIFICACIÓN GLOBAL (Ubique el coeficiente de validez obtenido en el intervalo respectivo y marque con un aspa en el círculo asociado)

CATEGORIA	INTERVALO
Desaprobado	(0,00 – 0,60)
Observado	<0,60 – 0,70)
Aprobado	<0,70 – 1,00)

IV. OPINIÓN DE APLICABILIDAD:

[ ] Contribuye a medir las dimensiones planteadas.
[ ] No contribuye a medir las dimensiones planteadas.

V. DATOS COMPLEMENTARIOS:

5.1. Nº DNI : 43451910
5.2. Correo electrónico : kathygo17.gg@gmail.com
5.3. Nº Celular : 929317549

Tacna; octubre del 2024

UNIVERSIDAD PRIVADA DE TACNA

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN POR CRITERIO DE JUECES Y FISCALES

I. **DATOS GENERALES**

1.1. Apellidos y nombres del Fiscal: DR. VARGAS ESPINOZA WILIAM
1.2. Cargo e institución donde labora: FISCAL PROVINCIAL
1.3. Nombre del instrumento evaluado:
1.4.

II. **ASPECTO DE LA EVALUACIÓN**

INDICADORES	CRITERIOS	Deficiente 1	Baja 2	Regular 3	Buena 4	Muy buena 5
1. Actualidad	Adecuado al avance de la ciencia y tecnología.				X	
2. Aplicación	Los datos permiten un tratamiento estadístico pertinente.				X	
3. Claridad	Está formulado con lenguaje apropiado y comprensible.				X	
4. Coherencia	Entre variables, dimensiones e indicadores				X	
5. Consistencia	Pretende conseguir datos basados en teorías o modelos teóricos.				X	
6. Metodología	Las estrategias responden al propósito de la investigación.					X
7. Objetividad	Permite medir hechos observables.					X
8. Organización	Presentación ordenada.					X
9. Pertinencia	Permite conseguir datos de acuerdo a los objetivos planteados.					X
10. Suficiencia	Comprende aspectos de las variables en cantidad y calidad suficiente.					X

CONTEO TOTAL DE MARCAS Realice el conteo en cada una de las categorías de la escala				20	25
	A	B	C	D	E

Coeficiente de validez= $\frac{1 \times A + 2 \times B + 3 \times C + 4 \times D + 5 \times E}{50} = 45$

III. **CALIFICACIÓN GLOBAL** (Ubique el coeficiente de validez obtenido en el intervalo respectivo y marque con un aspa en el círculo asociado)

CATEGORÍA	INTERVALO
Desaprobado	(0,00 – 0,60)
Observado	<0,60 – 0,70)
Aprobado	<0,70 – 1,00)

IV. **OPINIÓN DE APLICABILIDAD:**

(X) Contribuye a medir las dimensiones planteadas.
( ) No contribuye a medir las dimensiones planteadas.

V. **DATOS COMPLEMENTARIOS:**

5.1. **N° DNI : 16806416**
5.2. **Correo electrónico : waltervargasesg@mail.com**
5.3. **N° Celular : 965635642**

Tacna; marzo del 2025