FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

TRABAJO DE INVESTIGACIÓN

El papel del estado en la lucha contra los delitos informáticos en Perú

PARA OPTAR EL GRADO ACADÉMICO DE BACHILLER EN DERECHO

Autora

Rivera de la Cruz Angelica

https://orcid.org/0009-0007-9648-3156

Línea de Investigación

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

Sublínea de Investigación

Derecho Público y Derecho Privado

Pimentel – Perú
2025

DECLARACIÓN JURADA DE ORIGINALIDAD

Quien suscribe la **DECLARACIÓN JURADA** es Rivera de la Cruz Angelica, egresada del Programa de Estudios de Derecho de la Universidad Señor de Sipán S.A.C, declaro bajo juramento que soy somos autora del trabajo titulado:

EL PAPEL DEL ESTADO EN LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS EN PERU

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

En virtud de lo antes mencionado, firma:

Rivera de la Cruz Angelica	DNI: 73259449	

Pimentel, 31 de enero de 2025.

7% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto mencionado
- Coincidencias menores (menos de 8 palabras)

Fuentes principales

6% Fuentes de Internet
1% Publicaciones
4% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.° de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Índice

Resumen

El trabajo de investigación que se presenta es de tipo descriptivo, sigue un diseño no experimental y tiene como objetivo general determinar cuál es el papel del estado en la lucha contra los delitos informáticos en Perú y como específicos identifica a los organismos internacionales que colaboran con Perú en ciberseguridad, describe como se financia la lucha contra el cibercrimen en Perú y analiza si existen casos concretos de colaboración público-privada en este ámbito. La técnica utilizada fue de análisis documental y los instrumentos utilizados son las fichas, las mismas que fueron aplicadas a los diversos documentos obtenidos de diversas fuentes. Se concluye que el Estado peruano desempeña un papel crucial en la lucha contra los delitos informáticos, pero necesita seguir fortaleciendo su marco legal, capacitando a su personal y fomentando la colaboración tanto a nivel nacional como internacional. La educación y la concientización de la población son igualmente vitales para prevenir estos delitos, estas colaboraciones permiten a Perú fortalecer su capacidad para enfrentar los desafíos del cibercrimen y mejorar su infraestructura de ciberseguridad, la financiación de la lucha contra el cibercrimen en Perú proviene de una combinación de recursos estatales, cooperación internacional, iniciativas privadas y fondos para investigación. Para ser efectiva, es fundamental que estas fuentes de financiamiento se mantengan y amplíen, adaptándose a las crecientes demandas de ciberseguridad.

Palabras Clave: Ciberdelito, ciberseguridad, informatico

Abstract

The research work presented is descriptive, follows a non-experimental design and has as its general objective to determine the role of the State in the fight against cybercrime in Peru and as specifics, to identify the international organizations that collaborate with Peru in cybersecurity, describe how the fight against cybercrime is financed in Peru and analyze whether there are specific cases of public-private collaboration in this area. The technique used was documentary analysis and the instruments used are the files, the same ones that were applied to the various documents obtained from various sources. It is concluded that the Peruvian State plays a crucial role in the fight against cybercrime, but needs to continue strengthening its legal framework, training its staff and promoting collaboration both nationally and internationally. Education and awareness of the population are equally vital to prevent these crimes, these collaborations allow Peru to strengthen its capacity to face the challenges of cybercrime and improve its cybersecurity infrastructure, the financing of the fight against cybercrime in Peru comes from a combination of state resources, international cooperation, private initiatives and research funds. To be effective, it is essential that these sources of funding be maintained and expanded, adapting to the growing demands of cybersecurity.

Keywords: Cybercrime, cybersecurity, computer science

I. INTRODUCCIÓN

1.1. Realidad Problemática

Los ciberdelitos, o delitos informáticos, son difíciles de combatir debido a los rápidos avances tecnológicos y a la creciente cantidad de delitos en línea, no es sorprendente que alguien clone una página web o utilice una tarjeta de crédito ajena, ya que estos delitos existen desde hace mucho tiempo y han ido en aumento en la actualidad, por lo tanto, es crucial que el estado desempeñe un papel efectivo en la prevención, sanción y promoción de medidas para enfrentar esta problemática. (Avalos, 2021).

El problema de los delitos informáticos tiene un origen internacional, a diferencia de otros delitos que requieren la presencia física de los delincuentes, en el caso de los ciberdelitos, basta con que haya personas con habilidades en computación para llevar a cabo actos ilícitos y obtener información valiosa o datos personales con fines económicos, decimos que este problema es de alcance internacional porque los países deben unirse para combatir los ciberdelitos, esto no solo implica crear convenios o leyes, sino también implementarlos de manera efectiva y colaborar globalmente, ya que identificar a los autores de estos delitos es particularmente complicado. (Bruna, 2022).

A nivel local, los delitos informáticos abarcan una variedad de actos ilícitos que están tipificados en la ley, incluyendo fraudes, delitos contra la indemnidad y libertad sexual, así como infracciones relacionadas con datos y sistemas informáticos, y el secreto de las comunicaciones, entre estos, los fraudes son los más comunes, donde los delincuentes emplean diferentes métodos, como clonar páginas web de bancos, realizar compras ilegales en línea y utilizar teléfonos robados para cometer delitos, sin embargo, no todas las denuncias presentadas ante el Ministerio Público resultan en acusaciones; muchas acaban archivadas debido a la falta de pruebas o a la dificultad para identificar a los culpables, esto se debe a que los ciberdelincuentes suelen utilizar herramientas que les

permiten operar de manera anónima, y los investigadores a menudo carecen de los recursos, conocimientos y herramientas necesarias para rastrear a estos delincuentes y recopilar las evidencias digitales requeridas. (Avalos, 2021).

A nivel regional, los delitos cibernéticos son variados, pero su efectividad se refleja en la escasez de sentencias condenatorias, aunque hay muchas denuncias, pocas se traducen en una persecución efectiva y en fallos concretos, en el año 2022, solo se dictaron dos sentencias por delitos informáticos en el distrito de Lambayeque, esto indica que estamos ante un problema persistente, donde la criminalidad en línea es cada vez más especializada, por lo tanto, las instituciones de justicia deben abordar la investigación con un enfoque especializado y con el uso de herramientas tecnológicas adecuadas, lo que es especialmente crucial para fiscales, policías, peritos y otras entidades locales.

Los vacíos actuales se encuentran tanto en el ámbito del conocimiento como en la normativa, ya que no se cuenta con un presupuesto adecuado ni con inversiones en capacitación para las entidades especializadas, asimismo, resulta fundamental que la legislación peruana se ajuste a lo establecido en el convenio de Budapest y que esta adaptación se lleve a cabo de manera efectiva. (Diaz, 2019).

En su investigación titulada *Ley de Delitos Informáticos N° 30096 y su influencia en la población de Chiclayo durante la pandemia de COVID-19*, se destaca la importancia de que la falta de una aplicación efectiva de esta ley genera un deterioro mental y emocional en la población, la ineficacia en las investigaciones de peritajes y evidencias informáticas, lo que lleva al archivo de muchas denuncias, el objetivo del estudio es determinar cómo esta ley impacta a la ciudadanía en el contexto del COVID-19, la conclusión señala que existe una correlación positiva moderada de 0,403 entre el delito informático y la afectación a la integridad personal de los ciudadanos, por lo tanto se recomienda que las autoridades responsables difundan información sobre la ley de delitos informáticos. (Villanueva, 2023).

La investigación sobre las fiscalías especializadas en delitos informáticos destaca

la importancia de promover un uso adecuado de las tecnologías en el ámbito de la ciberseguridad, su objetivo fue analizar la creación de fiscalías especializadas en delitos informáticos, con el fin de abordar los aspectos que complican las investigaciones y juicios relacionados con el fraude informático, la conclusión obtenida señala que la dificultad para perseguir y responsabilizar penalmente a los delincuentes es mayor debido a la falta de conocimientos tecnológicos y herramientas que permitan seguir sus rastros, así como a los vacíos jurídicos existentes. (Carbajal, 2022).

En la tesis titulada *La calificación fiscal en los delitos informáticos en el distrito fiscal de Lima Centro, 2019 – 2020,* se destaca la importancia de establecer parámetros basados en la teoría actual de los delitos informáticos y en el contexto del trabajo de la fiscalía durante las investigaciones, su objetivo principal es identificar cómo la calificación realizada por la fiscalía influye en la investigación de los ciberdelitos en Lima, la conclusión obtenida indica que la implementación y los cambios en la ley han propiciado un notable avance en las investigaciones, ya que existen fiscalías especializadas que se encargan de dirigir y calificar las indagaciones de manera específica para obtener pruebas sólidas. (Sotomayor, 2022).

En la tesis titulada *El Phishing en Uruguay,* se busca analizar la relación entre el phishing como forma de delito informático y la legislación uruguaya, este estudio se llevó a cabo con un enfoque cualitativo y se concluyó que resulta fundamental modificar y actualizar la Ley de Delitos Informáticos para cerrar los vacíos regulatorios existentes, de igual forma se sugiere que los países deberían establecer un tratado o acuerdo que les permita colaborar en la lucha contra este tipo de delitos. (Martínez, 2020).

En la investigación denominada *el Phishing en Argentina*, se propone evaluar el problema del phishing como una forma de delinquir en el ámbito informático y su relación con la legislación argentina, también analiza la Ley N° 26388 y los vacíos normativos que presenta y a través de una investigación cualitativa, concluye que resulta importante

modificar y actualizar la Ley de Delitos Informáticos para cerrar estas lagunas, además, enfatiza la importancia de establecer tratados o acuerdos que faciliten la cooperación entre países en la lucha contra el ciberdelito. (Salvi, 2019).

En el artículo titulado “Calificación Penal del Phishing como medida de seguridad informática para frenar los delitos informáticos”, se argumenta la necesidad de incluir el phishing como un delito informático en el ámbito del derecho penal, con el objetivo de proteger los derechos de propiedad y prevenir la impunida, el estudio utilizó técnicas de análisis jurídico, así como enfoques deductivos, inductivos y comparativos, incluyendo la revisión de documentos y entrevistas, se concluyó que el phishing es relevante en el contexto del delito de estafa, ya que su objetivo principal es obtener un beneficio económico, sin embargo su creciente prevalencia es la razón principal para clasificarlo como un delito distinto, dado que se utilizan medios tecnológicos diferentes y no se trata simplemente de un delito común. (Montaño, 2019).

Además, esta investigación es relevante porque proporciona conocimientos sobre el papel del estado, ya que el problema no se limita a un delito penal, sino que abarca diversas áreas, como la protección y seguridad de la población, la efectividad en la aplicación de convenios internacionales y la salvaguarda de los derechos de defensa de las personas, que son objetivos fundamentales del estado y la sociedad, en este sentido, el trabajo busca generar un impacto en la prevención y, como resultado, aumentar la confianza en la sociedad. (Avalos, 2021).

La justificación teórica de esta investigación se basa en la aplicación de la teoría y la información necesaria para evaluar la efectividad del rol del estado en la persecución de delitos informáticos, para llevar a cabo este estudio, es crucial contar con una estructura metodológica adecuada y saber aplicar los distintos tipos de investigación, así como las técnicas correspondientes, en este caso, la investigación es cuantitativa, ya que implica un análisis detallado a través de un cuestionario, además de análisis e interpretaciones de

documentos, la importancia de seguir esta metodología radica en dirigir la investigación según normas y métodos que son esenciales para obtener resultados válidos, respetando al mismo tiempo criterios éticos y científicos. (Bruna, 2022).

Los delitos informáticos implican la realización de actividades delictivas a través de plataformas en línea, aunque el acceso a Internet es reconocido como un derecho constitucional, muchas personas lo utilizan de forma ilegal para obtener beneficios económicos, en 2013, se promulgó la Ley N°30096, conocida como la Ley de Delitos Informáticos, cuyo objetivo es combatir eficazmente los delitos cibernéticos, el desarrollo tecnológico y la modernización han llevado a la digitalización de la información personal, lo que permite ofrecer una amplia variedad de servicios y realizar operaciones a través de Internet. (Villavicencio, 2014).

En la actualidad, los delitos informáticos son considerados entre los más difíciles de investigar y resolver, lo que reduce las posibilidades de identificar a los responsables, su rápido crecimiento a nivel mundial ha llevado a que se desarrollen estrategias más sofisticadas para cometer estos delitos, brindando mayor protección y anonimato a los delincuentes.

El Consejo Europeo estableció hace años un tratado internacional conocido como el Convenio de Budapest, cuyo propósito es prevenir y mejorar los instrumentos de investigación, así como facilitar la cooperación internacional y la penalización de los delitos informáticos, pero no todos los países han logrado desarrollar legislaciones penales efectivas puesto que persisten vacíos legales y resulta crucial que todas las naciones se adhieran a este convenio, ya que permite a jueces y fiscales de un país solicitar asistencia a otros estados de manera rápida y efectiva. (Ministerio Público, 2020).

En el Estado de México faltan herramientas tecnológicas adecuadas para investigar en el contexto actual de Internet, sin embargo, el estado posee la responsabilidad de prevenir, investigar, sancionar y reparar las violaciones a los derechos humanos, conforme

a su legislación. (Tellez, 2022).

En Perú, las investigaciones de delitos informáticos exitosas son escasas, a pesar de que se ha creado una ley específica para abordar estos delitos, la ausencia de herramientas adecuadas resulta en un bajo índice de resolución de casos. No basta con crear una ley asimismo es esencial que tenga efectos reales, lo que implica que el estado debe involucrarse en la seguridad ciudadana en relación con Internet en 2022, Perú ocupó el quinto lugar en la incidencia de delitos informáticos, con 15 millones de intentos delictivos. (Fortinet, 2023).

El estado peruano debe responder con mayor eficacia a los delitos cibernéticos, ya que representan grandes riesgos y desafíos para la seguridad pública y la defensa nacional, además de afectar los derechos de quienes no están familiarizados con el manejo seguro de Internet, resulta también que el tratamiento de los delitos informáticos debe ser una prioridad en las políticas públicas, dado que el derecho a la seguridad ciudadana requiere acciones efectivas por parte del estado. (Defensoría del Pueblo, 2023).

Asimismo, el estado juega un papel crucial como mitigador y garantizador de los derechos de la población frente a los delitos informáticos, la carta magna peruana en su artículo 44, menciona los deberes del estado y su compromiso con acuerdos internacionales y normativas nacionales, es vital considerar los aspectos dogmáticos y los derechos fundamentales de la sociedad, como los relacionados con sistemas de información, bases de datos y telecomunicaciones, que deben ser protegidos como bienes jurídicos. Por ello, el estado peruano debe implementar urgentemente garantías legales para prevenir y proteger a la población de los delitos cibernéticos. (Leyva, 2021).

1.2. Formulación del problema

¿Cuál es el papel del estado en la lucha contra los delitos informáticos en Perú?

1.3. Hipótesis

El estado peruano desempeña un papel crucial en la lucha contra los delitos informáticos al implementar legislación específica, promover la capacitación de las fuerzas de seguridad y fomentar la cooperación internacional, lo que resulta en una mejora en la eficacia de la persecución y sanción de estos delitos, sin embargo, la falta de recursos adecuados y la existencia de vacíos legales limitan la efectividad de estas acciones.

1.4. Objetivos

General

Determinar cuál es el papel del estado en la lucha contra los delitos informáticos en Perú

Específico

- Identificar a los organismos internacionales que colaboran con Perú en ciberseguridad
- Describir como se financia la lucha contra el cibercrimen en Perú
- Analizar si existen casos concretos de colaboración público-privada en este ámbito

1.5. Teorías Relacionados

Los autores que respaldan esta teoría son Franz Von y Ernst Von, esta teoría se fundamenta en las ciencias experimentales y busca vincular la teoría delictiva con este enfoque, se considera que el comportamiento humano está relacionado causalmente con los resultados que se generan, así, una conducta se considera típica y antijurídica cuando tanto el comportamiento como la consecuencia están definidos en un artículo del código penal, por ejemplo, si alguien decide matar a otra persona y esto resulta en la muerte, esa acción está contemplada en el código penal, por lo que es considerada típica y contraria a la ley, al causar la muerte, se vulnera el bien protegido por el delito de homicidio, que es la vida de la víctima. (Avalos, 2021).

La teoría de la causalidad entiende el delito como una conexión entre causa y efecto que resulta de una conducta humana, para imputar la responsabilidad a una persona, es suficiente demostrar la existencia de esa causa, en otras palabras, la teoría causalista se centra en la intención detrás de la culpabilidad, en el contexto de los delitos informáticos, el autor tiene la intención de cometer actos ilícitos para obtener beneficios a través de la tecnología, según esta teoría, es fundamental comprobar cómo se realizó la extracción de información personal de otra persona o cómo se introdujo un virus, dependiendo del delito cometido, estas acciones generan efectos que incluyen la violación de derechos de las víctimas y el daño a su patrimonio, según el caso específico. (Barsallo, 2018).

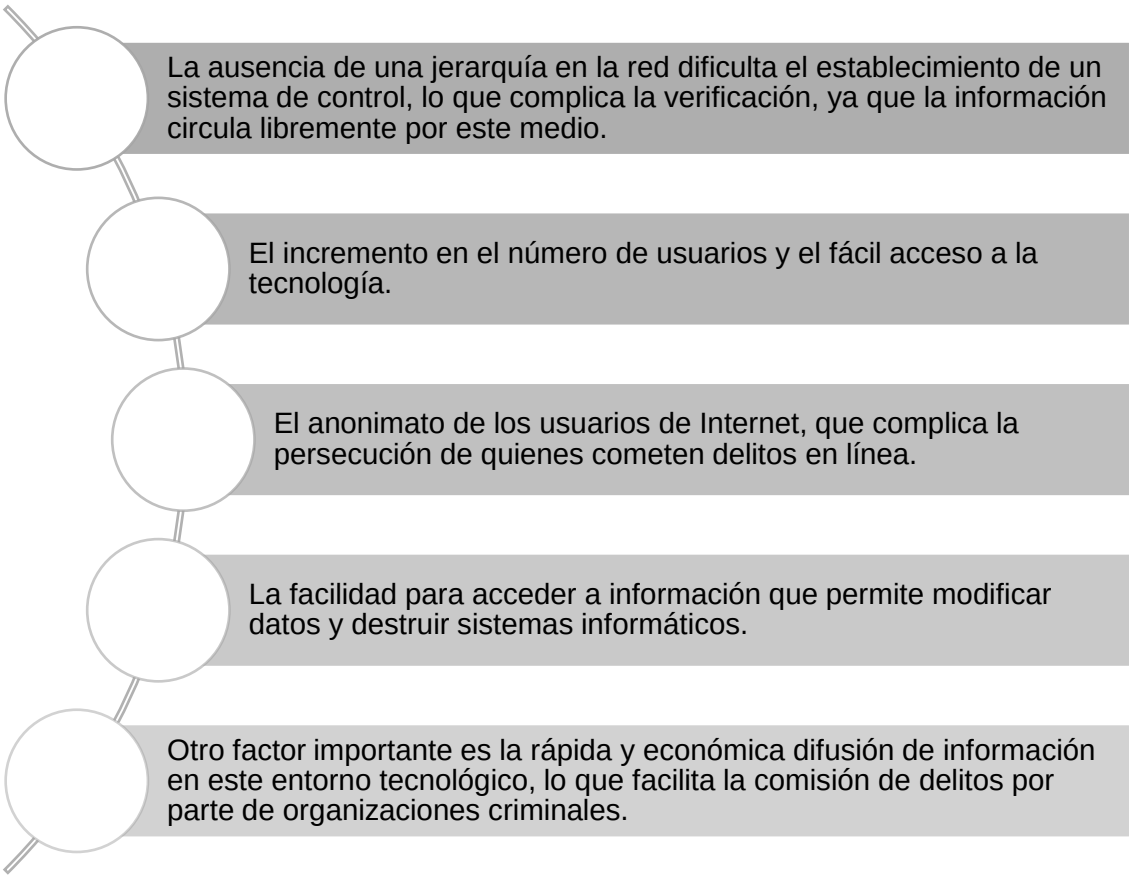
Es un sistema que reduce el poder y potencia el conocimiento judicial, sometiendo la validez de las decisiones a la veracidad y a un control lógico y efectivo de sus fundamentos, el garantismo penal se apoya en la comprensión del comportamiento delictivo, basándose en el estudio de métodos de convencimiento y refutación, en línea con los principios de legalidad y jurisdicción. (Ferrajoli, 1995).

Se fundamenta en una estructura organizada por requisitos específicos de procesos según la epistemología, como el efecto de una pena en relación con el delito, la comisión de un delito y el daño de sus consecuencias, la culpabilidad, así como los principios que rigen al juez y la acusación, y los derechos de prueba y defensa, al vincular esto con el papel del estado en la persecución de delitos informáticos, el garantismo penal otorga prioridad a la constitución y a los derechos fundamentales, incluso por encima de los poderes del estado, lo cual significa que a través de leyes penales y procesales, se asegura que se persiga el delito conforme a la ley, el estado debe cumplir su función de perseguir delitos de acuerdo con lo que establece la Constitución, garantizando así el respeto a los derechos fundamentales y procesales durante el proceso penal. (Avalos, 2021).

En el proceso penal, es importante conocer a los diferentes actores involucrados. En esta etapa, nos referimos al Ministerio Público, la Policía Nacional del Perú, el juez, el imputado, el abogado, la víctima, el agraviado y el actor civil, este procedimiento se desarrolla en varias fases, que se siguen de manera secuencial hasta llegar a su finalización, esencialmente el proceso penal se divide en tres etapas (a) la investigación preparatoria, (b) la fase intermedia y (c) el juicio o audiencia oral. (Carbajal, 2022).

Figura 1

Principales características de la vulnerabilidad en el ámbito informático



Nota: Elaboración propia

Es fundamental destacar que el hecho de que ciertos comportamientos en el ámbito informático sean considerados delitos no implica que se pasen por alto los beneficios y oportunidades que estos sistemas ofrece, los avances tecnológicos que se han incorporado a la sociedad a través de computadoras y tecnología de comunicación son evidentes, pero según el informe del XII Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, estos avances también han dado lugar a nuevas formas de delitos tradicionales, como el fraude y la pornografía infantil, además de crear un entorno propicio para la aparición de nuevos delitos, entre ellos los informáticos, como las intrusiones cibernéticas, el spam, el fraude de datos, la piratería digital, la propagación de virus maliciosos y otros ataques a infraestructuras. (Carriendo, 2022).

Figura 2

Rol del estado peruano

Preventivo

- El Estado garantiza la seguridad de la nación a través del sistema de seguridad y defensa nacional, cuya función es preparar, implementar y dirigir la defensa nacional en todos los ámbitos de la actividad nacional. (Fuentes, 2021).

Sancionador

- "Ius puniendi" es una expresión latina que se refiere a la capacidad del Estado para castigar o sancionar, esta facultad se relaciona específicamente con los órganos encargados de aplicar las leyess, la administración pública tiene la autoridad para imponer sanciones a través de procedimientos administrativos, especialmente en casos de mala gestión por parte de un administrador, con el objetivo de actuar de manera represiva ante comportamientos ilícitos. Las sanciones pueden implicar la privación de derechos o bienes, o la imposición de deberes prohibidos, incluyendo en algunos casos la privación de libertad. (Fuentes, 2022).

Promoción

- El Estado impulsa el desarrollo económico y social fomentando el crecimiento de la producción y la productividad, utilizando los recursos de manera eficiente, garantizando el pleno empleo y asegurando una distribución equitativa de los ingresos. (Fuentes, 2022).

Nota: Elaboración propia.

Esta medida tiene como objetivo verificar si se ha cometido un delito o identificar a los responsables por parte de las autoridades competentes, la persecución del delito comienza cuando los representantes de la fiscalía reciben información sobre un hecho delictivo, una vez que se conoce que las circunstancias están siendo investigadas, el fiscal debe iniciar el procedimiento preparatorio y luego avanzar a la fase preparatoria formal y durante este proceso, se llevarán a cabo diversas actividades de investigación para aclarar los delitos, las cuales pueden ser realizadas por las autoridades fiscales o con el apoyo de la Policía a través de unidades de investigación especializadas. (Garrido, 2020).

Existen factores que dificultan la investigación efectiva de los delitos y el cumplimiento de los objetivos de la fase preparatoria, las procuradurías deben enfocarse en capacitar a los nuevos empleados, sin importar la agencia, para que comprendan bien el sistema tributario y las operaciones de su propia institución, evitando así el desconocimiento que puede obstaculizar el trabajo de inspección tributaria, ese sentido, es importante que el Ministerio Público debe considerar los factores mencionados, así como otros no mencionados, para resolver los casos de manera oportuna y crear las condiciones necesarias para que esta agencia desempeñe sus funciones de manera eficaz. (Gutierrez, 2021).

Con respecto a los delitos informáticos se tiene que

Con el avance de la tecnología informática, ha emergido un nuevo tipo de delito conocido como delito informático, para abordar esta nueva forma de criminalidad, se implementó una ley penal especial destinada a prevenir y sancionar actividades ilegales que impacten los sistemas y datos informáticos, así como la privacidad de las comunicaciones y otros derechos legítimos afectados por estos actos delictivos, incluyendo la protección del patrimonio, la fe pública y la libertad sexual. (Leyva, 2021).

Los delitos informáticos fueron inicialmente definidos en el artículo 186, sección 3, segundo párrafo del Código Penal de 1991, actualmente estos delitos se regulan en el

Capítulo X(13) del Código Penal, que incluye el Artículo 207-A (acceso, interferencia o copia ilegal de contenidos en bases de datos), 207-B (modificación, daño o destrucción de bases de datos), 207-C (circunstancias agravantes) y 207-D (circulación ilegal de datos), además de estar contemplados en leyes penales especiales. (Leyva, 2021).

Entre las leyes penales especiales se encuentra la Ley 30096, conocida como la Ley de Delitos Informáticos la cual se divide en siete capítulos, organizados de la siguiente manera: el primer capítulo aborda el objeto y la finalidad de la ley, el segundo se centra en los delitos contra datos y sistemas informáticos; el tercero trata sobre los delitos informáticos relacionados con la reparación y la libertad sexual, el cuarto se ocupa de los delitos contra la intimidad y las comunicaciones, el quinto aborda los delitos contra la propiedad; el sexto se refiere a los delitos que afectan la fe pública; y el séptimo incluye disposiciones generales. (López, 2021).

Figura 3

Modificaciones a la Ley 30171 en relación con los delitos informáticos

Artículo 1: Se realizan cambios en los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096, que es la Ley de Delitos Informáticos.
Artículo 2: Se modifican las disposiciones complementarias finales tercera, cuarta y undécima de la Ley 30096.
Artículo 3: Se añade un nuevo inciso al artículo 12 de la Ley 30096.
Artículo 4: Se modifican los artículos 158, 162 y 323 del Código Penal.
Artículo 5: Se incorporan los artículos 154-A y 183-B al Código Penal.
Única Disposición Complementaria Derogatoria: Se deroga el artículo 6 de la Ley 30096.

Nota: Elaboración propia

El delito informático se refiere a la comisión de delitos a través de computadoras, Internet y otros medios digitales, sin embargo, estos dispositivos son solo herramientas que facilitan la actividad delictiva, pero no son los únicos factores que la determinan y aunque este término no se usa con frecuencia en el derecho penal aun representa una nueva categoría de delito que ha surgido con la creciente utilización de la tecnología informática.

Desde la perspectiva del concepto de delito informático, no todos los crímenes pueden clasificarse como tales solo porque involucren el uso de computadoras u otros medios tecnológicos, resulta importante definir qué conductas se consideran delitos informáticos y cuáles a pesar de utilizar sistemas informáticos, no lo son, un criterio relevante es que un delito sea considerado informático solo si no podría cometerse sin la tecnología de la información es decir, debe desarrollarse en un entorno digital, por ejemplo, difamar a alguien a través de correo electrónico, Facebook o Twitter no se clasifica necesariamente como un delito informático, ya que esta acción también puede realizarse de manera verbal o escrita sin tecnología, en cambio, delitos como el acceso no autorizado a sistemas o la destrucción de bases de datos sí son considerados delitos informáticos, ya que requieren la intervención de la tecnología para llevarse a cabo. (Morant, 2019).

En el ámbito de los delitos informáticos, Krutish identifica tres categorías: manipulación informática, sabotaje informático y acceso no autorizado a datos o sistemas, sin embargo, estas categorías se refieren más a las formas de llevar a cabo delitos informáticos que a tipos de delitos en sí.

Muehlen sostiene que cualquier acto delictivo que utilice una computadora como herramienta o como objetivo debe incluirse en la definición de delito informático, por su parte, Dannecker considera que el delito informático está directamente o indirectamente relacionado con el procesamiento electrónico de datos y se comete en presencia de equipos de computación. (Torres, 2019)

Según Davara, un delito informático se define como cualquier acción que cumpla con las características esenciales de un delito, que se lleva a cabo utilizando elementos informáticos y telemáticos, o que vulnere los derechos del propietario de esos elementos, ya sean hardware o software. (Morant, 2019).

Julio Téllez Valdez clasifica el delito informático en dos tipos: típico y atípico, el primero se describe como una conducta típica, ilícita y culposa en la que se utilizan computadoras como herramienta o como objetivo, mientras que el segundo se refiere a una relación ilícita en la que las computadoras actúan como herramienta o como fin.

Se prohíben los actos de corrupción con el objetivo de garantizar el correcto y regular funcionamiento del gobierno, sin embargo, la definición del beneficio jurídico que se protege en los casos de tráfico de influencias sigue siendo un tema controvertido en la doctrina y la jurisprudencia penal, esto se debe a que está influenciado por diferentes teorías, entre las que se incluye la teoría del gobierno institucional. (Montoya, 2018).

De acuerdo con esta teoría, la institucionalidad se entiende como un conjunto de valores, principios y responsabilidades que guían el trabajo de los funcionarios en la administración pública, por lo tanto, es fundamental proteger la institucionalidad de conductas que, aunque no la violen de manera directa, fomenten la corrupción y presenten a la administración pública como una entidad débil y susceptible a intereses privados ilegales. (Guimaray, 2020).

Por lo tanto, recurrir a influencias, ya sean reales o imaginarias, para que otros crean que puede haber interferencias en el funcionamiento adecuado de la administración pública es una violación de la institucionalidad, es así que el delito de tráfico de influencias tiene como objetivo prevenir que la administración pública sea vista como controlada o vulnerable, y que la influencia percibida exceda su capacidad para investigar y hacer justicia. (Torres, 2019).

La vía penal permite que un comportamiento sea tanto consciente como ilegal, lo que incluye la ruptura y los obstáculos relacionados con datos informáticos y las emisiones electromagnéticas que transmiten esos datos a programas privados.

Este artículo menciona tres circunstancias que agravan las penas:

- La primera se aplica cuando el interceptor accede a información clasificada como secreta o reservada, conforme a la Ley 27806 sobre transparencia y acceso a la información, lo que conlleva una multa de entre cinco y ocho años.
- La segunda se refiere a la interceptación de información relacionada con la defensa nacional, la seguridad o la soberanía, cuya pena oscila entre ocho y diez años.
- La tercera circunstancia agravante se relaciona con la identidad del autor, es decir, si es miembro de una organización criminal, lo que incrementa la pena en un tercio de la máxima establecida en los casos anteriores.

Este tipo de delito, relacionado con la interceptación de datos informáticos, se considera de alta peligrosidad en términos abstractos, por lo tanto, basta con demostrar que se ha producido la interceptación para que el delito sea reconocido, se trata de un delito simple, ya que la mera acción de interceptar datos informáticos es suficiente para que se considere un delito, por ejemplo, esto incluye bloquear archivos con información relevante para una investigación que está legalmente restringida o interrumpir comunicaciones que contengan información secreta que un país podría usar en un contexto bélico. (Mori, 2019).

El sujeto activo según el profesor chileno Garrido (2020) la persona en cuestión es aquella que lleva a cabo total o parcialmente las acciones descritas en el tipo penal, lo que nos lleva a concluir que es la persona que cometió el delito.

En Perú, debido a la invalidación del principio del delito social, las personas jurídicas no pueden ser consideradas como entidades activas, sin embargo, el derecho penal

peruano incluye disposiciones sobre consecuencias adicionales (artículo 105 del Código Penal), así como otras normas (artículo 27 del Código Penal) y procedimientos del Código Procesal Penal, en el incidente de 2004, se trató de delitos cometidos a través de la ley. Además, el Acuerdo Integral 7-2009/CJ-116 aborda a las personas jurídicas y sus efectos colaterales. (López, 2021).

La Ley de Delitos Informáticos, por su parte, establece dos situaciones administrativas: una es cuando una persona jurídica se niega a proporcionar información sobre la revelación de secretos bancarios (disposición adicional décima final), y la otra es cuando se niega a facilitar información sobre grabaciones de conversaciones telefónicas (disposición adicional undécima) a solicitud del tribunal, en estos casos, la SBS y Osiptel impondrán las sanciones administrativas correspondientes en forma de multas. (Mori, 2019).

Con respecto al sujeto pasivo se refiere a la persona que es propietaria del bien jurídico protegido por la ley y sobre la cual se ejerce la acción del sujeto activo, en términos simples, es la persona física o jurídica que sufre el delito.

Las personas jurídicas, al igual que las empresas públicas y privadas (como bancos, agencias gubernamentales, industrias y compañías de seguros), pueden ser consideradas sujetos pasivos, sn embargo, en algunos casos, estas entidades no denuncian los delitos de los que son víctimas por temor a perjudicar o influir negativamente en sus clientes, lo que podría llevar a pérdidas económicas. (Peralta, 2022).

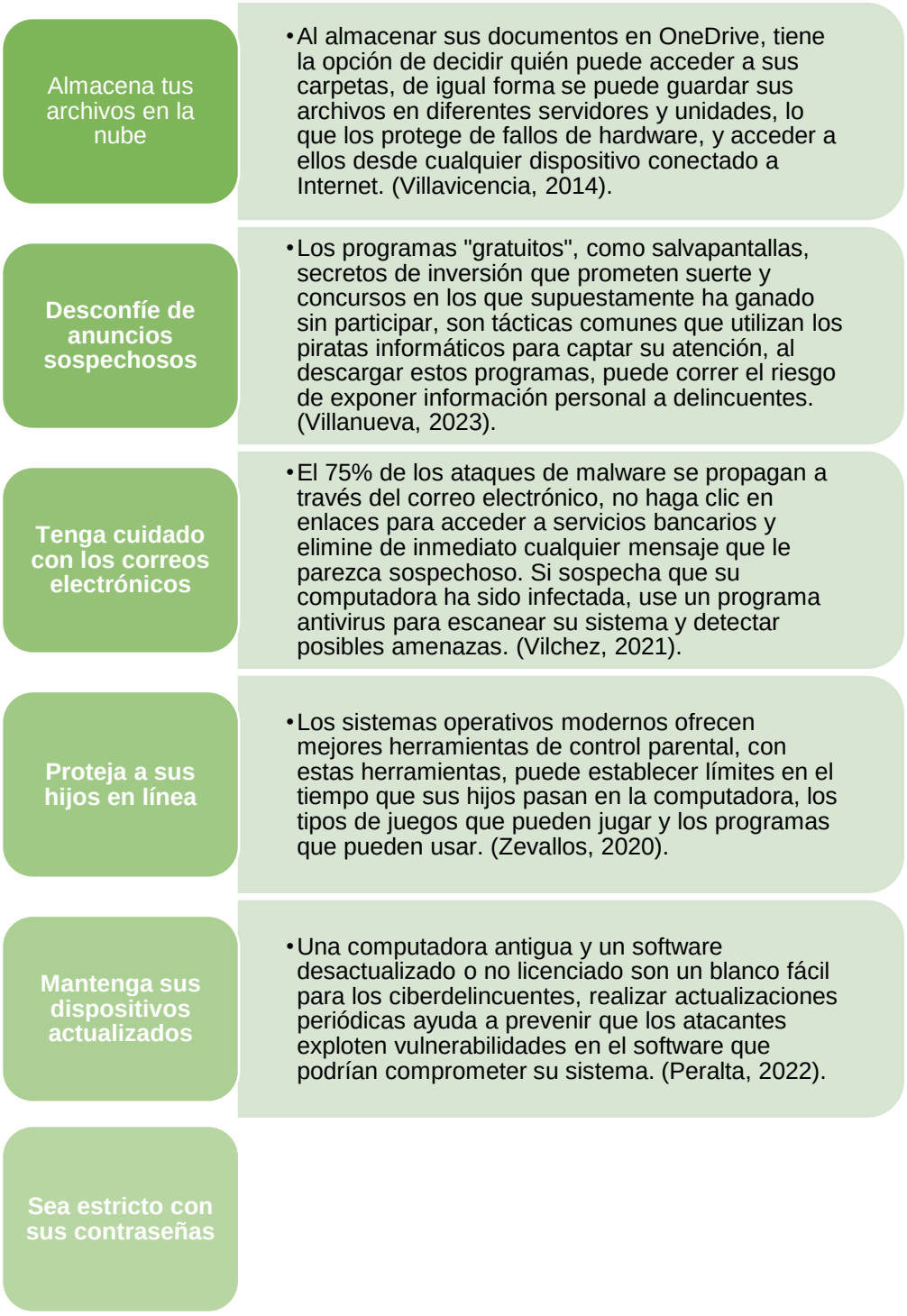
Además, la ley identifica dos situaciones en las que las personas jurídicas son sujetos pasivos de delitos informáticos: (i) el artículo 6, que trata sobre el tráfico de datos, incluyendo la creación, introducción o uso indebido de bases de datos de personas físicas o jurídicas, y (ii) el artículo 9, que se refiere al robo de identidad, donde se utilizan tecnologías informáticas para suplantar a una persona física o jurídica, las personas jurídicas son los principales sujetos pasivos en delitos informáticos debido a su capacidad

económica, lo que las convierte en los sectores más afectados, como bancos, agencias gubernamentales e industrias procesadoras. (Peralta, 2022).

La Ley de Delitos Informáticos tiene como objetivo prevenir y penalizar las actividades ilegales que impactan los sistemas y datos informáticos, la privacidad de las comunicaciones, la propiedad, la opinión pública y la libertad sexual, todo ello relacionado con el uso de las tecnologías de la información y la comunicación (TIC). (Vilchez, 2021).

Figura 4

Medidas a implementar para asegurar los datos y evitar ciberdelitos



Nota: Elaboración propia

La División de Investigación de Alta Tecnología es una unidad especializada con habilidades técnicas y profesionales que forma parte de la Dirección General de Investigaciones Criminales de la Policía Nacional del Perú, su función es prevenir, controlar, investigar y reportar delitos informáticos bajo la supervisión legal del fiscal, también se encarga de investigar delitos cometidos con tecnologías de la información y las comunicaciones, tanto por delincuentes comunes como por organizaciones criminales en todo el país, asimismo resulta responsable de llevar a cabo actividades de geolocalización dentro de su jurisdicción. (Tellez, 2019).

Se encargan de:

1. Llevar a cabo la localización o geolocalización de dispositivos móviles en casos de desapariciones de personas.
2. Mantener una comunicación constante con las unidades policiales que participan en la investigación y búsqueda de personas desaparecidas.
3. La resolución PGN N° 3743/15 dio origen a la creación de la Unidad Fiscal Especializada en delitos cibernéticos, con el propósito de mejorar la efectividad en la detección, persecución y captura de delitos relacionados con el crimen organizado en el ámbito digital, que afectan la seguridad de los ciudadanos. Esta unidad fiscal tiene la autoridad para iniciar investigaciones sobre delitos que amenacen los sistemas informáticos, prestando especial atención a los casos de crimen organizado.
4. Con la formación de esta unidad, se busca diferenciar la fiscalía para ofrecer respuestas rápidas y efectivas a los delitos cometidos en línea, un desafío actual para la justicia peruana, dado el uso frecuente de tecnologías que manejan información valiosa. Sin embargo, a pesar de esto, aún no hay una cultura sólida de prevención y protección de la información personal, se espera que los peritos también reciban capacitación adecuada en este ámbito.

Para establecer la UFECI, Perú se basó en modelos analizados a través del derecho comparado, priorizando la coordinación a nivel nacional para ofrecer asistencia técnica y capacitación a fiscales, esta unidad organiza a las diferentes fiscalías que manejan casos de delitos informáticos y estafas agravadas, esta última definida en el inciso 5 del artículo 196-A del Código Penal, de igual forma la UFECI cuenta con el apoyo de la Unidad de Cooperación Judicial Internacional y Extradiciones de la Fiscalía en los procesos relacionados con delitos informáticos. (MP, 2020).

La OFAEC (2021) señaló que la UFECI lidera las investigaciones especializadas y tiene competencia en todo el territorio peruano, aunque está sujeta a la fiscalía de la nación en términos administrativos y funcionales.

Por su parte, el CONASEC – Consejo Nacional de Seguridad Nacional (2021) mencionó que uno de los factores que llevó a la fiscalía a poner más atención en los delitos cibernéticos fue el aumento en el porcentaje de estafas en línea durante la pandemia de COVID-19.

Por lo tanto, la fiscalía especializada fue establecida en respuesta al incremento de delitos informáticos, respaldada por un informe que presenta las recomendaciones de la Comisión encargada de analizar técnicamente la creación de una fiscalía especializada piloto, esta comisión recibió apoyo del programa de asistencia contra el crimen transnacional organizado de la Unión Europea, así como de la embajada de EEUU en Perú.

La UNICEF cuenta con 68 fiscales especializados, incluyendo un fiscal titular y un alterno, que actúan como contratados entre la unidad fiscal especializada y su respectivo distrito fiscal. Los fiscales son designados mediante resoluciones.

Las funciones específicas de la unidad son:

- Gestionar los casos que le corresponden y apoyar a otros fiscales.
- Recibir denuncias y llevar a cabo las investigaciones necesarias.

- Servir de enlace con organismos nacionales e internacionales en temas de delitos cibernéticos, incluyendo lo estipulado en el convenio de Budapest en el marco de la red 24/7.
- Colaborar con procuradurías y otras entidades fiscales para desarrollar estrategias efectivas para prevenir delitos cibernéticos.
- Capacitar a otros fiscales en el uso de herramientas técnicas, laboratorios, métodos de investigación, así como en la elaboración, análisis y conservación de pruebas disponibles en el país.
- Analizar las modificaciones en reglamentos y leyes pertinentes.
- Realizar estudios y diagnósticos sobre el crimen organizado en el ámbito de la ciberdelincuencia.
- Llevar a cabo actividades de asistencia, promoción y capacitación en temas de cibercrimen.
- Brindar apoyo técnico a los fiscales en las investigaciones de delitos informáticos.
- Implementar y supervisar un programa virtual de la Fiscalía relacionado con estos temas.

No obstante, una de las principales dificultades para avanzar en las investigaciones de las denuncias es la lentitud o falta de respuesta por parte de los bancos y las empresas de telecomunicaciones ante las solicitudes judiciales, además, algunas de estas entidades no cumplen con lo establecido en la segunda disposición complementaria del DL N°1182, que se refiere al uso de datos de telecomunicaciones para identificar, localizar y geolocalizar equipos, esta información es esencial para combatir la delincuencia y el crimen organizado, resulta crucial que estas empresas mantengan los datos por un mínimo de un año en sus sistemas y que respondan de manera ágil a los operadores de justicia. (Fuentes, 2021).

Como parte de las estrategias de la fiscalía especializada, se ha establecido una alianza con el programa global sobre ciberdelincuencia de la UNODC para ofrecer cursos básicos y técnicos a todos los miembros de la fiscalía especializada, así como a los fiscales de la red en Lima Centro de igual forma se han desarrollado 14 módulos de aprendizaje que abordan métodos de investigación de delitos cibernéticos, estudios forenses digitales y la cooperación judicial internacional, entre otros temas. (Gutierrez, 2021).

La fiscalía también inauguró el primer laboratorio de delitos informáticos para apoyar las investigaciones y la identificación de los delincuentes, este laboratorio está equipado con tecnología de última generación, gracias al apoyo de la UNODC y del gobierno de Noruega. (Galdamez, 2019).

Según la Defensoría del Pueblo (2023), los ciberdelincuentes emplean diversas herramientas para ocultar su identidad, por tal razón, la red de fiscales puede acceder al programa mencionado de forma anónima, lo que les permite evitar los riesgos asociados con códigos maliciosos, esto les ayuda a obtener valores hash y recopilar pruebas digitales, protegiendo así su integridad y la de la red institucional.

Por otro lado, en 2020 se estableció la UFECI, y en mayo del año siguiente, la jefa de esta dependencia mencionó que sería beneficioso contar con una fiscalía corporativa especializada en delitos informáticos, en el contexto de la implementación del CPP en el distrito fiscal de la capital, esto se proponía para ofrecer un enfoque estratégico en esa área, pero debido a la falta de financiamiento, la Secretaría Técnica de Implementación del CPP sugirió convertir la tercera fiscalía corporativa penal de Santiago de Surco - Barranco en una entidad especializada en delitos informáticos. (DP, 2023).

Según Avalo (2021), a pesar de las dificultades, se estableció la Fiscalía Corporativa Penal especializada en el distrito fiscal de Lima Centro a mediados de 2021, esta fiscalía está formada por una fiscalía superior especializada y cuatro ministerios públicos provinciales penales corporativos, todos ellos con jurisdicción en Lima para abordar los

delitos informáticos.

A pesar de los obstáculos, se creó la Fiscalía Corporativa Penal especializada en el distrito fiscal de Lima Centro a mediados de 2021, esta institución incluye una fiscalía superior especializada y cuatro ministerios públicos provinciales penales corporativos, los cuales tienen jurisdicción en Lima para tratar los delitos informáticos. (Avalo, 2021).

El desarrollo normativo surge como respuesta al aumento de los delitos cibernéticos en nuestro país, lo que ha llevado a una evolución en las sanciones establecidas por la ley, el primer artículo de esta ley señala que su objetivo es prevenir y sancionar conductas delictivas que afectan los sistemas, la información, el secreto de las comunicaciones, la libertad sexual y los bienes, entre otros aspectos que son vulnerados a través del uso de la tecnología, se busca garantizar condiciones mínimas para que la sociedad pueda ejercer su derecho a la libertad y al desarrollo, la ley de delitos cibernéticos tiene como meta combatir eficazmente los delitos informáticos, alineándose con el convenio de Budapest, sin embargo, también presenta vacíos y falta de herramientas que podrían limitar su efectividad. (Carbajal, 2022).

La actual ley de delitos de ciberdelincuencia regula diversos delitos, como el acceso no autorizado (art. 2), la vulneración de la integridad de la información en la web (art. 3), la afectación de sistemas informáticos (art. 4), las propuestas sexuales a menores a través de internet (art. 5), la apropiación de información (art. 7), el fraude informático (art. 8) y el robo de identidad (art. 9). (Diaz, 2019).

Además, la ley incluye disposiciones sobre los actos previos a las conductas de los infractores, por ejemplo, en el artículo 10 se aborda el abuso de mecanismos y conectores informáticos, y el artículo 11 establece penas severas para casos con agravantes, como el involucramiento de organizaciones criminales, el abuso de funciones para acceder a información confidencial, la búsqueda de beneficios económicos ilícitos y situaciones que comprometan la asistencia y la soberanía del país.

Asimismo, el artículo 12 establece una excepción a la responsabilidad penal, que se aplica cuando una persona lleva a cabo las actividades mencionadas en los artículos 2, 3, 4 y 10 con el propósito de obtener pruebas autorizadas y realizar acciones destinadas a proteger los sistemas informáticos.

La ley de delitos informáticos fue elaborada conforme a las disposiciones del convenio de Budapest, que se firmó en 2001 y entró en vigor en 2004 para los países que se adhirieron, con el objetivo de establecer instrumentos que unifiquen las normas del derecho penal y faciliten la cooperación internacional, sin embargo, el poder legislativo de Perú aprobó el convenio en 2019, y un mes después, el poder ejecutivo lo ratificó mediante un decreto supremo, resulta importante destacar que desde 2013 ya existía una ley que prevenía y sancionaba los delitos informáticos, por lo que la implementación del convenio de Budapest podría haber sido muy útil para sensibilizar y educar a los responsables del sistema de justicia sobre la era digital. (Zevallos, 2020).

El convenio de Budapest es un acuerdo establecido en 2001 entre varios países, que regula los delitos digitales, este tratado, promovido por el Consejo de Europa, busca fortalecer la cooperación internacional y establecer normas coherentes entre las naciones para combatir los delitos informáticos y las actividades en el entorno digital.

Es cierto que era necesario un convenio internacional que aborde los delitos informáticos, ya que estos comportamientos ilegales no requieren la presencia física de los infractores; basta con saber utilizar internet y actuar de manera anónima para cometer delitos, por ejemplo, alguien en México puede modificar o robar información de una persona en Perú, con el convenio de Budapest, los países pueden establecer normas que faciliten la cooperación internacional en este ámbito.

Según Bruna Martins (2022), la adhesión del Estado peruano al Convenio de Budapest permite que las solicitudes de los profesionales legales a nivel nacional se envíen rápidamente a los otros países miembros del convenio.

Un aspecto relevante que destaca el tratado en el artículo 35 es la creación de la Red 24/7, que proporciona apoyo inmediato para investigar delitos digitales relacionados con internet y datos informáticos lo cual permite a los países miembros solicitar la conservación de información, así como la obtención de pruebas y la localización de posibles ciberdelincuentes.

Una de las principales metas del convenio de Budapest es fomentar la cooperación internacional, en sus artículos 23, 24, 25 y 28, se aborda la extradición y la asistencia mutua que deben proporcionar los países miembros para perseguir los delitos informáticos, dado que estos delitos suelen tener un carácter transfronterizo, es crucial que los estados colaboren para identificar a los ciberdelincuentes.

Es importante señalar el artículo 35, ya que ofrece una explicación clara de los compromisos asumidos para lograr una cooperación internacional efectiva, este artículo exige que los países miembros tengan un punto de contacto disponible las 24 horas del día, los 7 días de la semana, para facilitar la obtención rápida de pruebas electrónicas relacionadas con delitos, para cumplir con este requisito, deben contar con personal capacitado y adecuadamente equipado. (Molina, 2021).

El artículo 35 se refiere a la red 24/7 y establece que cada país debe tener un medio de contacto disponible en todo momento, todos los días, esto tiene como objetivo asegurar un apoyo rápido en las investigaciones de delitos informáticos y en la obtención de pruebas digitales, estos medios pueden incluir asistencia técnica, mantenimiento de datos, recolección de pruebas, intercambio de información legal y localización de posibles autores de delitos. (Molina, 2021).

Por lo tanto, la comunicación entre un estado y otros estados se realizará a través de un procedimiento ágil, si el punto de contacto designado por una parte no está bajo la autoridad de las instituciones responsables de la asistencia mutua internacional o extradición, se asegurará que pueda colaborar de manera coordinada con ellas mediante

un proceso rápido, cada parte se compromete a contar con personal adecuadamente capacitado y con los recursos necesarios para garantizar el buen funcionamiento de la red.

II. MATERIALES Y METODOS

La investigación cualitativa inicia con la identificación de un problema de investigación claro y específico, se centra en aspectos externos particulares del tema en cuestión y se elabora un marco teórico basado en una revisión de la literatura existente. (Hernández, 2010).

El enfoque cualitativo del estudio se manifiesta en la realización simultánea del análisis y la recolección de datos, ya que ambas actividades son cruciales para identificar los indicadores de la variable, y se llevan a cabo al mismo tiempo.

El tipo de investigación es exploratorio, lo que sucede cuando se examinan contextos que han sido poco analizados. Además, se da cuando la revisión de la literatura revela pocos estudios sobre el tema, con el objetivo de encontrar nuevas perspectivas. (Hernández, 2010).

En cuanto al tema de estudio, no se puede afirmar que se haya explorado por completo el conocimiento sobre la descripción de los procedimientos legales y aunque existen antecedentes relacionados con la variable que se analiza en este trabajo, este estudio adopta un enfoque hermenéutico. (Hernández, 2010).

a investigación tuvo un carácter descriptivo, ya que se centró en detallar los atributos o características del tema en cuestión, de igual forma la recolección de datos sobre la variable y sus elementos se realizó tanto de manera individual como simultánea, antes de pasar al análisis. (Hernández, 2010).

Al respecto, Mejía (2004) Se señala que en las investigaciones descriptivas se examina con detenimiento el fenómeno, utilizando de manera constante y exhaustiva las bases teóricas para identificar sus características y definir su perfil, lo que permite determinar la variable, en este estudio específico, la naturaleza descriptiva se manifiesta en varias etapas: 1) en la selección de la unidad de análisis, 2) en la recolección y análisis de datos, donde se hace un uso intensivo de las teorías, y 3) en las acciones que se dirigen

según los objetivos específicos establecidos..

El diseño de la investigación fue no experimental, lo que significa que el fenómeno se observó en su entorno natural, así los datos reflejan el desarrollo natural de los eventos, sin la intervención del investigador. (Hernández, Fernández & Batista, 2010).

III. RESULTADOS

OG.

Figura 5

El papel del Estado en la lucha contra los delitos informáticos en Perú

Legislación

- Marco Legal: Perú ha desarrollado leyes específicas para abordar los delitos informáticos, como la Ley N° 30096, que sanciona el acceso ilícito a sistemas informáticos.
- Actualización Normativa: La legislación debe adaptarse constantemente a las nuevas formas de delitos cibernéticos, como el phishing y el ransomware.

Instituciones Competentes

- Policía Nacional del Perú (PNP): A través de la División de Delitos de Alta Tecnología, se encarga de investigar y prevenir delitos informáticos.
- Ministerio Público: Tiene la responsabilidad de perseguir penalmente a los infractores y coordinar con otras instituciones para la prosecución de estos delitos.

Prevención y Educación

- Campañas de Concientización: El Estado realiza campañas para educar a la población sobre los riesgos de los delitos informáticos y cómo prevenirlos.
- Formación de Recursos Humanos: Capacitación a funcionarios y personal de seguridad sobre tecnologías y delitos cibernéticos.

Cooperación Internacional

- Alianzas Estratégicas: Perú colabora con organismos internacionales como INTERPOL y la Organización de Estados Americanos (OEA) para mejorar su capacidad de respuesta a delitos transnacionales.
- Intercambio de Información: Participación en redes internacionales para compartir información sobre ciberamenazas y mejores prácticas.

Tecnología y Recursos

- Infraestructura Tecnológica: Inversión en tecnología para mejorar la capacidad de investigación y respuesta ante incidentes cibernéticos.
- Centros de Respuesta a Incidentes de Seguridad Informática (CSIRT): Creación de entidades dedicadas a gestionar y responder a incidentes de seguridad.

Nota: Elaboración propia

OE1

Figura 6

Perú colabora con varios organismos internacionales en el ámbito de la ciberseguridad.

INTERPOL

- Proporciona apoyo en la investigación de delitos informáticos y facilita la cooperación entre fuerzas policiales de diferentes países.

OEA (Organización de Estados Americanos)

- A través de su Ciberseguridad Cybersecurity Program, ofrece capacitación y asistencia técnica a los Estados miembros, incluyendo Perú.

EUROPOL

- Colabora en el intercambio de información y mejores prácticas en la lucha contra el cibercrimen a nivel europeo y global.

UNODC (Oficina de las Naciones Unidas contra la Droga y el Delito)

- Brinda asistencia técnica y programas de capacitación para mejorar las capacidades de los países en el combate al cibercrimen.

APEC (Cooperación Económica Asia-Pacífico)

- Promueve la cooperación en ciberseguridad entre economías de la región, facilitando el intercambio de información y recursos.

ISO (Organización Internacional de Normalización)

- Aunque no es un organismo de seguridad, establece normas internacionales que ayudan a los países a mejorar sus prácticas de ciberseguridad.

FIRST (Forum of Incident Response and Security Teams)

- Ofrece un foro para la colaboración y el intercambio de información sobre incidentes de seguridad cibernética.

GCCS (Global Conference on Cyber Space)

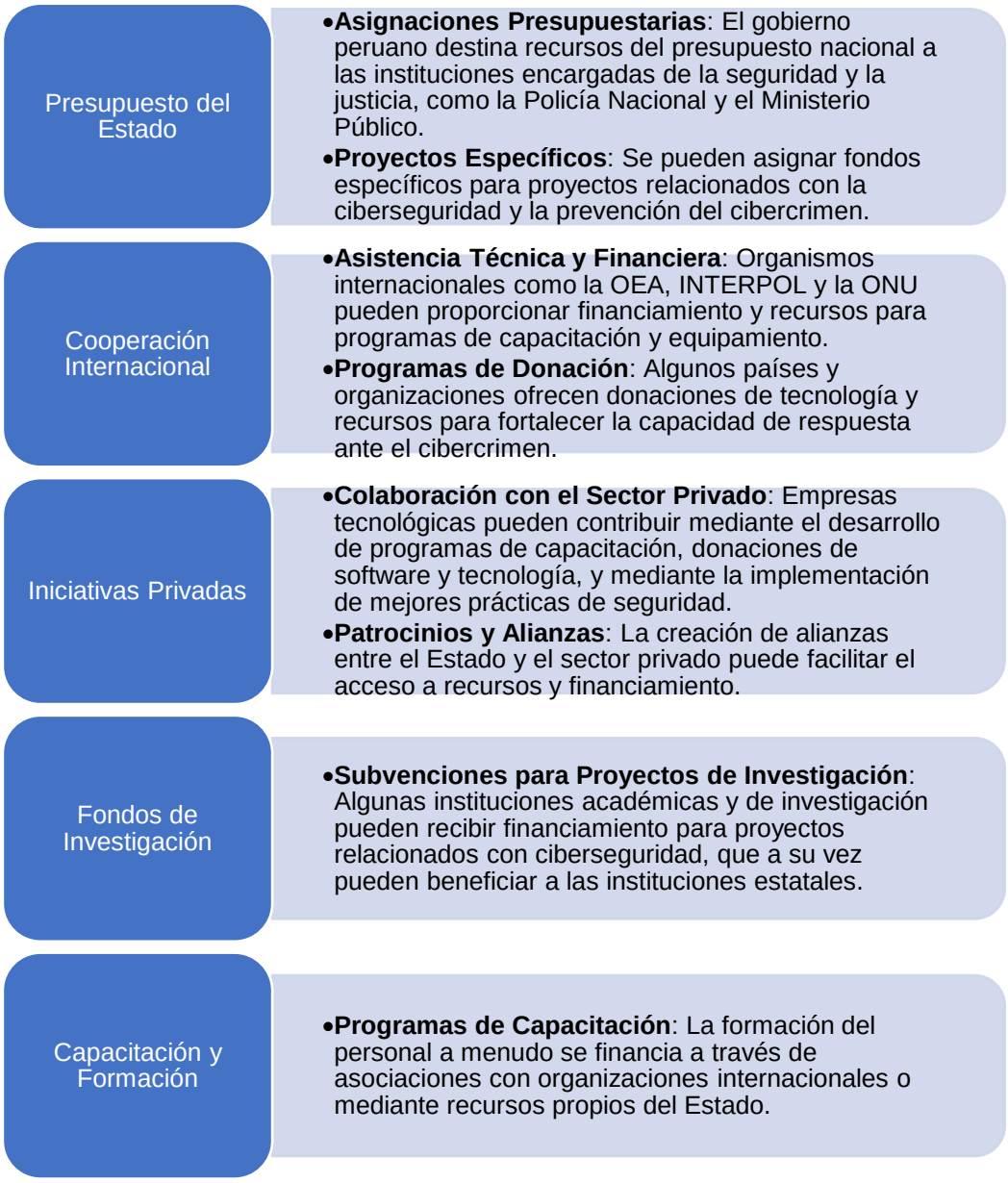
- Reúne a gobiernos, empresas y organizaciones para discutir y promover la ciberseguridad a nivel global.

Nota: Elaboración propia

OE2

Figura 7

La lucha contra el cibercrimen en Perú se financia a través de diversas fuentes y mecanismos

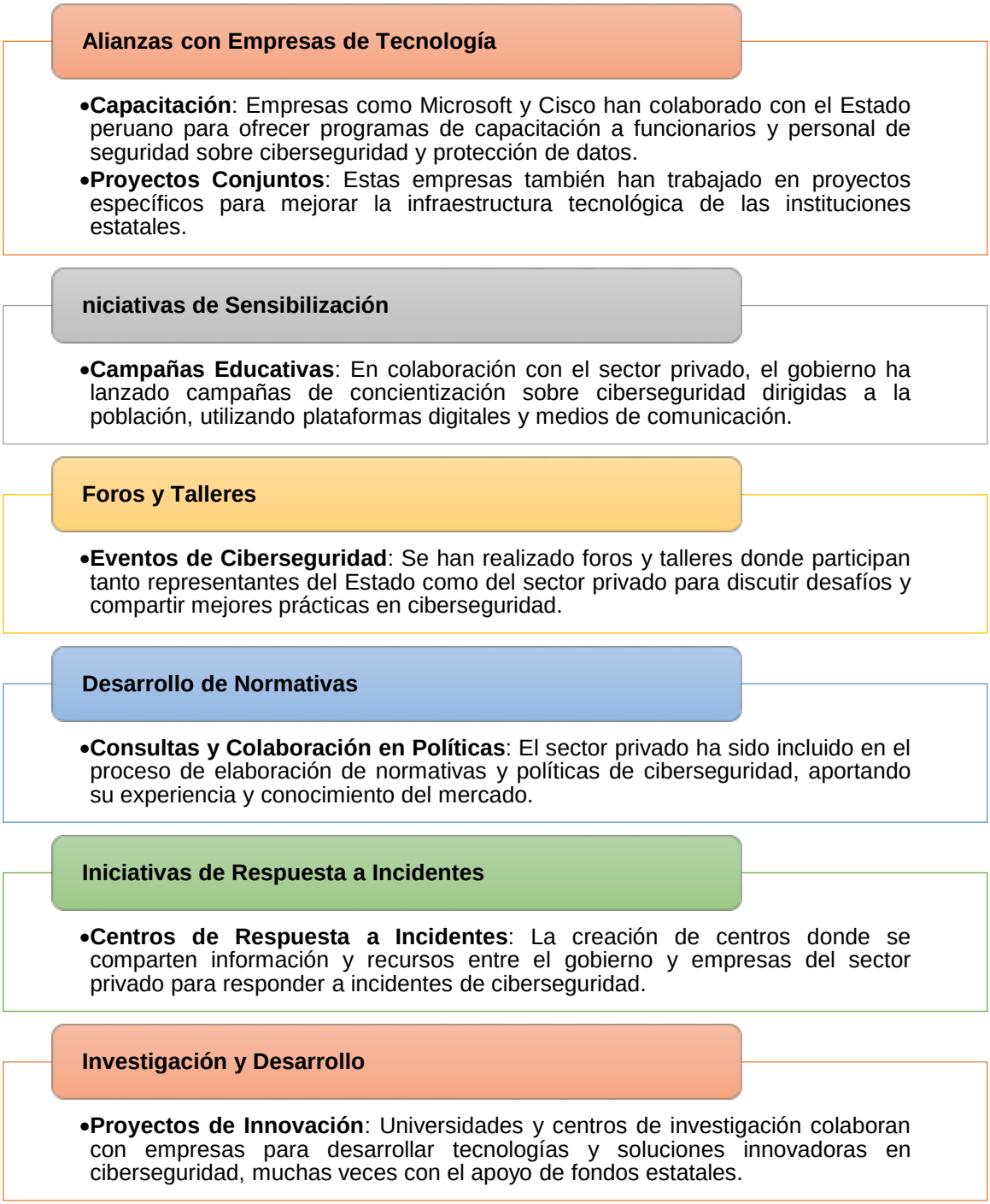


Nota: Elaboración propia

OE3

Figura 8

Colaboración público-privada en la lucha contra el cibercrimen en Perú.



Nota: Elaboración propia

IV. DISCUSION Y CONCLUSIONES

Discusión

La ciberdelincuencia es un problema global que no solo afecta datos personales, propiedad y otros bienes jurídicos, sino que también puede poner en grave peligro la integridad e incluso la vida de sus víctimas, como niños y adolescentes, el avance de la tecnología en la vida diaria se ha reflejado en el aumento de delitos cibernéticos en los últimos años, especialmente durante la fase más crítica de la pandemia de Covid-19, cuando las restricciones impuestas por gobiernos de todo el mundo contribuyeron a este incremento, varias organizaciones internacionales, como las Naciones Unidas y el Banco Interamericano de Desarrollo, han realizado diagnósticos sobre la ciberdelincuencia a nivel mundial, incluyendo a Perú en sus estudios y destacando los problemas y brechas que aún deben abordarse, especialmente en lo que respecta a la atención a recursos y colaboración entre los distintos actores involucrados. (CNPC, 2020).

La Policía Nacional ha reportado un notable aumento en las denuncias por ciberdelitos, conforme a lo establecido en la Ley de Delitos Informáticos, en los últimos cinco años, de hecho, las denuncias se cuadruplicaron entre 2018 y 2021, pasando de 3,031 a 12,827, si observamos la tasa de ciberdelitos por cada 100,000 habitantes, esta aumentó del 10% al 39%. (MINJUS, 2021).

En cuanto a los tipos de ciberdelitos denunciados a la Policía Nacional, el fraude informático fue el más común en 2021, representando el 72% de los casos, seguido por la suplantación de identidad, que alcanzó el 20% Juntos, estos dos tipos de delitos abarcaron nueve de cada diez denuncias, la forma más frecuente de fraude informático involucra operaciones o transferencias electrónicas de fondos no autorizados, que son el resultado de engañar a las personas a través de mensajes de texto, correos electrónicos o redes sociales para que proporcionen su información bancaria o financiera. (MINJUS, 2021).

Mucho menos comunes que estos ciberdelitos fueron el abuso de mecanismos y dispositivos informáticos, que representó el 4%, así como los ataques a la integridad de datos y sistemas informáticos, las propuestas a niños y adolescentes con fines sexuales a través de medios tecnológicos (grooming), el acceso no autorizado y la interceptación de datos informáticos, cada uno de los cuales tuvo un promedio del 1%. (DP, 2023).

En este contexto, el Observatorio Nacional de Política Criminal del Ministerio de Justicia y Derechos Humanos ha establecido una relación entre las denuncias por ciberdelitos y sus posibles víctimas, se ha identificado que son especialmente vulnerables las personas y empresas que compran y venden bienes y servicios a través de canales virtuales, aquellas que no saben cómo manejar y proteger sus datos, así como los niños y adolescentes. (MINJUS, 2020).

A menudo, en las investigaciones sobre ciberdelitos se solicita el levantamiento judicial de los secretos bancarios y de las comunicaciones, en el caso del secreto bancario, las entidades financieras deben entregar la información requerida en un plazo de 30 días hábiles y en cuanto al secreto de las comunicaciones, las empresas de telecomunicaciones están obligadas a facilitar de inmediato la intervención, grabación o registro de las comunicaciones en tiempo real, de manera continua durante las 24 horas del día. (DP, 2023).

Lamentablemente, en muchos casos estos plazos no se cumplen, llegando a extenderse más de seis meses, o las respuestas son parciales o, en el peor de los casos, no se reciben, lo que afecta el avance de la investigación policial, en cuanto a los datos de localización y geolocalización de teléfonos celulares y dispositivos similares, solo Movistar, Claro y Entel han implementado plataformas virtuales que permiten el acceso directo e inmediato, sin embargo, esta ubicación es solo indicativa, ya que se basa en las antenas que transmiten la señal, con un margen de error de entre 100 y 200 metros en áreas urbanas y de 1 a 2 kilómetros en zonas rurales, y no señala la ubicación exacta del celular.

(Nayia, 2020).

Esto requiere más recursos humanos y logísticos para la búsqueda y localización del objetivo, tal vez por eso, el 30% de los suboficiales que trabajan en la sede limeña de la Divindat-PNP están dedicados a esta tarea, cualquier evidencia digital, ya sean dispositivos electrónicos, computadoras o medios de almacenamiento, que se incauta es sometida a un análisis forense para obtener los elementos necesarios que el fiscal necesita para presentar su acusación contra los investigados por ciberdelitos, sin embargo, muchos de los equipos y software utilizados para la recolección, análisis y procesamiento de esta información se han vuelto obsoletos debido al avance de las tecnologías de la información y las comunicaciones, y sus licencias han caducado, lo que limita la capacidad operativa de la policía. (DP, 2023).

En lo que se refiere a los ciberdelitos que afectan la indemnidad y la libertad sexual de niños y adolescentes, esta organización internacional de Policía Criminal permite que la Divindat-PNP tenga acceso a la Base de Datos Internacional de Explotación Sexual (ICSE) y al programa Child Protection System (CPS), ambos impulsados por organizaciones estadounidenses como el Centro Nacional para Niños Desaparecidos y Explotados y la Coalición de Rescate Infantil, estas herramientas tecnológicas son fundamentales para identificar tanto a las víctimas como a los ciberdelincuentes que aparecen en el material de abuso y explotación sexual en línea. (Nayia, 2020).

Conclusiones

1. El Estado peruano desempeña un papel crucial en la lucha contra los delitos informáticos, pero necesita seguir fortaleciendo su marco legal, capacitando a su personal y fomentando la colaboración tanto a nivel nacional como internacional. La educación y la concientización de la población son igualmente vitales para prevenir estos delitos.
2. Estas colaboraciones permiten a Perú fortalecer su capacidad para enfrentar los desafíos del cibercrimen y mejorar su infraestructura de ciberseguridad.
3. La financiación de la lucha contra el cibercrimen en Perú proviene de una combinación de recursos estatales, cooperación internacional, iniciativas privadas y fondos para investigación. Para ser efectiva, es fundamental que estas fuentes de financiamiento se mantengan y amplíen, adaptándose a las crecientes demandas de ciberseguridad.
4. Estas colaboraciones han permitido fortalecer la capacidad del Estado para enfrentar el cibercrimen y mejorar la concienciación y preparación de la población y las empresas. La continuidad y expansión de estas iniciativas son esenciales para enfrentar los desafíos en el ámbito de la ciberseguridad.

V. REFERENCIAS

Ávalos Rivera, Z. (2021). Necesidad de especialización para combatir la ciberdelincuencia. *Revista institucional*, n° 15, pp. 43 – 62. file:///C:/Users/user/Documents/85-Texto%20del%20art%C3%ADculo-136-1-10-20211231%20(2).pdf

Barrado Castillo, R. (2018). *Teoría del delito: evolución, elementos integrantes*. https://ficp.es/wp-content/uploads/2019/03/Barrado-Castillo. Comunicaci%C3%B3n.pdf

Bruna Martíns. (16 de mayo de 2022). Convenio de Budapest sobre la ciberdelincuencia en América Latina. *Derechos digitales*. https://www.derechosdigitales.org/18451/convenio-de-budapest-sobre-la-ciberdelincuencia-en-america-latina/

Consejo nacional de seguridad nacional (9 de junio de 2021). *Implementan en Lima fiscalías especializadas*. https://conasec.mininter.gob.pe/noticias/implementan-en-lima-fiscal%C3%ADas-especializadas-en-ciberdelincuencia

Defensoría del Pueblo (mayo del 2023). Informe Defensorial N° 001 – 2023 – DP/ ADHPD. *La ciberdelincuencia en el Perú: estrategias y retos del estado*. https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Díaz Bohórquez, C. (2019). *La aplicación de la ley N° 30096 – Ley de delitos informáticos respecto a su regulación en el derecho penal peruano*. (Tesis para optar título de abogada, Universidad César Vallejo). https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/51569/D%c3%adaz_BCZ-SD.pdf?sequence=1&isAllowed=y

Carbajal Camones, M. (2022). *Las fiscalías especializadas en delitos informáticos como mecanismo para la lucha contra el cibercrimen*. (Tesis para optar título de maestría, Universidad de San Martín de Porres). https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/11398/carbajal_cm.pdf?sequence=1&isAllowed=y

Souto, M. (2023). La doctrina del derecho comparado en España, Revista general de

derecho público comparado, ISSN 1988-5091, Nº. 33.

Carriendo Téllez, L. (2022). *Delitos informáticos frente a estándares de derechos humanos y libertad de expresión en México*. (Maestría en Derecho de las tecnologías de información y comunicaciones). https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/518/1/SOLUCIONESTRATEGICA_LMCT.pdf

DAVARA, M. (2018). “Los Delitos Informáticos”, Editorial Aranzadi, Pamplona.

Defensoría del Pueblo. (2023). La ciberdelincuencia en el Perú: estrategias y retos del estado. https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Fauvarque-Cosson B., “Development of Comparative Law in France”, en Reimann M. & Zimmermann R. (eds.), *The Oxford Handbook of Comparative Law*, Oxford, UK: Oxford University Press , 2018.

Ferrante, A., “Entre Derecho Comparado y Derecho Extranjero. Una aproximación a la comparación jurídica”, en *Revista Chilena de Derecho.*

Ferrajoli Luigi. (1995). Derecho y razón, teoría del garantismo penal. *Editorial Trotta*. https://clea.edu.mx/biblioteca/files/original/5694a779b4871166c0edb73b407c9529.pdf

FortinetGuard Labs. (27 de febrero de 2023). *Fortinet informa que América Latina fue el objetivo de más de 360 millones de intentos de ciberataques en 2022*. https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent

Fuentes Garrido, K. (2021). *Modificación de la ley 30096 para incorporar los delitos de phishing, pharming y carding como delitos penalizables con prisión, para reducir la ciberdelincuencia, Lima 2019*. (Tesis para optar título de abogado, Universidad Señor de Sipán).

https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/8345/Fuentes%20Garrido%2C%20Karla%20Vanessa.pdf?sequence=1

Galdámez, L. (2019). “El uso del derecho y jurisprudencia extranjera en los fallos del Tribunal Constitucional de Chile: 2019”, en *Revista Chilena de Derecho*.

GARRIDO, M. (2020). Nociones Fundamentales de la Teoría del Delito Edit. Jurídica de Chile.

Guerrero, B. (2016). La investigación cualitativa. Revista de Innovación INNOVA, 1(2), pg. 1 - 9. file:///C:/Users/Usuario/Downloads/Dialnet-LaInvestigación Cualitativa-5920538.pdf

GUTIÉRREZ, M. (2021). Fraude informático y estafa. Madrid: Ministerio de Justicia.

Hirschl, R.,“The Question of Case Selection in Comparative Constitutional Law”, *The American Journal of Comparative Law*, Vol. LIII: 1, 2020

González J. (2018). EL DERECHO INTERNACIONAL DESDE ABAJO. EL DESARROLLO, LOS MOVIMIENTOS SOCIALES Y LA RESISTENCIA EN EL TERCER MUNDO BALAKRISHNAN RAJAGOPAL Instituto Latinoamericano de Servicios Legales Alternativos – ILSA 2018, Bogotá, Colombia, ISBN: 958-926255-4, 366 pág , International Law: Revista Colombiana de Derecho Internacional: Vol. 4 Núm. 7.

KRUTISH, Luis. Delitos informáticos. en: Revista Peruana de Derecho de la Empresa, Derecho informático Y Teleinformática Jurídica. No. 51. Lima: Asesor Andina, 2020.

Leyva Serrano, C. (2021). Estudios de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. Lucerna Iuris Et Investigatio, (1), 29–47. https://revistasinvestigacion.unmsm.edu.pe/index.php/Lucerna/article/view/18373/16528

López-Medina, D. (2021). “El nacimiento del Derecho Comparado moderno como espacio geográfico y como disciplina; instrucciones básicas para su comprensión y uso desde América Latina”, en *Revista Colombiana de Derecho Internacional*, Vol. 26,

Ministerio Público Fiscalía de la Nación. (2020). *Convenio sobre la ciberdelincuencia permite a jueces y fiscales realizar requerimientos de cooperación internacional*. [Nota informativa]. Lima, Perú. https://www.gob.pe/institucion/mpfn/noticias/302628-convenio-sobre-la-ciberdelincuencia-permite-a-jueces-y-fiscales-realizar-requerimientos-de-cooperacion-internacional

Morant , J. (2019). Protección penal de la intimidad frente a las nuevas tecnologías. Valencia – España : Práctica de Derecho.

Mori Quiroz, F. (2019). Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de Lima, periodo 2008 al 2012. (Tesis para optar título de maestría, Universidad Nacional Federico Villareal). https://repositorio.unfv.edu.pe/bitstream/handle/20.500.13084/3519/UNFV_MORI_QUIROZ_FRANCISCO_MAESTRIA_2019%20%283%29.pdf?sequence=1&isAllowed=y

Mühlen, J. (2018). Modelos de imputación en el derecho penal informático. pg: 41, Mexico.

Nogueira, H. (2021). “El uso del derecho extranjero y del derecho internacional por parte del tribunal constitucional chileno durante el período 2006-2007”, en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, núm. XXXVII.

Oficina de análisis contra la criminalidad (2021). Informe de análisis N.° 04. *Ciberdelincuencia en el Perú: pautas para una investigación fiscal especializada*. https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf

Peralta Castro, R. (2022). *Los delitos informáticos y los datos en sistemas informáticos*. (Tesis para optar título de abogado, Universidad peruana de las Américas). http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/2572/1.Ricardo%20Peralta%20-%20Delitos%20informaticos%20-%2015%20Marzo.pdf?sequence=1&isAllowed=y

Sotomayor Rodríguez, G. (2022). *La calificación fiscal en los delitos informáticos en el distrito fiscal de Lima Centro, 2019 – 2020*. (Tesis para optar título de abogado,

Universidad Cesar Vallejo). https://repositorio.ucv.edu.pe/handle/20.500.12692/95834

Tellez, J. (2019). “Los Delitos informáticos. Situación en México”, Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida.

Vílchez Vera, M. (2021). *Modificación del artículo 5 de la ley 30096 en función a la desproporcionalidad de la pena en el delito de child grooming, Chiclayo 2018*. (tesis para optar el título de abogado, Universidad Señor de Sipán). https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/8600/Vilchez%20Vera%2c%20Miguel%20Angel.pdf?sequence=1&isAllowed=y

Villanueva, J. (2023). *Ley de delitos informáticos N° 30096 y su influencia en la población de Chiclayo en tiempos de Covid – 19*. (Tesis para optar título de abogado, Universidad Señor de Sipán). https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/10627/Villanueva%20Calderon%20Juan%20Amilcar.pdf?sequence=1&isAllowed=y

Villavicencio F. (2014). Delitos Informáticos. *IUS ET VERITAS*, *24*(49), 284-304. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Zevallos, O. (2020). Delitos informáticos: ¿Cuáles son los principales fraudes informáticos que se pueden cometer a través del E-Commerce?. *Ius Et Veritas*. https://ius360.com/delitos-informaticos-cuales-son-los-principales-fraudes-informaticos-que-se-pueden-cometer-a-traves-del-e-commerce-oscar-zevallos-prado/

Nayia (2020). Amenazas emergentes en ciberseguridad: implicaciones para América Latina y el Caribe.

Banco Interamericano de Desarrollo y Organización de los Estados Americanos (2020). Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte Ciberseguridad 2020. Washington D.C, página 28