Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

**FACULTAD DE DERECHO Y CIENCIA POLÍTICA**

# LA SEGURIDAD DE LA INFORMACIÓN DIGITAL Y SU IMPACTO EN LA CONFIGURACIÓN DE DELITOS INFORMÁTICOS EN EL DERECHOPENAL PERUANO EN LIMA METROPOLITANA 2023

**Línea de investigación:**
**Procesos jurídicos y resolución de conflictos**

Tesis para optar el Título Profesional de Abogado


**Autor**

Sangama Huarmiyuri, Cheryl

**Asesor**

Jiménez Herrera, Juan Carlos

ORCID: 0000-0001-9996-2047


**Jurado**

Gonzales Loli, Martha Rocio

Ambrosio Bejarano, Hugo Ramiro

Moscoso Torres, Víctor Juber

**Lima - Perú**

**2025**

# SANGAMA HUARMIYURI, Sheryl.docx

INFORME DE ORIGINALIDAD

| 26% | 25% | 9% | 14% |
|---|---|---|---|
| INDICE DE SIMILITUD | FUENTES DE INTERNET | PUBLICACIONES | TRABAJOS DEL ESTUDIANTE |

FUENTES PRIMARIAS

| | | |
|---|---|---|
| 1 | Submitted to Universidad Nacional Federico Villarreal<br>Trabajo del estudiante | 4% |
| 2 | repositorio.unfv.edu.pe<br>Fuente de Internet | 3% |
| 3 | hdl.handle.net<br>Fuente de Internet | 3% |
| 4 | repositorio.ucv.edu.pe<br>Fuente de Internet | 1% |
| 5 | cdn.www.gob.pe<br>Fuente de Internet | 1% |
| 6 | www.coursehero.com<br>Fuente de Internet | 1% |
| 7 | repositorio.autonoma.edu.pe<br>Fuente de Internet | 1% |
| 8 | www.informatica-juridica.com<br>Fuente de Internet | <1% |
| 9 | dspace.unl.edu.ec<br>Fuente de Internet | <1% |
| 10 | repositorioacademico.upc.edu.pe<br>Fuente de Internet | <1% |
| 11 | www.ohchr.org<br>Fuente de Internet | <1% |
| 12 | "Ciência, Desenvolvimento e Humanidades: desafios para a transformação no conhecimento", Editora Cientifica Digital, 2024<br>Publicación | <1% |

Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACION

**FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS**

# LA SEGURIDAD DE LA INFORMACIÓN DIGITAL Y SU IMPACTO EN LA CONFIGURACIÓN DE DELITOS INFORMÁTICOS EN EL DERECHOPENAL PERUANO EN LIMA METROPOLITANA 2023

**Línea de investigación:**

Procesos Jurídicos y Resolución de Conflictos

**Tesis para optar el Título Profesional de:**

Abogado

**Autor:**

Sangama Huarmiyuri, Cheryl

**Asesor:**

Jiménez Herrera, Juan Carlos

ORCID: 0000-0001-9996-2047

**Jurado:**

Gonzales Loli, Martha Rocío

Ambrosio Bejarano, Hugo Ramiro

Moscoso Torres, Víctor Juber

**Lima-Perú**

**2025**

**DEDICATORIA**

A mi adorada madre, a mis hermosas hijas y a mi amado esposo**.**

**AGRADECIMIENTO**

A mis padres, hermano y hermana por impulsarme y apoyarme en cada paso de mi desarrollo profesional

**INDICE**

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

# RESUMEN

**Objetivo:** Determinar la manera en que la seguridad de la información digital impacta en la configuración de los delitos informáticos en el derecho penal peruano en Lima Metropolitana durante el año 2023. **Método:** El tipo de investigación llevado a cabo se desarrolló de forma básica, con alcance correlacional, diseño utilizado no experimental, transeccional – correlacional. Por otro lado, la muestra para el presente trabajo estuvo conformada por 50 abogados especialistas en la rama de derecho penal y procesal penal, así también como juristas experimentados en la misma rama, los cuales serán seleccionados a través del muestreo probabilístico aleatorio simple. Asimismo, se utilizó diversas herramientas como es el caso de las encuestas la cual fue comprobado a través del juicio de expertos por los cuestionarios, y de la igual forma, se empleó el análisis del contenido. **Resultados:** Es necesario definir las fuentes de información a tomar en cuenta con la finalidad de establecer la calidad de la seguridad de la información digital en Lima Metropolitana, y más aun tomando en consideración que el tema de los delitos informáticos son uno de los grandes asechos para la sociedad limeña con respecto a la seguridad de datos. **Conclusiones:** A través de las encuestas se puede concluir que la configuración de los delitos informáticos en el derecho penal peruano en Lima Metropolitana durante el periodo del 2023 está determinada por la falta de seguridad de la información por lo tanto es necesario que se amplíen o modifiquen las normativas referentes a la protección de datos.

**Palabras clave:** Seguridad de información, Información digital, Delitos informáticos, Protección de datos, Normativa penal digital.

## ABSTRACT

**Objective:** To determine how digital information security impacts the configuration of computer crimes in Peruvian criminal law in Metropolitan Lima during the year 2023. **Method:** The type of research carried out was developed in a basic way, with correlational scope, non-experimental, transectional-correlational design. On the other hand, the sample for the present work consisted of 50 lawyers specialized in the field of criminal law and criminal procedure, as well as experienced jurists in the same field, who were selected through simple random probability sampling. Likewise, several tools were used, such as surveys, which were checked through expert judgment by means of questionnaires, and content analysis was also used. **Results:** It is necessary to define the sources of information to be taken into account in order to establish the quality of digital information security in Metropolitan Lima, and even more so taking into consideration that the issue of computer crimes is one of the greatest threats to Lima's society with respect to data security. **Conclusions:** Through the surveys it can be concluded that the configuration of computer crimes in Peruvian criminal law in Metropolitan Lima during the period of 2023 is determined by the lack of information security therefore it is necessary that the regulations concerning data protection are expanded or modified.


**Keywords:** Information security, Digital information, Computer crimes, Data protection, Digital criminal law.

# I. INTRODUCCIÓN

El presente proyecto de tesis titulado “La seguridad de la información digital y su impacto en la configuración de los delitos informáticos en el derecho penal peruano en Lima Metropolitana 2023” desarrolla una problemática para la cual es indispensable conceptualizar así como analizar cada uno de los elementos que la conforman, así también, es necesario, establecer los lineamientos para la elaboración de la presente tesis, pues si bien tema escogido de por sí reviste de complejidad, también es un tema de gran amplitud. Por lo tanto, es que es tocaremos que la base legal en la cual se fundamenta, en este caso es únicamente la Ley N°30096.

Una vez que se pone en vigencia la Ley N°30096, es que podemos determinar los vacíos legales que se encuentran dentro del Código Penal peruano, pues la primera ley mencionada y las modificatorias realizadas a esta, es la única que regula los delitos informáticos entendiéndolos como aquellos actos ilícitos que van en contra o afectan los sistemas informáticos y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas a través de la utilización de tecnologías de la información o de la comunicación (lo que comúnmente se conoce como TIC´s), todo esto con la finalidad de garantiza la lucha eficaz contra la ciberdelincuencia.

Por otro lado, tenemos a la seguridad de la información digital entendida como la ausencia del peligro de delitos informáticos, así como que los usuarios sientan plena confianza con los mecanismos que implante las entidades del sector público como privado con respecto a la información personal o base datos, tales como normativas, controles, acciones y medidas de seguridad.

Por tal razón es que nuestra investigación se centra en la falta de implementación de mecanismos de alta seguridad de información digital, pues la misma se convierte en un elemento determinante para la configuración de los delitos informáticos, por lo tanto, es que

llevaremos a cabo un análisis de la falta de normativa, la colaboración internacional, el fomento de confianza en la población hacia las entidades, así como las posibles medidas que permitan adaptarse a nuevas amenazas.

## 1.1. Descripción y formulación del problema

### *1.1.1. Descripción del problema*

Teniendo en cuenta que la presencia masiva de los delitos informáticos a nivel global es uno de los temas que asecha a los seres humanos, es que aseguraros que su principal causante es la falta de seguridad de la información digital en los sistemas informativos.

Ahora bien, el tema de la seguridad de información es amplia, pero podemos conceptuarlo como la protección de la confidencialidad, la integridad, así como la disponibilidad de los datos, pero conservando la privacidad de los datos personas de las personas naturales, así como de las personas jurídicas, ya sean tanto públicas como privadas. Por lo tanto, una vez que los ciberdelincuentes sobrepasen las barreras de seguridad informativa que son impuestas por los usuarios de manera válida, pero a través de datos falsos o incompletos, es que se da inicio con lo que nosotros denominamos como delitos informáticos, pues son estos quienes una vez al acceso de esta información los destinan para hacer uso de las mismas, pero en distintas modalidades, generando así distintos tipos de delitos.

Si nos ponemos a analizar la situación es que podemos decir que tan fiable son los mecanismos impuestos para la seguridad de la información digital, pues la seguridad como tal implica la ausencia del peligro, daño o riesgo, permitiendo que los usuarios que acudan a ella, desarrollen la sensación completa de confianza, pero si tomamos referencia de la seguridad que ofrecen otros países con el territorio peruano, no hay duda alguna que la cantidad de ciudadanos que optan por acceder a seguridades especiales en el territorio peruano en entidades públicas como en privadas son en menor cantidad en referencia con los ciudadanos de otros países y más

aún si toma en cuenta, que la legislación peruana no tiene normativa alguna que regule o estipule seguir ciertas normas, o en todo caso, afiliarse con sistemas de protección de datos informáticos especiales o internacionales.

Llevando esto a la práctica, tendríamos que, dentro del ámbito internacional, la seguridad de información digital o también denominado como ciberseguridad se ha convertido en uno de los mayores temas de debate, pues la ciberdelincuencia implica la vulneración de derechos fundamentales, como es el caso del derecho a la privacidad. Y, en concordancia con esto último, tenemos que la Organización de las Naciones Unidas se ha pronunciado sobre este tema acotando que, el derecho a la privacidad es un derecho fundamental para el goce y el ejercicio de los derechos humanos en línea y fuera de línea, además, desempeña un papel fundamental en la realización de una amplia gama de derechos humanos, inclusive dentro de la esfera digital, los cuales van desde la libertad de expresión, asociación, así como de reunión, pasando por el acceso y el disfrute de los derechos económicos y sociales.

Por lo tanto, se han establecido normativas las cuales regulan el derecho de la seguridad de información de manera implícita como es el caso del art.12 de la Declaración Universal de los Derechos Humanos, y también, el art. 17 del Pacto Internacional de Derechos Civiles y Políticos, pues ambos establecen que ninguna persona deberá ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia o su correspondencia, ni de ataques ilegales a su honra y reputación. Si analizamos esto último, podríamos decir que, si bien no se menciona literalmente la palabra ciberdelincuencia, lo que si se infiere que esta es una injerencia ilegal que afecta directamente a una persona a través de su honra y su reputación. De igual manera, ambos artículos disponen que, toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques; por lo que, de esto último se infiere que el Estado o el gobierno está en la obligación de establecer normas o mecanismos que fortalezcan la confianza de la población con respecto a la seguridad de la información digital, así como la sanción drástica hacia aquellos

que cometen delitos informáticos.

A pesar de ello, la normativa planteada la seguridad de la información digital es muy general, por lo tanto, es necesario que cada Estado implante sus normativas locales con respecto a este. Un ejemplo claro, es España, pues cuenta con una gran cantidad de normativas con respecto a las ciberseguridad, entre ellas podemos rescatar a la Estrategia de Seguridad Nacional implementada en el 2017, la Ley 36/2015 de Fomento de la Financiación Empresarial, la cual se encarga de exigir a las empresas del sector financiero a contar con sistemas de seguridad especializados y adecuados, las cuales garanticen la protección de la información financiera de los usuarios registrados, y finalmente, está el Real Decreto Ley 12/2018 de Seguridad de las Redes y Sistemas de información. A pesar de esto, no cabe duda que, a nivel internacional, hay muchos países que cuentan con una gran regulación con respecto a la seguridad de la información digital.

Por otro lado, si nos ponemos en el lado contrario, lo primero que podemos decir es que a diferencia con España, Perú se ha demorado más de 10 años en implementar normativas referentes a este tema, y más aún la situación es preocupante, pues nuestro territorio, cuenta únicamente con la Ley N°30096 con respecto a los delitos informáticos, y con respecto a la seguridad de la información digital, en caso del sector de la administración pública, esta está a cargo del Centro Nacional de Seguridad Digital y Transformación Digital y con ella, la normativa principal es la ISO 27001 – Sistema de Gestión de Seguridad, la cual se encarga de otorgar un marco de trabajo para los sistemas de gestión de seguridad de la información con la finalidad de proporcionar confidencialidad, integridad y disponibilidad de la información, así como el cumplimiento legal de dichos sistemas. A pesar de esto, no se debe olvidar que se está hablando únicamente de una sola normativa, lo que hace que la confiabilidad de los usuarios en el sistema público sea escasa, y, por ende, tengan que acudir a sistemas de información privados.

Esto último también es preocupante, pues dentro del sector privado, si bien cada empresa es autónoma con respecto a los mecanismos empleados para la seguridad de información, no se presenta norma alguna que regule de manera conjunta a todas las entidades a nivel nacional, lo que hace aún mayor el problema, dejando al criterio de los usuarios la elección con respecto con qué entidad se desea trabajar, y esto dependerá únicamente, de la publicidad y los beneficios que otorguen a sus usuarios. Por lo tanto, es de aquí que se desarrolla nuestra problemática, la seguridad de la información digital que emplea cada sector en el territorio peruano, lo cual conlleva a la configuración de los delitos informáticos.

### *1.1.2. Formulación del Problema*

#### *a. Problema General*

- ¿De qué manera la seguridad de la información digital impacta en la configuración de los delitos informáticos en el derecho penal peruano en Lima Metropolitana 2023?

#### *b. Problemas Específicos*

- ¿Cuáles son las principales amenazas a la seguridad de la información digital que influyen en la configuración de delitos informáticos en el Perú?
- ¿Cómo ha evolucionado la normativa penal peruana para abordar los delitos informáticos en relación con la seguridad de la información digital?
- ¿Qué desafíos enfrenta el derecho penal peruano en la tipificación y sanción de delitos informáticos relacionados con la seguridad de la información digital?

## 1.2. Antecedentes

Para llevar a cabo la redacción de la presente tesis se tomó en cuenta como referencias distintos repositorios virtuales, todo esto con la intención de recabar información de distintos

trabajos y líneas de investigación, tales como artículos, tesis, revistas, así también como libros publicados en línea, las cuales se encuentran ligadas directamente con el título de esta investigación. Con todo lo anterior, se logrará saciar las condiciones objetivas previamente establecidas y también las metodológicas, con la finalidad de que esta tesis se considere posible.

### *1.2.1. Antecedentes Nacionales*

En primera resaltamos a Portugal (2024) pues a través de su trabajo titulado *"Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano 2023"* para optar el título profesional de Abogado en la Universidad Privada San Carlos, Puno, donde se acota que, los seres humanos han adaptado su estilo de vida a la tecnología a tal punto, no es raro encontrar diversos medios digitales almacenados con gran cantidad de información personal de millones de personas, sin embargo, se ha llegado al punto que, se ha transformado en un mecanismo que es desarrollado por terceras personas que se aprovechan de esto para vulnerar los derechos de los primeros a través del Internet y de los medios electrónicos, a esto es lo que se denomina "delito informático" o también conocido como ciberdelito o ciberdelincuencia, lo cual está lejos de convertirse en mecanismo beneficioso para la sociedad a nivel mundial. (p. 18)

De igual manera, tenemos a Urdanegui (2023) a través de su trabajo de investigación titulado *"Los Delitos Informáticos y la Vulneración del Derecho fundamental de Protección de Datos Personales en Lima Metropolitana"* para obtener el Título profesional de Abogado en la Universidad Autónoma del Perú, Lima, llegó a la conclusión que, con el paso del tiempo, sin duda, se van sumando nuevas tecnologías los cuales, si bien son una gran ventaja para la sociedad, también significa una oportunidad a la mayor concurrencia de los delitos informáticos, y aunado a esto, tenemos que las TIC´s otorga más facultades a los ciberdelincuentes permitiéndoles establecer planes para la comisión de hechos delictivos superando las barreras de la seguridad para la información, así también como eliminar las pistas que permitan reconocerlos como autores del delito. (p.15)

Continuando, es que ponemos en evidencia lo que menciona Román (2020) pues a través de su proyecto el cual lleva por título *"Modificación Legislativa de la Ley 30096 de Delitos Informáticos para su eficacia contra la Ciberdelincuencia en la Ciudad de Chiclayo"* para optar el Título Profesional de Abogado en la Universidad Señor de Sipán, Lambayeque, acota que, los delitos informáticos se cometen a través de diversos mecanismos mediante la red de Internet, atentando o vulnerando la seguridad de la información así como de las personas ya sea natural o en todo caso, jurídica, todo ello, con la finalidad de acceder a información personal y privada para llevar a cabo actos ilícitos como el fraude virtual. Uno de estos, es el phishing, que consta en robar las contraseñas o números de tarjetas por medio de correos electrónicos falsos los cuales son ajenos a las organizaciones reales y oficiales de que la proviene el correo, a pesar de esto, el phishing no es el único delito, sino que, al contrario, la variedad de delitos de informáticos hace que la preocupación por sanear estos los vacíos jurídicos sea uno de los grandes temas de discusión para la modificatoria de la Ley N° 30096. (p. 11)

Por otro lado, tenemos a Osco (2019) quien a través de su tesis *" La admisibilidad y el valor probatorio de la evidencia digital en el Sistema Jurídico Peruano 2018*" para optar el grado académico de Maestro en Derecho Penal y Procesal Penal en la Universidad César Vallejo, Lima, aclara que los delitos informáticos es un término, una nueva forma de determinar a lo que en la práctica se conoce como ciberdelincuencia, la cual se define como aquellas conductas las cuales están destinadas a evadir los protocolos establecidos para la seguridad de la información virtual a través del uso de herramientas digitales como las computadores, laptops, etc. y de claves válidas las cuales son obtenidas de manera ilegal para obtener información privada. Además, se caracteriza y acentúa por la constante evolución de las TIC´s, por tal razón es que se ha promulgado una Ley especial la cual está destinada a prevenir y hacer frente a las actos ilícitos virtuales, los cuales tienen como fin dañar el sistemas de información y/o datos informáticos, así como el secreto de las comunicaciones, a pesar de ello, una ley

especial no cubre con las necesidades que asecha un problema de gran magnitud como este sino que también depende en gran medida de los sistemas de control de red, los cuales en el territorio peruano es uno de los mayores problemas pues no permite verificar la información publicada así como los datos de los ciberdelincuentes, y de igual manera permite que las alternativas para poder modificar datos, perjudicando los sistemas de seguridad sea mayor, otorgando así, más facilidades de arruinar los sistemas de información virtual. (p. 41 -42)

Finalmente, es que resaltamos a Chávez (2018) quien a través de su tesis "*El delito contra Datos y Sistemas Informáticos en el Derecho fundamental a la Intimidad Persona en la Corte Superior de Justicia de Lima Norte, 2017"* para obtener el grado académico de Doctor en Derecho en la Universidad Nacional Federico Villareal, manifiesta que, la tecnología con respecto a la seguridad de la información y la telecomunicación ha evolucionado significativamente, lo cual ha conllevado a que se implementen nuevas metodologías experimentales para que la información que es almacenada o tratada de forma privada a través de los medios digitales sea transmitida de manera ilícita a través de los sistemas informáticos actuales, perjudicando así los derechos fundamentales de los ciudadanos, y por tal razón, es que se ha puesto en vigencia la Ley N° 30096 (o también conocida como la Ley de los Delitos Informáticos" la cual ha modificada por la Ley N° 30171 y que trata básicamente de los delitos contra la protección de datos y sistemas informáticos, contra la libertad sexual, la intimidad, el patrimonio, así como también como el secreto de las comunicaciones e información. (p.22)

### *1.2.2. Antecedentes Internacionales*

Bascur (2023) a través de su trabajo *"Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459 – Primera parte"* para obtener el grado académico de Doctor en Derecho en la Universidad Austral, Chile, establece que, debido a los continuos avances de la tecnología sobre acceso a la información y la relevancia

social a la que esto conlleva, ha generado que el centro de estudio se centre en los sistemas de almacenamiento de información, el procesamiento de los mismos, así también como en la transferencia de los datos, sin embargo, debido a las grandes masas de delitos informáticos que se cometen diariamente, es que en la actualidad, en el centro de estudio se fija en la protección penal y la seguridad de la información que para los ciberdelincuentes son de fácil acceso. Por tal razón es que el Estado Chileno se ha visto en la necesidad de promulgar la Ley 21.459 de la cual, se regula los delitos informáticos en cinco categorías: los que afectan a la integridad, los que van en contra de la disponibilidad, la tercera contra la confidencialidad de los datos informáticos o sistemas informáticos, los delitos que tienen como destino el aprovechamiento y finalmente, los que son de naturaleza mixta." (p.6)

Continuando es tiene a Peña (2023) quien realizó un estudio de investigación titulado *"Delitos Informáticos"* para optar el grado académico de Maestro en Ciencias Penales y Criminológicas en la Universidad Libre, Colombia, podemos entender que, el uso masivo del Internet sobre todo en el sistema financiero ha provocado que diariamente miles de personas realicen transacciones digitales, lo cual involucra que el intercambio de información sea extenso; y es de ahí de donde inicia los delitos informáticos a través del acceso y uso posterior de esta información para llevar a cabo estafas o fraudes en línea, poniendo el juego la confianza de las personas en la entidades financieras cuando estas reciben llamadas de personas que se hacen pasar por laboradores de estas empresas. Todo ello ha generado, que los famosos delitos informáticos se consideren como uno de los temas más grande de seguridad en el territorio colombiano, poniendo a prueba la capacidad de las autoridades para llevar a cabo medidas drásticas para sancionar a aquellos que incurran en estos delitos, así como también promover de manera eficiente seguridad de la información personal disponible en internet". (p.19)

Continuando, se tiene a Contento (2023) quien a través de su investigación *"La problemática de los Delitos Informáticos en el Ecuador, su persecución y capacidad preventiva*

*de la legislación ecuatoriana en contrataste con el Derecho Comparado"* para obtener el título de Abogado en la Universidad de Loja, Ecuador, menciona que, la seguridad informática se ha convertido en una de las bases fundamentales del Internet en la actualidad. La protección actual de la información actúa como aval para la expansión masiva del internet, así como la entrada de usuarios nuevos, los cuales hoy en día poseen una total desconfianza del sistema de seguridad de las distintas webs. Si bien es cierto que la legislación ecuatoriana cuenta con una regulación con respecto a la protección de la información a través de la incorporación de los delitos informáticos dentro de su Código Penal a partir del 2014, esto no ha tenido según el autor un "enfoque adecuado", por tal razón es que el Estado se ha visto en la necesidad de hacer diversas modificatorias desde el 2016 al 2022, dentro de los arts. 103 y 104; sin embargo, estos no son suficientes, pues revisten de diversos vacíos legales, los cuales hacen que los delitos informáticos se conviertan en uno de los temas de mayor preocupación para la sociedad ecuatoriana. (p.78-79)

De igual manera, se tiene a Carranza (2022) quien a través de su tesis *"El delito de Estafa Informática en El Salvador"* para optar el grado de Licenciado en Ciencias Jurídicas en la Universidad de El Salvador, El Salvador, acota que los delitos informáticos se encuentran regulados dentro de la ley especial de los Delitos Informáticos así también como dentro del Código Penal, y son definidas como el ataque a la seguridad de un sistema informático ya sea de manera total o parcial, y dentro de todos estos delitos, la estafa informática es que más aqueja en Argentina, la cual se comete a través de la manipulación ilegal en el ingreso de sistemas informáticos, así como el procesamiento de los datos y transmisión o manejo de los mismos a través del uso de datos falsos o incompletos, con la finalidad de obtener un beneficio personal patrimonial. Con respecto a su regulación, la estafa informática está prevista dentro del artículo 216 numeral 5 del Código Penal argentino, y también dentro del art. 10 de la Ley especial de los Delitos Informáticos y Conexos de El

Salvador". (p.112)

Por último, tenemos a Gómez (2021), pues a través de su tesis titulada *"Aspectos Procesales de los delitos informáticos y tecnológicos"* para optar el grado de Doctor en Ciencias Sociales y Jurídicas en la Universidad de Rey Juan Carlos, España, menciona que, los delitos informáticos es el tema de estudio del Derecho Informático, el cual es entendido como un derecho que reviste de autonomía y sustantividad propia; que se caracteriza por ser el conjunto de normas jurídicas las cuales están destinadas a regular el medio informático. A pesar de ello, esta rama no es la única que las regula, sino que también, a través del Código Penal español se sancionan una cantidad de delitos informáticos, las cuales se originan por la constante evolución de las tecnologías de la información y comunicación (lo que en la práctica se conoce como TIC´s) y además de, la facilidad de acceso de las mismas hacia población, conllevando así a que millones de españoles terminen siendo afectados por al menos uno de estos delitos. (p.49)

## 1.3. Objetivos

### *1.3.1. Objetivo General*

- Determinar las formas en que la seguridad de la información digital impacta en la configuración de los delitos informáticos en el derecho penal peruano.

### *1.3.2. Objetivos Específicos*

- Establecer las principales amenazas la seguridad de la información digital que influyen en la configuración de delitos informáticos en el Perú.
- Definir la evolución de la normativa penal peruana para abordar los delitos informáticos en relación con la seguridad de la información digital.
- Establecer los desafíos que enfrenta el derecho penal peruano en la tipificación y sanción de delitos informáticos relacionados con la seguridad de la información

digital.

## 1.4. Justificación de la investigación Justificación

La presente investigación presenta su justificación a través de los siguientes:

### *1.4.1. Justificación Teórica*

La tesis en presentación busca hacer un análisis sobre la configuración de los delitos informáticos en el derecho penal peruano a través de la vulneración de la seguridad de la información digital, por lo que, para esto, se deberá tener en cuenta las bases legales y conceptuales para la determinación de los delitos informáticos, así también como su relación con la seguridad de la información, todo lo anterior con la finalidad, de mejorar su compresión no solo de manera teórica sino también como es que se desarrolla en la práctica.

### *1.4.2. Justificación Metodológica*

Debido a su enfoque cuantitativo, y teniendo como objetivo analizar la relación entre la seguridad de la información digital con la configuración de los delitos informáticos en el derecho penal peruano, creemos que, es de suma importancia que se realice la revisión de la normativa legal actual correspondiente, así también como la situación en Lima metropolitana.

Este último, se logrará a través de las herramientas para la investigación como es el caso de las encuestas, las cuales estarán dirigidas a los profesionales en Derecho, pero especializados en la rama del derecho penal, esto debido a que el tema desarrollado en la presente tesis corresponde a la misma rama, por lo tanto, es necesario enfocarnos en estos especialistas a fin de los mismos, nos otorguen respuestas debidamente sustentadas a cada una de las interrogantes planteadas.

### *1.4.3. Justificación Social*

La presentación masiva y exponencial de los delitos informáticos en Perú, ha generado

un gran impacto en la sociedad limeña la cual afecta diariamente a miles de peruano, así también como instituciones tanto públicas como privadas. Además, la falta de conciencia sobre la seguridad de la información digital debido a los vacíos legales en la normativa del derecho penal, ha permitido la proliferación de estos delitos, conllevando a la vulnerabilidad en la protección de los datos personales como patrimoniales. Por esta razón, es que esta investigación reviste de gran importancia, pues busca contribuir a la comprensión de los operadores jurídicos, legisladores y ciudadanos en general sobre la problemática actual, la prevención y mitigación de los delitos informáticos mediante la modificación de la legislación y la comprensión del desarrollo de la seguridad digital.

## 1.5. Hipótesis

### *1.5.1. Hipótesis General*

- La configuración de los delitos informáticos en el derecho penal peruano se ve determinada por falta o la insuficiencia de la seguridad de la información digital, facilitando que cada vez más los ciberdelincuentes actúen con más frecuencia.

### *1.5.2. Hipótesis Específicas*

- Las principales amenazas a la seguridad de la información digital en el Perú como el malware y el phishing, tienen un impacto significativo en la configuración de los delitos informáticos, aumentando la incidencia de delitos cibernéticos.
- La normativa penal peruana ha evolucionado de manera insuficiente para abordar los delitos informáticos, lo que ha llevado a una desactualización en la legislación frente a las nuevas amenazas a la seguridad de la información digital.
- El derecho penal peruano enfrenta desafíos significativos en la tipificación y sanción de delitos informáticos, debido a la falta de capacitación en ciberseguridad de los operadores de justicia y a la dificultad de prueba en entornos digitales.

# II. MARCO TEÓRICO

## 2.1. Bases Teóricas

### *2.1.1. Información digital*

Para empezar, tenemos que empezar definiendo el término “información”, pues bien, según el diccionario de la Real Academia de la lengua española (RAE) concibe a la información como comunicación o adquisición de conocimiento que permiten ampliar o precisar los que se poseen sobre una materia determinada.

Es aquí, en donde lo que concibe como la adquisición de conocimientos se le añade el término “digital” el cual hace referencia a lo virtual de la información. Si bien antes, la información se tenía que buscar a través de documentos físicos, libros o revistas, ahora es fácil de encontrar información virtual, es decir, información la cual se encuentra anclada en sitios webs. Pero para llegar a transición, es que hemos tenido que pasar por un período de actualización, es así que podemos que la llegada del Internet, cobra gran importancia pues se este se ha convertido en un elemento clave la transición de lo físico a lo digital.

La constante evolución de la tecnología ha traído grandes cambios para la sociedad con respecto a la información, pues a través de las tecnologías de la información y la comunicación (lo que comúnmente se conoce como TIC´s) se permite el acceso y el intercambio de información de manera rápida, preciosa, y, sobre todo, a nivel global, consiguiendo la internacionalización de la información y su difusión entre los seres humanos sin importar en donde se encuentren.

Por lo tanto, es podemos concebir a la información digital como todo aquel tipo de dato de información la cual se almacena, se lee, se transfiere y se utiliza a través de los

dispositivos electrónicos, facilitando su compartimiento y disposición desde cualquier lugar y en cualquier momento, destacándose de los procedimientos manuales por ser más rápido y preciso.

Además, en concordancia con lo anterior, tenemos que, para Paletta (2022) la información digital es el conjunto de bases y bancos de datos. Además, incluyen sistemas de gestión de contenidos, gestión de documentos electrónicos, sistemas de recuperación, así también como técnicas de programación de web, los cuales incluyen preservación y conservación digital. (p. 150)

Además, este mismo autor, Paletta (2022) acota que la información digital posee ciertas características, las cuales permite su diferenciación, entre ellas se tiene:

a) **Su heterogeneidad:** pues no solo estamos hablando de simples letras, oraciones o libros digitales, sino que también la información digital puede ser representada a través de imágenes o sonidos.
b) **Su computabilidad:** pues solo basta un ordenador, una computadora, laptop, Tablet para que se pueda acceder a la información digital.
c) **Su virtualidad:** esto hace referencia al uso del internet, pues sin ella no sería capaz la conexión que permita acceder a este tipo de información.
d) **Su capacidad:** Esto debido a que, a través del uso del internet, se puede acceder a una cantidad ilimitada de información.
e) **Fragilidad:** según el autor, esto más que una característica, se podría considerar como una desventaja, pues el fácil acceso a la información digital permite que terceros con intenciones contrarias al conocimiento, se aprovechen de estas para poder cometer actos ilícitos que vayan en contra de los derechos de las personas.

De igual manera, Hincho (2023) señala que la información digital debe ser transparente, esto como un regla general que debe ser aplicada a todo tipo de información que se encuentra en línea, es decir, tanto los servidores públicos, como los directores así como los gerentes de compañías e instituciones del sector privado deben conducirse de manera viable, previsible y

comprensible con respecto a la información que manejen en sistemas información o páginas webs, todo esto con la finalidad de impulsar la participación y la confianza de los usuarios hacia las entidades. (p. 25)

Por otro lado, es necesario entender que, debido a la importancia del uso del Internet en la vida de cada persona, es necesario que los diferentes gobiernos de todas las partes del mundo establezcan, desarrollen, fortalezcan o modifiquen sus políticas públicas y privadas con respecto a la uso y desarrollo de la información digital, pues este último debe transformarse como un medio para el fortalecimiento de la sociedad en todas sus esferas, social, política, económica, académica y no como herramienta que conlleve a la destrucción de la misma. (Torres, 2017)

En esa misma línea, podemos entender que la importancia de la información digital radica en su expansión, pues cada día aumenta la cantidad de información que se intercambia entre un creciente número de usuarios, generando una mayor productividad entre los diversos sectores, tanto públicos como privados, así también como en cada una de las esferas de desarrollo, como el social, económico, político, así también como mercantil, otorgando un beneficio amplio a cada uno de los ciudadanos a nivel mundial.

### *2.1.2. Seguridad de información digital*

Teniendo a la información como una herramienta que está a disposición de la sociedad en cualquier parte del mundo, es necesario entonces que, debido a su importancia esta debe protegerse a tal medida, que no afecte al desarrollo de la población ni que vulnere los derechos fundamentales de los usuarios o personas que optan por poner su información personal en línea. Aunque a primera vista, pueda sonar como una alternativa facultativa de las personas el hecho de que puedan subir su información a línea (convirtiéndose automática en información digital), lo innegable es que la constante evolución de los TIC´s ha impedido que esto no sea facultativo.

Ahora bien, si este último lo queremos llevar a la práctica, podemos darnos cuenta que hoy en día es raro encontrar a una persona que no tenga redes sociales, hasta los más jóvenes y pequeños ya se encuentran inmersos dentro del esfera digital. Al hacer uso de estas redes, lo lógico es que estas posean una cuenta, lo que indirectamente significa subir información personal a estas páginas, lo que en algunos casos termina en malas situaciones como son los famosos hackeos de cuenta, la cual implica una vulneración de los derechos fundamentales, como el derecho a la privacidad.

Por otro lado, a diferencia de las cuentas de redes sociales que son las más comunes, es que se tiene el uso de las tarjetas bancarias. Cuando una persona se acude a una entidad bancaria (usuario) para obtener una tarjeta, se somete a los requisitos pre establecidos por la entidad privada y otorga datos e información, la cual, a diferencia de las redes, no se encuentra a la libre disposición de otros usuarios, sino que se almacena en grandes sistemas informativos, sin embargo, esto no significa que la misma se vea envuelva por un delito informático, conllevando de igual manera, a la afectación de los derechos fundamentales de miles de usuarios.

Pese a esto, para llegar al hecho de que se comentan los delitos informáticos es porque hay un factor clave que no actúa de manera eficiente, esta es la seguridad o los mecanismos que se imponen para la protección de la información digital. En tales líneas, es que podemos recatar a Ramírez (2022) quien menciona a través de la Revista Ibérica de Sistemas e Tecnologías de la Información que, teniendo a la información digital como un activo vital dentro de cualquier tipo de institución, pública o privada, es que la seguridad de la información o también denominado como ciberseguridad está integrado por una cantidad de instrucciones y elementos, los cuales tienen como finalidad principal brindar tres características fundamentales de la información: su disponibilidad, su confidencialidad y su integridad, asimismo, la seguridad de la información digital está conformado por políticas establecidas y previamente

definidas, así también como controles de seguridad, todo esto con la finalidad de que las organizaciones mantengan salvaguarda sus sistemas de ataques, daños o pérdidas de información a través de delitos informáticos. (p.88)

De la misma manera, a través de un comunicado de la Unión Europea por el año 2013 por el secretario general de Europa titulado *"Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro"* nos menciona que la ciberseguridad abarca medidas de salvaguardas las cuales pueden ponerse en práctica en el ciberespacio, en todas y cada de las esferas de desarrollo de la población, contra las posibles amenazas que esta sufra o altere la información. Por esta razón, es que seguridad de la información digital tiene como finalidad principal mantener la disponibilidad e integridad de las redes e infraestructura y la confidencialidad de la información que contiene. (p.31)

Además, a través de la una de las revistas virtuales emitidas por la Universidad Internacional de Valencia en España durante el 2023, mencionaron que, la seguridad de la información digital debe basarse sobre cuatro aspectos, principios o pilares, los cuales son concebidos como un conjunto de medidas pre establecidas con la finalidad de que las mismas contribuyan a la reducción de los riesgos, así también como de las amenazas, y la recuperación de los sistemas informáticos en caso se presente algún tipo de problema. Estos principios conllevan a un objetivo principal, la protección de datos e información dentro de entidades tanto públicas como privadas, y estas son:

- **Confidencialidad:**

  Este aspecto asegura que la información que se encuentra almacenada dentro de los sistemas informáticos solo puede accederse mediante por el usuario o en todo caso por en la entidad pública o privada que maneja la información, pero a través de una autorización la cual es otorgada por el usuario.

  Por lo tanto, al ser manejada por terceras personas, es necesario que el titular

tome algunas medidas de seguridad, como es el control de acceso físico (es decir, a las instalaciones físicas donde se almacena la información), el control lógico (a través de los famosos “inicios de sesión” o esquemas de permisos las cuales deben estar debidamente protegidos), y finalmente, tenemos a los cifrados como última medida de seguridad, con la cual, el acceso a la información será únicamente para aquellas personas que cuenten con los permisos previamente establecidos.

Cabe resaltar que estas medidas de seguridad, son de gran importancia, y deben aplicarse debidamente pues se debe recordar que se está hablando de masas de información personal de millones de personas, los cuales viajan a través de la red y sistemas operativos, los cuales hacen más vulnerable a una posible alteración.

- **Disponibilidad:**

La información que se encuentra almacenada debe ser estar siempre disponible al usuario, por lo tanto, las entidades deben implementar constantes estrategias que permitan que el usuario sienta plena confianza.

Dentro de estrategias podemos encontrar a: la elaboración de discos los cuales almacenen la información, las copias de seguridad, el balanceo de carga entre las máquinas y los sistemas que permitan el fácil acceso a la información, las ubicaciones de las instalaciones tanto externas como internas de la entidad, la implementación adicional de sistemas informativos como el desarrollo de sistemas RAID de discos. A pesar de ello, las posibles amenazas de ataques cibernéticos o hackeos sigue en pie, por lo tanto, es común que las empresas siempre cuenten con un área de informática y expertos en ciberseguridad, más aún cuando son empresas que cuentan millones de datos, como son el caso de las entidades bancarias.

- **Autenticación:**

Esta medida de seguridad no solo se viene implementando en empresas, sino que también diversos gobiernos lo vienen incluyendo para proteger la información pública.

Tal y como su nombre lo indica, la autenticación se trata de autenticar la identidad tanto del servidor que administra la información, así como la del usuario. Si llevamos esto a la práctica, pongamos otra vez la situación de las tarjetas de

crédito. Si una persona pierde su tarjeta, ¿Qué hace? Acude al centro bancario para anular la tarjeta que perdió y sacar una nueva, pero, ¿Cómo sabe la empresa que la persona que solicita la tarjeta es verdaderamente el dueño o el titular de la misma? Existe la posibilidad de que esta persona no sea el titular, sino que sea un delincuente que se hace pasar por otro con la finalidad de obtener la información personal del usuario, entonces para esto, es que la entidad de ver en la necesidad de hacer emplear el método de autenticación o también denominada como validación de identidad, y ¿Cómo se hace esto? Pues sencillo, a través de huellas digitales, preguntas de las cuales solo el usuario conoce las respuestas, los datos del usuario y contraseñas de inicio de sesión en las cuentas, etc.

A pesar de esto, hay dos métodos de autentificación que son pocos reconocidas pero que, su uso es cada vez mayor, son el token y los certificados digitales. El token es considerado por la Universidad de Valencia como un método especial de autenticación y se basa en las solicitudes que se alcanzan a través de la presentación de una determinada información firmada, en pocas palabras, funciona como una tarjeta de embarque cuando uno se sube al avión. Por otro lado, los certificados digitales, a diferencia de los primeros, son documentos virtuales, los cuales tienen como finalidad demostrar la propiedad de una clave que solo el usuario verdadero lo sabe. Además, incluye también el reconocimiento de la firma electrónica del usuario y son usados más

por los gobiernos como el de España.

- **Integridad:**

Se concibe a la integridad como la máxima garantía de exactitud y fiabilidad de los datos que se encuentran almacenados dentro de los sistemas operativos de las entidades. Por lo tanto, para conseguir una información íntegra, es necesario que el usuario limite lo permisos sobre los datos que este desea proteger, y para ello, es que las empresas tienden a aplicar técnicas de informática más avanzadas como el desarrollo de algoritmos para que lo datos que se encuentran almacenados no se modifiquen bajo ninguna circunstancia, la demostración de sistemas ante el usuario de que la información no ha sido manipulada sin autorización, la firma digital de toda la documentación, etc.

A pesar de esto, debido a la calidad o importancia de la información que se encuentra almacenada, es muchos usuarios se aseguran a través de otros medios que los mismos no hayan sido manipulados, perdidos, o destruidos, ni accidental ni intencionalmente por la compañía.

Por todas estas razones es importante entender, que la seguridad de la información de la información digital se ha convertido un elemento de suma relevancia y fundamental. Pues, a través de esta, se avala la protección de los datos las cuales son pertenecientes a los usuarios pero que incumbe a todas las entidades, tanto públicas como privadas que usan, disponen y desarrollan esta información para el desarrollo de sus actividades, por lo tanto, toda vez que signifique su uso para fines contrarios, provoca la destrucción, alteración o intromisión no autorizada, se afecta directamente a cada uno de los usuarios, a su derecho de privacidad, generando que se pierda la confianza en las mismas. (Chávez, 2018, p.36)

***a. Amenazas a la seguridad de la información***

Teniendo en cuenta la relevancia de la seguridad de la información digital en el mundo social para los delitos informáticos, es que podemos indicar que, ante la falta de buenos mecanismos para la seguridad, es que la información se ve envuelta por algunas amenazas. Es así que, a través de una revista publicada por el Gobierno peruano titulada *"Seguridad y confianza digital"* se entiende que, las amenazas son conceptualizadas como problemas potenciales a la seguridad del activo (información, hardware o software, datos) la cual no se puede controlar directamente. En pocas palabras, esto puede traducirse cuando una persona con fines contrarios al conocimiento y buen desarrollo de la información digital, ingresa a los servidores informáticos, extrae la información con el fin de alterar o dañarlo, o en todo caso, hacer uso malintencionado de las mismas.

Dentro de esta misma línea, y de acuerdo lo sustentado por esta revista del Gobierno peruano, se tiene que las principales amenazas de la seguridad de la información digital son las siguientes:

- **Phishing:** Lo conciben como el ciberdelito más recurrente no solo a nivel nacional, sino también internacional; y consiste básicamente, en el engaño hacia el usuario a través correos electrónicos o e-mails, en donde el ciberdelincuente se hace pasar por un personal de alguna empresa cualquiera con la finalidad de que la primera le revele su información bancaria.
- **Smishing (SMS):** Este es un tipo de phishing, funciona con la misma modalidad y finalidad, sin embargo, a diferencia de este, el Smishing se caracteriza por el uso de mensajes de texto para cometer el acto ilícito, y no de correos electrónicos.
- **Ingeniería Social:** Este delito se diferencia de otros por consistir en el ciberdelincuente se gana la confianza del usuario con la finalidad de que este

último ejecute programas maliciosos para el sistema informativo, instalar un malware, así también como robar información o facilitar claves privadas. Además se caracteriza por el uso de ciertas técnicas, dentro las cuales podemos rescatar al Pretexting (en donde el ciberdelincuente a través de la confianza consigue que el usuario le permita el acceso a sus ordenadores), el Tailgating (en donde el atacante logra evadir controles, puertas electrónicas, así también como el ingresos a ciertos espacios sin autorización alguna), Dumpster diving o también conocido como Trashing (de la cual el acceso a la información se obtiene a través de la "basura digital" del usuario), también se tiene el Shoulder surfing (la cual consiste en espiar al usuario para saber sus contraseñas), Baiting (en donde el delincuente le otorga un dispositivo con software malicioso o un virus el cual le permita obtener información del usuario) y finalmente, está el Vishing (el cual se caracteriza porque el atacante llama de manera directa al usuario, y a través de la intimidación, obtiene la información que lo beneficia.

- **Malware:** Aunque a veces es mal entiendo como los virus, en realidad es un tipo de software que se instala dentro de un ordenador, afectándola a través del uso de la red. Los malware son de diferentes tipos, dentro de las cuales encontramos a los virus, el gusano informático, troyano, spyware, adware, ransomware.
- **Suplantación de identidad:** Tal y como su nombre lo indica, el ciberdelincuente se hace pasar por otra persona a través del uso del Internet, ya sea creándose perfiles falsos o mediante la creación de correos electrónicos.

A pesar de ello, estos tipos de amenazas que se presentan en el territorio

peruano, estas no se desarrollan en la misma intensidad en otros países, por lo que establecer una lista con las amenazas más frecuentes a nivel mundial es casi imposible, sin embargo, lo que sí es factible es mostrar las amenazas que considera cada país (sobre todo de aquellos que en donde los delitos informáticos son más comunes) a través de diversos estudios de investigación. En esa línea, tenemos entonces a la Thompson (2024) pues a través de un artículo publicado para la Universidad Veracruzana, manifiesta que las siete amenazas más potentes en ciberseguridad que afectan a los ciudadanos de México son:

- **La ignorancia:** Este es el mayor problema que presenta la población, y no solo en México, sino que también a nivel mundial, pues es común encontrar a miles de usuarios que descargan distintas aplicaciones sin saber o conocer que estos pueden contener algún tipo de malware lo cual genera algún tipo de infección en el dispositivo, o en todo caso, exigen a los usuarios al registrarse información la cual no es necesaria para dichos aplicativos, como el registro de información bancaria.
- **Los malware:** De los cuales, el tipo más común para cometer delitos informáticos son los virus, a través de los cuales, los hackers se apoderan de todos los sistemas informáticos de los ordenadores, todo esto con la finalidad de obtener las contraseñas y los movimientos que realizan los usuarios.
- **El phishing:** A través de esta técnica, los delincuentes crean las cuentas falsas con información que pareciera ser de alguna entidad legal, lo cual les facilitará tener la información del usuario, para posteriormente cometer fraudes electrónicos.
- **Los Spam – Correos no deseados:** Según la Universidad la cual publicó el artículo, mencionan que el 99.9% de los correos no deseados equivale

correos basura, inclusive, la mayoría de estos, contiene al menos un enlace o archivo que al momento de ser descargado por el usuario, es que se descargan automáticamente ciertos virus.

- **Las Redes inalámbricas inseguras:** Esto sucede con los servicios de línea telefónica o de Internet, los cuales contienen claves o sistemas informáticos de baja protección. En primero, las claves, según un estudio realizado por la Universidad Veracruzana, el 50% de las claves de líneas son: 123456789, 987654321 o secuencias de numéricas muy comunes, los cuales facilita que cualquier persona hasta con pocos conocimientos de informática acceda fácilmente a las redes, rompiendo reglas de seguridad de información con baja protección.
- **Datos perdidos:** Esto se cuándo los sistemas informáticos los cuales almacenan información digital no tienen contraseñas se seguridad, como son el caso de los ordenadores, donde generalmente se guardan datos personales, archivos, fotos, hasta datos de tarjetas bancarias.
- **Ataques por Wi-Fi:** Los ataques de hackeo son más frecuentes cuando las personas acceden a zonas de Wi – fi otorgada a masas de población, como son los casos de los Wi-fi en los aeropuertos, en los centros comerciales, cibercafés, compañías privadas, etc.

De esto podemos entender que, si bien los malware, y el phishing son unos de los grandes problemas que amenaza a tanto al territorio peruano como mexicano, lo cierto es que, para cada gobierno, las amenazas con respecto a la ciberseguridad pueden ser ordenadas o clasificadas de manera diferente, a pesar de ello, eso quita de que cada uno de ellos trabaje diariamente de la mano con sus organismos tanto públicos como privados, con la única finalidad de salvaguardar la seguridad de la información que se

encuentra en línea para cada uno de los usuarios.

### *2.1.3. Normativa Internacional sobre la Información digital*

Debido a que la era digital viene siendo un tema boom en los últimos años y más con respecto a la información digital, garantizando la protección de los mismos, la privacidad de los usuarios y la calidad de los sistemas informáticos frente a las posibles amenazas como la concurrencia de los delitos informáticos a gran nivel, que organismos internacionales a nivel mundial se han visto en la necesidad de pronunciarse sobre este tema a través de un enfoque colaborativo y normativo con la finalidad de establecer directrices clara, las cuales favorezcan la seguridad cibernética a nivel global. Es así, que, dentro de estos, podemos rescatar a la Organización de las Naciones Unidas y la Unión Europea, las cuales han desarrollado un rol esencial para la formulación de políticas y estrategias que buscan fortalecer la seguridad digital y reducir el impacto de los delitos informáticos.

#### a. La ONU y su recomendación sobre la Seguridad de la Información digital

A través de una de las revistas publicadas por la Organización de las Naciones Unidas (en adelante ONU) titulada “Normas internacionales relativas a la privacidad digital” es que ha mostrado su postura con respecto a la seguridad de la información digital, manifestando que este derecho se fundamenta en la importancia de garantizar otros los cuales se encuentran directamente relacionados con el entorno digital. Dentro de estos, encontramos al derecho de la privacidad, la cual según la ONU sería el base cuando se trata de la seguridad de la información, y más aún cuando este derecho está relacionado con otros derechos como la liberta de expresión, la libertad de asociación y de reunión hasta el acceso y el disfrute de los derechos económicos.

Por tal razón, es que se resalta paralelamente la Declaración de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos, pues dentro de sus

arts. 12 y 17 respectivamente es que establece que ninguna persona tiene que ser objeto de injerencias arbitrarias o ilegales en todas las esferas que incluye su desarrollo, como su vida privada, su familia, su vivienda o su correspondencia, ni de ataques a su honra y reputación, y por tal razón, es necesario su protección

legal ante tales actos, y con más razón dentro de esfera virtual, pues ahí en donde radican la mayor cantidad de amenazas.

En ese sentido, es que la ONU mediante su Asamblea general y su Consejo de Derechos Humanos, a partir del 2013 han aprobado diversas resoluciones vinculadas con el derecho a la privacidad en la era digital. Dentro de las cuales podemos resaltar a la resolución A/HRC/RES/42/15. De esta última se puede rescatar que cada uno de los Estados deben implementar mecanismos y desarrollar estrategias que se dediquen exclusivamente a la protección del derecho de la privacidad de las personas, los cuales deben extenderse hasta el ámbito virtual o digital, y además, esta debe respetar los principios de legalidad, necesidad y proporcionalidad, desarrollando al máximo las herramientas tecnológicas, como son la Inteligencia artificial, con la finalidad de que el usuario disfrute de su derechos sin sentir miedo a una posible amenaza o vulnerabilidad.

Por otro lado, también se ha pronunciado con respecto a la seguridad digital, promoviendo ciertos consejos relacionados con la comisión de delitos informáticos, como son el caso del cuidado cuando una persona navega en Internet, sobre todo cuando quiere descargar alguna foto, video, archivo, documento, pues estas propensas a que infecte el servidor. De igual manera, indica la protección de los servidores de internet con sistemas de seguridad confiables, partiendo desde las contraseñas, recomendando la no utilización de contraseñas comunes, convirtiéndolas en una barrera fácil de sobrepasar hasta por un adolescente, y generando que los ciberdelincuentes accedan a información y datos personales, y finalmente, rescata la importancia de no contestar o

descargar algún dato proveniente de correos spam, mensajes de texto, así también como proporcionar datos de gran relevancia a través de llamadas telefónicas, pues tranquilamente puede ser una persona haciéndose pasar por otro, lo que genera que el phishing se convierta en uno de los delitos informáticos más frecuentes, y uno de los mecanismos más fácil para robar información. Por esta razón, es de suma importancia, que los Estados pongan su foco de atención en la esfera digital, desarrollando una mayor seguridad, con la finalidad de que millones de usuarios se sientan seguros dentro de la esfera digital.

Es así que podemos que concluir que, la ONU ha reconocido la ciberseguridad como una prioridad global, desarrollando estrategias y emitido resoluciones que buscan una cooperación internacional efectiva con la finalidad de combatir los delitos informáticos y proteger la infraestructura crítica a nivel mundial.

**b. La Unión Europea y la Información digital**

Debido a las ciberamenazas constantes y el desarrollo masivo de los delitos informáticos, es que la Unión Europea (UE) ha puesto en vigencia la Estrategia de Ciberseguridad, esto debido a que, con el avance de la tecnología, y la dependencia de todos los sectores, en especial el de finanzas, administración y economía; en la misma, es que delitos informáticos son cada vez más frecuentes, tratando de dar una postura sólida a los ciudadanos, generando en estos últimos, confianza en las herramientas y servicios digitales.

La UE inició la lucha contra los delitos digitales en el 2016 cuando el Consejo General de esta organización, mediante un acuerdo con los ministros de Justicia

de todos los países integrados, iniciaron debate sobre los puntos críticos de la ciberdelincuencia, teniendo como resultado medidas de cooperación entre los países miembros, así también como la puesta en marcha de acciones de supervisión, control,

y recolección de datos con respecto a esta problemática, esto a través de la implementación de la Directiva NIS o también conocida por otros como al Directiva SRI, la cual está conformada por el Parlamento Europeo, así también por el Consejo de la Unión Europea, pero pese a que su propuesta se dio a finales del 2016, esta entró en vigencia pasando mediados del 2017.

La Directiva NIS es considerada como la primera entidad legisladora sobre la seguridad de redes y sistemas de la información que surgió como respuesta inmediata a los ataques a la ciberseguridad, además, como respuesta a su rápida labor, es que pocos meses después, crearon el Equipo de Respuesta a Emergencias Informáticas (CERT-UE) destinada a dar respuesta inmediata y coordinada entre las instituciones a cargo frente a la presencia de los ciber ataques, a pesar de ello, su alcance para los ciberataques se limitaba a las empresas que se desempeñaban dentro de infraestructuras críticas.

Para el 2018, el SRI puso en vigencia el Reglamento General de Protección de Datos (también denominado como RGPD), destinado al establecimiento de recopilación, procesamiento, y almacenamiento de todos los datos personales de los usuarios en línea. Paralelamente, establecía lo derechos de los usuarios sobre el uso y la posesión de sus datos en cualquier momento, los cuales debían ser proveídos por las entidades de manera rápida y adecuada. Y finalmente, con respecto a estos últimos, con las entidades, se les establecía su responsabilidad de

ofrecer los datos de información de manera transparente y de fácil acceso para los usuarios. La finalidad principal de este reglamento, además de proteger los datos digitales, era modernizar y unificar las normas para que las empresas reduzcan su burocracia con respecto al desarrollo de sus actividades, lo cual, a su vez, permitía a las personas que tengan un control más directo sobre sus datos personales.

Posteriormente, para el segundo trimestre del 2019 es que la UE adopta una

Agencia para la Ciberseguridad (o lo que por otros es más conocido por sus siglas ENISA), en donde las autoridades estaban facultadas de imponer sanciones a todos aquellos que se encuentren responsables o culpables de atentar contra la seguridad de la información digital, pero no estos, sino también la sanción a todos aquella personas naturales o jurídicas que prestaban ayuda económica, tecnológico o material, así también a todos los que se encuentren conexos a la comisión del acto ilícito vulnerando la seguridad de la información digital. Cabe resaltar que esta facultad de ejercer su función sancionadora propia de la UE no solo se aplicaba para aquellos países miembros, sino también para aquellos que no eran pertenecientes a la misma.

Por otro lado, durante el mismo año se aprobó el Reglamento sobre Ciberseguridad, la cual trajo consigo un Sistema de Certificación para todos los países de la Unión Europea, teniendo esta última como finalidad de actuar como garantía con respecto a los derechos cuando se produzcan los ataques, así también como las normas en materia de ciberseguridad, otorgando a todos los usuarios confianza, incentivando el crecimiento del mercado de la ciberseguridad, y paralelamente, facilitando el comercio dentro de Europa.

Para el 2022, la Directiva NIS fue “actualizada” por la Directiva NIS 2 o como otro suelen conocerlo, por la SRI 2, con la finalidad de crear un nuevo entorno de ciberseguridad igual para todos los Estados que son miembros, protegiendo de forma más igualitaria a la infraestructura digital, ampliando su alcance de labor a diversos sectores incluyendo no solo empresas en situaciones críticas, sino también abarcando empresas que se consideraban esenciales dentro de la economía europea, así como empresas grandes. Ello conllevaba a aplicación de multas y medidas coercitivas más estrictas, así también como una supervisión más amplia y enfocada en áreas mínimas, incluyendo inspecciones hasta el uso de auditorías sobre el desempeño de las empresas.

La última actuación de la UE con respecto a la ciberseguridad es la implementación del Reglamento de la Cibersolidaridad en diciembre del 2024, recordando a los Estados miembros sobre la crisis digital y apoyando en las respuestas inmediatas ante los ataques, reforzando los mecanismos de cooperación entre ellos, tomando conciencia de las amenazas de ciberseguridad, así también como apoyar continuamente con la seguridad de la protección de información digital en entidades y servicios.

De acuerdo a las líneas anterior, es que podemos indicar que la UE por su parte, ha implementado diversas iniciativas normativas, como el Reglamento General de Protección de Datos (GDPR), así también como la Directiva NIS, las cuales buscan crean un entorno seguro para desarrollo del manejo de la información digital dentro de los países miembros.

### *2.1.4. Delitos Informáticos*

En la actualidad, el constante desarrollo y la implementación de nuevas tecnologías de información y comunicación (lo que comúnmente se conoce como TIC´s) ha transformado rápidamente diversos sectores, haciendo que muchos de ellos en la actualidad, dependan de ello. De igual manera, no cabe duda alguna que el constante uso del Internet, no solo a nivel nacional sino también internacional por millones de personas, hace que el intercambio de información por minuto sea impresionante, no solo entre usuarios sino también a nivel de la informática, lo que aparentemente es beneficioso para la sociedad. A pesar de ello, siempre hay terceros que buscan aprovecharse de estos intercambios masivos de información los cuales generalmente no se encuentran protegidos, y no solo de estos, sino también de aquellos que se encuentran sumamente protegidos y almacenados en sistemas informáticos a nivel mundial, lo que deja a la presencia de ciertas amenazas, significando una puerta abierta a las fechorías de

los ciberdelincuentes.

Es así que, para Urdanegui (2024), los delitos informáticos son concebidos como aquella conducta ilícita ejercida por un ciberdelincuente, esto quiere decir que el delincuente utiliza programas informáticos, la instalación de virus, la suplantación de identidad mediante el uso de los sitios web o redes sociales, con la finalidad de cometer delitos, los cuales debido a los mecanismos que empleados es que denomina delitos informáticos. (p.12)

De igual manera para Acosta, Benavides y García (2020) esta categoría de delitos se diferencia de los delitos tradicionales por el uso avanzado e ilegal de la tecnología, violando la seguridad de la información de millones de usuarios en línea con la finalidad de extraerles

los datos personales almacenados en redes informáticas, para posteriormente, usarlos para su propio beneficio.

Por otro lado, Chávez (2018) añade que, en la comisión de los delitos informáticos, se puede identificar a las partes, teniendo en primera al sujeto activo, quien vendría a ser el ciberdelincuente, aquella persona que tenga altos conocimientos sobre informática. Por otro lado, se tiene al sujeto pasivo, si bien podría identificarse con la víctima, en realidad son los datos y los sistemas informáticos, los cuales son concebidos como el conjunto de información y datos cuyo titular radica en una persona natural o jurídica, y finalmente, se tiene al bien jurídico protegido, el cual vendría a ser la información que se encuentra almacenada y posee un carácter económico para su titular, la que posteriormente, después de su robo sistemático, será tratada y trasmitida hacia terceros. (p.49)

A partir de las líneas anteriores, se entiende que, los delitos informáticos significan una problemática para los derechos humanos y fundamentales, por lo tanto, es necesario que, los Estados pongan en marcha políticas nacionales, convenios o asociaciones estratégicas con otros países, que permitan que una lucha constante contra la ciberdelincuencia.

### a. La convención de Budapest sobre el Cibercrimen

Debido a los constantes ataques a la seguridad de la información, es que varios países se han visto en la necesidad de hacer un esfuerzo internacional para encarar este problema, es así como nació el Convenio Budapest. (Acosta, Benavides y García, 2020)

El Convenio de Budapest o también conocido como el Convenio de Ciberdelincuencia fue firmado en el 2001 en Hungría, a pesar de esto, dicho tratado

internacional entró en vigencia en 2004. Su importancia radica en ser el primer tratado internacional destinado a hacer frente a los delitos informáticos a través de leyes, técnicas de investigación y la constante cooperación internacional, y sobre en Latinoamérica, pues más de 18 países han ratificado dicho convenio.

En concordancia con lo anterior, tenemos a Delgado (2022) quien manifiesta que, la Convención de Budapest es el reflejo de la primera lucha oficial contra la ciberdelincuencia legal, debido a que la misma, engloba una gran cantidad de delitos informáticos e infracciones contra los sistemas de red, los datos, el patrimonio y la fe pública, la impunidad, la libertad sexual e intimidad, así como el secreto de las comunicaciones. Pero no se estanca ahí, sino que también prevé un marco legal general, el cual incluye las responsabilidades de los sujetos (personas naturales o jurídicas), así como las sanciones las cuales se encuentran destinadas a cada uno de los gobiernos que se encuentran suscritos, constituyéndose así, como un estándar universal en el área de la informática. (p.10-11)

Ahora bien, la tipificación establecida dentro de la normativa sobre los delitos es bastante amplia, sin embargo, se puede mencionar a: el Fraude informático (dentro de su ar. 8), los delitos relacionados con el contenido, como es el caso de la pornografía infantil (art.9) y la propiedad intelectual (como es el caso de los delitos vinculados a los derechos de autor. También se encuentran los delitos que van en contra de la confidencialidad, la integridad, así como la disponibilidad de los datos y sistemas

informáticos, dentro de la cual se puede encontrar a las interferencias de los datos, los daños que están puedan sufrir, como su eliminación, deterioro o modificación, incluyendo también, el abuso de los dispositivos.

Por otra parte, se caracteriza por incluir puntos importantes para determinar la responsabilidad penal de los culpables, como el sistema de extradición y la jurisdicción y competencia de los organismos jurisdiccionales. Todo ello, demuestra que el Convenio de Budapest trae consigo grandes oportunidades para los Estados miembros que dieron su consentimiento para formar parte de este proyecto, como, por ejemplo; aplicar una política penal general o común en todos los países, complementar sus legislaciones o normativas previamente establecidas, compartir tecnología de información, así como el uso igualitario de herramientas con finalidad de combatir a la ciberdelincuencia. (Tenorio, p.75, 2018).

En Latinoamérica, de acuerdo a lo planteado por Tenorio (2018), es que CEPAL (Comisión Económica para América Latina y el Caribe) mediante su agenda digital, la cual es elaborada por y para sus miembros, es que influye directamente al desarrollo de mecanismos nacionales para frenar la ciberdelincuencia, no dejando de lado las legislaciones vigentes destinadas a la seguridad de la información digital.

Para el caso peruano, Delgado (2022) resalta que, el ex presidente ha ratificado la Convención en el 2019 mediante el Decreto Supremo 010-2019-RE, debido a que esta, representa un beneficio a los intereses de nuestro país, fortaleciendo lo que se encuentra plasmado en los Arts. 56 y 118 inciso 11 de nuestra Carta Magna, así como la Ley N° 26647 en su Art.2. (p.15)

A partir de la línea anterior es que podemos concluir que, el Perú, así como distintos países de América Latina y del mundo se sumergen por los lineamientos establecidos por el Convenio de Budapest contra la ciberdelincuencia, aunque, si

bien estos lineamientos son pautas generales de aplicación, lo importante aquí es la cooperación internacional que, para el 2001 significó una respuesta rápida ante la aparición de lo que hoy denominamos como delitos informáticos.

### *2.1.5. Los desafíos en la Tipificación y sanción de los Delitos informáticos en el Derecho Penal peruano*

El Estado peruano, a nivel de Latinoamérica, fue uno de los primeros en añadir a sus legislaciones temas de seguridad de información digital, esto a través de una legislación que incorporaba dentro de sus términos legales a los "delitos informáticos". (Tenorio, p.73, 2018)

Ahora bien, antes de la puesta en vigencia de la actual ley que regula los delitos informáticos resulta de gran relevancia resaltar que, dentro de nuestro Código Penal de 1991, únicamente en su inicio, se tipificaba el delito informático (art. 186, inciso 3) como agravante del delito de hurto (lo que nos da a entender que este no era un delito autónomo sino era dependiente de otro), sin embargo, no fue hasta años después en donde se incorporaron otros delitos informáticos, como es el caso de la Interferencia, el acceso o copia ilícita de datos (la cual se encontraba tipificada dentro del Art. 207-A), el Daño, alteración o destrucción de base de Datos (mediante el Art. 207-B), las Circunstancias cualificadas agravantes, esto a través del Art. 207-C, y finalmente por medio del Art. 207-B se regulaba el Tráfico Ilegal de Datos.

Ahora bien, a partir del 2013, fecha en la que se incorpora la Ley 30096 o más conocida como la Ley de los delitos informáticos, es que se empiezan a tipificar diversos delitos informáticos, lo cual trajo consigo la derogación de los Arts. que se encontraban en el Código Penal. Dentro de estos delitos informáticos, los podemos categorizar de la siguiente manera:

- Capítulo I - Delitos contra datos y sistemas informáticos: Dentro de la cual encontramos los delitos de Acceso ilícito y Atentado a la integridad de datos

informáticos.

- Capítulo II - Delitos informáticos contra la indemnidad y libertad sexual: Dentro de la cual encontramos las Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.
- Capítulo III - Delitos informáticos contra la intimidad y el secreto de las comunicaciones: A través de este capítulo encontramos el delito de Tráfico ilegal de datos y la Interceptación de datos informáticos.
- Capítulo IV - Delitos informáticos contra el Patrimonio: En esta sección encontramos el delito de Fraude informático.
- Capítulo V - Delitos informáticos contra la fe pública: Dentro de la cual encontramos el delito de Suplantación de Identidad.

Además de esto, dentro de su capítulo VII el cual se titula Disposiciones Comunes, encontramos algunos complementarios a los delitos informáticos como es el caso del abuso de mecanismos y dispositivos informáticos, las agravantes (con respecto a las penas privativas de libertad), la exención de la responsabilidad penal. Así mismo, también se señala la codificación de la pornografía infantil, se trata la labor de los agentes encubiertos, así como su capacitación, y finalmente, la coordinación que debe haber entre la Policía Nacional del Perú (PNP) con el Ministerio Público.

Un año después de su promulgación, es que entró en vigencia la Ley 30171, la Ley que modifica la Ley 30096, y ¿Esto por qué? Pues la idea principal era incorporar a la Ley 30096 los lineamientos establecidos por el Convenio de Budapest sobre la ciberdelincuencia. Ahora bien, de acuerdo a Tenorio (2018) la legislación peruana supera por lejos al Convenio de Budapest pues, dentro del marco legal peruano se consideran elementos que sirven de base para determinar el delito informático, como es el caso de la responsabilidad penal. A pesar de ello, a nuestro criterio, podemos determinar que, sin la modificatoria a la Ley 30096 no hubiera sido

posible incorporar algunas definiciones básicas, como es el caso de los delitos informáticos, es decir, dentro de la Ley 30096 no se encontraba definido el término “delitos informáticos”, lo que era factible en todo caso, era sacar una definición de ello a base de la comprensión del objeto de la Ley.

Esto último hace evidencia de otros de los desafíos con respecto a la tipificación de los delitos, los vacíos legales en la norma y más, al tratarse de una sola norma que este enfocada al 100% en este tema. Es cierto que hay otras normas vinculadas al tema de los ciberdelitos, como la Ley que Incorpora diversos artículos al Código Penal Relativos a la seguridad en los centros de detención o reclusión, la Ley de protección de datos personales, la Ley de vigilancia Electrónica Procesal, la Ley que regula el uso del Correo comercial no Solicitad (SPAM), entre otros. A pesar de ello, lo ideal es que estén netamente enfocados en el tema, como es el caso del Código Penal y Procesal penal, lo recomendable es que haya secciones completas enfocadas en los delitos informáticos, sin embargo, solo son artículos. Lo mismo sucede con la Ley de protección de datos personales, lo que a primera instancia nos indicaría la protección de los datos tanto de personas jurídicas como naturales, sin embargo, se enfoca al tratamiento y el uso de los datos por parte de los bancos de datos, y en ninguna sección hablan de delitos informáticos, más solo de infracciones, lo que indica la gran cantidad de vacíos por sanear.

La legislación peruana sobre los delitos informáticos se resume a una, a la ley 30096 o a su modificatoria, la ley 30171, pero sigue siendo una sola legislación. Ahora bien, por otro lado, la ley modificatoria no es que este completa, sino que abunda los vacíos legales, como por ejemplos las sanciones, cada delito debería estar sancionado al igual que el Código Penal, sin embargo, la ley, habla de manera general de las sanciones a imponerse. Es de aquí en donde parte otro desafío, la falta de complementariedad legal con respecto al Código Penal. Desde nuestro punto de vista, creemos que los delitos que encontraban en este documento no deberían haberse derogado, al contrario, la Ley 30096 debería haber complementado los vacíos que se

presentaban en el código al igual que sucede con otros delitos que se encuentran complementados en otras normas o leyes, debería haberse presentado una complementariedad y no una derogación.

Aunado a esto, no sería de extrañar que esta fuera el desafío a superar, las normas partes son un reflejo de la opinión de las autoridades que "consideran que es mejor para la sociedad", sin embargo, sabemos que, en nuestra actualidad, la gran mayoría de estos no están calificados en temas que afectan a nivel mundial. Por esta razón, en concordancia con lo anterior, tenemos a Segrera y Cano (2020) pues para ellos, los delitos informáticos se han convertido en uno de los mayores dolores de cabeza del sistema judicial peruano debido a que, las autoridades no son lo suficientemente capaces, y esto se debe precisamente a eso, a la falta de capacitación que es responsabilidad del Estado, lo que, a grandes rasgos, genera que no todas las autoridades correspondientes tengan los conocimientos necesarios para actuar en este tipo de situaciones, y los que tienen conocimientos, pues lamentablemente son

demasiados básicos, lo que termina siendo un reflejo de un gran desafío para la actuación de las autoridades a esta problemática. (p.222)

### *2.1.6. La relación de la Seguridad de la Información digital con los Delitos informáticos*

En líneas anteriores se había determinado a la seguridad de la información digital como el mecanismo para evaluar los riesgos y las amenazas a través de estrategias, planes tecnológicos, o hasta normas que permitan la máxima protección de la información y/o datos con la finalidad de elevar o mantener la confianza de los usuarios en las entidades tanto públicas como privadas que almacenan los datos personales en sistemas informáticos.

Por otro lado, se tiene a los delitos informáticos, los cuales se consideran como toda aquella conducta ilícita que se caracterizar por sobre pasar las barreras de la seguridad de la información digital con la finalidad de obtener datos personales de usuarios, para

posteriormente usarlos a su conveniencia, esto último mediante la puesta en práctica de los medios electrónicos o informáticos.

A partir de esto, es que tomamos importancia a la seguridad de la información digital para evitar la presencia de los delitos informáticos. Ahora bien, con respecto a esto, es de gran relevancia entender cómo es que las entidades públicas y privadas manejan sus mecanismos, estrategias, y normativas para proteger la información.

Es así que, dentro del caso peruano, podemos mencionar que, de acuerdo a una revista publicada por el Estado peruano titulada "Seguridad y confianza digital", la seguridad de la información pública se encuentra a sujeta al Centro Nacional de Seguridad Digital (SNSD), el cual se encuentra relacionado a la Presidencia del Consejo de ministros a través de la

Secretaría de Gobierno y Transformación digital (SGTD). El CNSD tiene como responsabilidad principal el gestionar, dirigir, articular, supervisar y detectar las amenazas, así como las operaciones de movimiento y protección de la información. Así mismo, tiene a su cargo fomentar la colaboración y cooperación con otros organismos para la seguridad digital, todo esto con la finalidad de fortalecer la confianza de los usuarios.

Ahora bien, dentro de esta cooperación internacional es que podemos resaltar a otra normativa que complementa la seguridad de la información digital peruana, como es el caso del ISO 27001 – Sistema de Gestión de Seguridad de la Información, el cual actúa como un estándar internacional que establece los requisitos para la gestión de la seguridad digital, sin olvidar la confidencialidad, integridad, disponibilidad y autenticación de la información. Además, su implementación en la normativa peruana es esencial para identificar los riesgos y amenazas de la información implementado controles de seguridad, asegurando los derechos de acceso a los datos de los usuarios a través de altos mecanismos de identificación con la finalidad de reducir las posibilidades de suplantación de identidad para acceder ilícitamente a la información.

Ahora bien, con respecto a las entidades privadas, en primera, es importante rescatar que, las empresas privadas tienen la posibilidad de acatarse a lo dispuesto por ISO 27001.

Continuando, es vital resaltar la información publicada por la Superintendencia de Banca, Seguros y AFP a través de una de sus revistas titulada “Seguridad de la Información digital y ciberseguridad: nuevo reglamento para promover un entorno seguro y confiable en beneficio de los usuarios de los sistemas supervisados”. Dentro de esta publicación se destaca la publicación de la Res. N°504-2021, la cual aprobó el Reglamento para la Gestión de

seguridad de la información y ciberseguridad, el cual tiene como misión solicitar a las empresas a que cuenten con los mecanismos necesarios para promover confianza a los usuarios sobre sus sistemas informativos, esto, mediante tres niveles de proporcionalidad: 1. Simplificado; el cual incluye las medidas mínimas a la seguridad digital, como es el caso de los reportes con las amenazas a la ciberseguridad, así como los mecanismos de respuesta a los usuarios y recuperación de información en caso de pérdida. 2. Aplicación General; el cual se relaciona a las medidas de autenticación, subcontratación del procesamiento de datos, así como la ciberseguridad, y 3. Reforzado; el cual se caracteriza por las medidas adicionales que quisiesen las empresas añadir, con la finalidad de garantizar la máxima protección de la información, velando por la efectividad del sistema de gestión de seguridad informativa.

Para finalizar, concluimos con la importancia de la seguridad de la información digital como elemento crucial para evitar o disminuir la presencia de los delitos informáticos como el hacking, el phishing o el fraude informático, garantizando la confidencialidad de los datos los cuales son trasmitidos por medios o sistemas digitales.

### *2.1.7. Derecho comparado*

#### 2.1.7.1.España

En este país, la ciberseguridad se ha convertido uno de los temas de mayor

preocupación tanto para el Estado como las empresas españolas, esto debido a que, según el Instituto Nacional de Ciberseguridad (INCIBE) durante el 2022 se reportaron 118 820 denuncias con respecto a delitos informáticos, de los cuales la mayoría eran por ataques informáticos a través de malwares y el phishing, y por esta razón justamente, es que se ha convertido en uno de los países en tener una gran cantidad de normativas y legislaciones con respecto a este tema. Dentro de estas normativas encontramos:

- **La Ley 34/2002, Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico:** el cual se considera como la primera normativa española referente a la ciberseguridad, y se enfocaba únicamente en regular los servicios con respecto a la protección de la información digital.
- **Ley 36/2015 o Ley de fomento de la financiación empresarial:** la cual, de acuerdo a su nombre, se solicita a las empresas que conforman el sector financiero a que implementen mecanismos adecuados que permitan asegurar la seguridad de la información de los usuarios que la conforman.
- **La Estrategia Nacional 2017:** el cual se caracteriza por abarcar pautas para las actuaciones relacionadas a la seguridad nacional, y dentro de ellos se encuentra el área de ciberseguridad, en la cual se establecían los lineamientos a seguir en caso de robo de información o datos de los usuarios, así como su recuperación.
- **La Ley orgánica 3/2018, de Protección de Datos Personales y Garantía de Derechos Digitales:** la cual se resumen en la obligación de las empresas españolas para entablar medidas de seguridad informativa con respecto a los datos personales.
- **Real Decreto-Ley 12/2018, de Seguridad de las redes y sistemas de información:** se caracteriza por la obligatoriedad de las empresas de notificar los incidentes con respecto a sus redes y sistemas de protección de seguridad hacia los usuarios.
- **Reglamento General de Protección de datos (RGDP):** es la principal norma del

Parlamento Europeo con respecto a la ciberseguridad, y de la cual, España la ha adoptado debido a su gran importancia a nivel internacional.

Ahora bien, se hace mención de la implementación de mecanismos para garantizar la protección de los datos, sin embargo, ¿Cuáles son estos mecanismos? Estamos hablando de medidas generales, como en primera, la creación del departamento de Ciberseguridad en cada empresa, lo que no solo implica en la contratación de personal altamente calificado, sino también su capacitación constante. Así mismo, incluye también en la utilización de sistemas de protección eficaces, lo que incluye, el uso de firewalls y antivirus, los cuales permitan la más alta seguridad de la información.

Jurado (2020) asegura que la presencia de los delitos informáticos seguirá creciendo en los próximos años, y a pesar de las normativas y las estrategias implementadas en España, aún siguen significando insuficientes para erradicar o evitar que los altos índices de ciberdelincuencia sigan en aumento, y para ello es necesario fomentar la cooperación internacional, no solo europea sino también a nivel mundial.

**2.1.7.2.México**

Alcalá y Meléndez (2023) a través de un estudio confirman que en el 2017 las autoridades estatales han solicitado la incorporación del Convenio de Budapest a la legislación mexicana, y que, además, durante el 2019 hasta el 2022 se han presentado al menos 15 iniciativas hacia el Congreso para sancionar y tipificar los delitos informáticos, esto debido a que, hasta años anteriores, México no contaba con una norma especializada.

Como resultado de estas iniciativas, y la constante presencia de los delitos informáticos es que, en el 2022 se aprueba la Ley Federal de Ciberseguridad y a, mediados del 2023 se publica oficialmente la Ley. De esta ley, se puede rescatar a la Agencia Nacional de Ciberseguridad, entidad encargada de velar por la seguridad de la información digital, el cual

deberá trabajar de la mano con el Registro Nacional de Incidentes de Ciberseguridad, el Poder Judicial, las Dependencias de la Administración Pública Federal, con la finalidad de establecer los mecanismos y estrategias de acuerdo a la realidad social para limitar la presencia de los delitos informáticos.

De igual manera, a través de la ley, mediante su título cuarto y quinto, se establecen los derechos de los usuarios, así también como las responsabilidades de las entidades almacenadoras de los datos personales, respectivamente.

Y finalmente, a partir de su título octavo, se norman, sancionan y tipifican los delitos informáticos, esto a través de sietes secciones, los cuales están dirigidos a: 1. Los delitos contra la confidencialidad, integridad y disponibilidad; 2. Los delitos contra la integridad del sistema informático; 3. De la interceptación de datos; 4. De la falsificación informática; 5. Del abuso de dispositivos tecnológicos; 6. Del fraude por medio informático; 7. De los delitos contra la integridad y libertad de las personas; 8. De la propiedad intelectual; y finalmente; 9. De los sistemas bancarios, financieros, gubernamentales e infraestructuras críticas de información.

Ahora bien, probablemente, debido a la reciente publicación de esta normativa, es que cuente con diversos vacíos legales que aún faltan por sanear, lo importante es que México se ha sumado a esta lucha contra la ciberdelincuencia.

#### 2.1.7.3.Colombia

Para Álvarez (2023) por medio de su revista “Colombia registró un crecimiento de ataques informáticos en el último año” menciona que, durante el 2022 se registró un total de 54 mil denuncias relacionadas a los delitos informáticos, lo que, a comparación del 2021, se registraba un aumento de más 11 mil casos, de los cuales, los delitos más frecuentes eran el robo de datos mediante ordenadores y teléfonos celulares.

Teniendo en cuenta lo anterior, es necesario rescatar que, Colombia es uno de los países que ha desarrollado normativa vinculante a la ciberseguridad y los delitos informáticos, un

ejemplo claro de esto es la Ley 527 de 1999 (Ley de comercio electrónico) por el cual se reglamentaba el acceso y el uso adecuado de los mensajes de datos, así también como de las firmas electrónicas para el comercio electrónico, es decir, las empresas estaban en la obligación de implementar medidas de seguridad que garantizaran la identidad del usuario al momento que este deseara acceder a su información personal.

De igual manera, se tenía la Ley 599 de 2000, que, si bien no era una ley que se dedicaba a la regulación de los sistemas de seguridad informativa, se tiene que, dentro de Art. 195 se sancionaba con una multa a quien intentara sobrepasar abusivamente los sistemas informáticos protegidos con medidas de seguridad. Por otro lado, se tiene la Circular 052 del 2007 emitido por la Superintendencia a Financiera de Colombia, la cual se encarga de establecer los requisitos mínimos de seguridad de la información digital para usuarios y clientes.

Todo lo anterior, evidencia la preocupación estatal colombiana por la ciberseguridad, sin embargo, a pesar de que hay diferentes leyes, estos no tienen una sección especifica

destinada a la ciberseguridad, si tenían artículos que se preveían ciertas situaciones, lo que demuestra la rápida atención del Estado a esta problemática.

A pesar de ello, no fue hasta el 2009 que entró en vigencia la Ley 1273, ley principal colombiana que regula la protección de información y de los datos, por el cual se modifica el Código Penal colombiano y se tipifican diversos delitos informáticos, entre los cuales tenemos: el acceso abusivo a un sistema informático, la obstaculización ilegítima de sistema informáticos o redes de telecomunicación, la interceptación de datos, el uso de malwares, la violación de datos personales, la suplantación de sitios web, etc.

Es necesario rescatar que, la Ley 1273 se encuentra acompañada de otras legislaciones que se han dedicado a sanear los vacíos legales existentes. Es así, que tenemos en primera a la Ley 1341 del 2009, por la cual se estable la creación de la Agencia Nacional de Espectro para organización de las TIC´s y su protección, y en segunda, tenemos la Resolución de la Comisión

de Regulación de Comunicaciones 2258 de 2009, la cual establece la obligatoriedad de seguridad para las redes y establecimientos de servicios de internet, esto mediante la implementación contraseñas (medidas de autenticación) y marcos de seguridad, con la finalidad de salvaguardar la confidencialidad y la integridad de datos, previniendo posibles ataques de delitos informáticos y garantizando la seguridad de la información digital.

A partir de todo lo establecido, se puede concluir que Colombia, en la actualidad no cuenta con una ley independiente que se dedique a la sanción de los delitos informáticos, es así que el marco normativo para esta problemática se establece mediante su código penal y las demás leyes complementarias que se han tomado en cuenta en esta investigación, como es el caso de la Ley 1273 del 2009, la cual únicamente modifica el código colombiano, y a consecuencia de ello, se aparta dentro de este documento un nuevo bien jurídico protegido "la información y los datos", teniendo como base la tipificación de los delitos informáticos. (Gamba, 2019, p. 118)

### *2.1.8. Impacto de la Seguridad de la Información digital en Lima metropolitana*

El uso constante del Internet y de las TIC´s se ha convertido en una herramienta de dependencia para diversas áreas de actividades en Lima, como las empresariales, financieros, bancarios, educativos, administrativos, entre otros. Todo ello ella conllevado a que, los delitos informáticos se conviertan en dolor de cabeza para las autoridades estatales no solo durante el 2023 sino también durante los últimos 4 años.

Evidencia de esto último tenemos al reporte anual de la Defensoría del Pueblo (2023) y de la mano con los informes de Interpol, se informa que, debido a la pandemia y el uso indiscutible de mecanismos electrónicos, es que durante el 2021 se obtuvieron un total 11 985 denuncias por ciberdelitos, de las cuales 70% de estas denuncias, correspondía al fraude informático. (p.6)

Además, mediante las cifras emitidas en el Diario El Peruano (2023), se ha reportado que, durante el primer trimestre del 2022 las denuncias por ciberdelincuencia alcanzaron los 3946 casos, de las cuales, 2382 fueron por fraude informático, convirtiéndolo en la denuncia más recibida. Por otro lado, para el 2023, mediante un informe de la Divindat (División de Investigación de delitos de alta tecnología) se reportó que, cada mes, se reciben al menos 300 denuncias vinculadas a los delitos informáticos, de los cuales, hasta la fecha, el phishing se cataloga como la modalidad más denunciada.

De igual manera, a través de un informe por el Instituto de Defensa legal (2023) se informa que el número total de los ciberdelitos registrados en Lima Metropolitana entre enero y junio del 2023 alcanzaron las 154 791 denuncias, lo que representa un aumento de más de 61 mil delitos más a comparación del 2022, de los cuales, San Juan de Lurigancho se convierte en la zona con mayor cantidad de denuncias presentadas durante los últimos dos años, seguidos de Los Olivos e Independencia.

A partir de todos los datos anteriores, se puede deducir que, en la actualidad, la sociedad limeña padece de la protección de la información digital, lo cual es esencial para que prevalezcan los derechos y libertadas humanas.

Ahora bien, Lima Metropolitana como tal, se encuentran exhibido al constante uso y exposición del internet, lo que traduce en la presencia de constantes peligros de robo de información, y si bien, el Estado peruano ha puesto en marcha la lucha contra la ciberdelincuencia mediante la vigencia de la Ley 30096, lo cierto es que, esta es no es suficiente para disminuir las cifras alarmantes de denuncias sobre delitos informáticos.

## 2.2 Marco Conceptual

**A. Delitos informáticos:** De acuerdo al portal web del Observatorio de CEPLAN se tiene que, los delitos informáticos se configuran como aquellos actos ilícitos cometidos por

delincuentes que utilizan instrumentos electrónicos para el robo de datos personales de usuarios. (p.1)

**B. Seguridad de la información:** Paguay (2020) menciona que, en la actualidad existen millones de personas que dependen del uso constante del Internet y de herramientas digitales para el desarrollo de sus actividades, por lo tanto, es de suma importancia que los Estados establezcan mecanismos y estrategias que se dediquen exclusivamente a la protección de la información que se encuentra almacenada en las redes y sistemas informáticos. (p. 29)

**C. Protección de Datos:** Polo (2020) plantea que, debido a la evolución de las TIC´s y la exposición de los datos personales a la virtualidad, es que estos se ven en la necesidad de resguardar la información y limitar su acceso hacia terceros, esto último mediante la implementación de mecanismos informáticos que permitan salvaguardar los derechos fundamentales de los usuarios. (p.8)

D. **Ciberdelincuencia:** Astorayme (2023) señala que la ciberdelincuencia en Lima se ha convertido en una de las principales problemáticas por afrontar debido a la falta de normatividad de los delitos informáticos como el Smishing y Vishing, así como de fiscalías especializadas que luchen contra la ciberdelincuencia. (p.9)

# III. MÉTODO

## 3.1. Tipo de Investigación

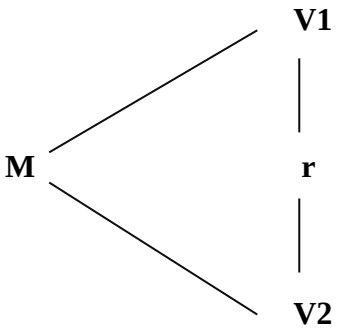
De acuerdo a Hinojosa (2024) cualquier tipo de investigación siempre tendrá como finalidad principal la obtención de conocimientos nuevos (investigación básica), o en todo caso, profundizar a fondo un tema ya existente mediante la resolución de problemas específicos (investigación aplicada).

Por lo tanto, de acuerdo a líneas anteriores, podemos indicar que, este estudio de investigación es de tipo aplicada. Además de acuerdo a sus características, es que este estudio posee un nivel de estudio tipo descriptivo, de corte correlacional y explicativo, pues se buscará proporcionar a los lectores una representación detallada de los hechos enfocados en la investigación, determinando la relación entre las variables planteadas, así como especificando su vínculo, es decir, explicando cómo es que una influye en la otra. Además, el espacio temporal utilizado será el 2023.

- **Nivel de la Investigación**

  Debido a que se trata de una tesis descriptiva, de corte correlacional y explicativo, es que se va determinar y analizar el vínculo y los efectos de las variables. En ese sentido, para Zúñiga (2023) la variable independiente produce efectos sobre la variable dependiente.

  En ese sentido, tenemos que:



*Fuente. Elaboración propia*

En donde:

**M** = Muestra

$\mathbf{V_1}$ = Variable 1

$\mathbf{V_2}$ = Variable 2

***r*** = Relación de las variables de estudio.

- **Método y diseño Método de Investigación**

Medina (2023) Se caracteriza por ser un proceso sistemático y organizado la cual es empleo por diversos autores para responder a la problemática de la investigación. A pesar de esto, es erróneo creer que el método incluye únicamente la problemática, sino que también abarca la recopilación, así como el análisis de datos, las conclusiones obtenidas y las recomendaciones respecto de estas últimas.

- **Diseño de la Investigación**

El diseño empleado es de tipo no experimental descriptivo, según Zúñiga (2023) este tipo de investigación se caracteriza por la recopilación de información de acuerdo a la realidad, sin dejando de lado las variables. Además, también es descriptiva, pues permite realizar la observación, descripción y análisis de cada una de ellas.

## 3.2. Ámbito temporal y espacial

### *3.2.1. Ámbito temporal*

La presente investigación se circunscribe dentro del año 2023.

### *3.2.2. Ámbito espacial*

El estudio se centra específicamente en cómo interactuaron la seguridad de la información digital y los delitos informáticos dentro de los límites geográficos de Lima

Metropolitana, cubriendo el período de un año calendario (2023).

### 3.3. Variables

**Tabla 1**

*Variables de investigación*

| Variables | Definición conceptual | Definición operacional | Dimensiones | Indicadores |
|---|---|---|---|---|
| **Variable independiente:** La seguridad de la información digital | Este mecanismo contribuye a la protección de datos e información personal privada tanto de personas como de empresas. Por lo que si no se implementan los mecanismos adecuados la presencia de ciberdelincuencia es mayor. | Es de gran relevancia argumentar la Importancia de mecanismos informáticos así también como las amenazas que pueden presentarse para que se pueda sistematizar el plan de tesis. | Legislación normativa | ONU |
| | | | | Unión Europea |
| | | | | A nivel nacional |
| | | | Características de la información | Confidencialidad |
| | | | | Autenticación |
| | | | | Integridad |
| | | | | Disponibilidad |
| | | | Amenazas a la seguridad de la información digital | Phishing |
| | | | | Fraude |
| | | | | Malware |
| | | | | Suplantación de identidad |
| **Variable dependiente:** | Son uno de los desafíos para el | Se requiere hacer el estudio de la | Legislación normativa | A nivel nacional |
| | | | | Convención de |

| | | | | |
|---|---|---|---|---|
| La configuración de los delitos informáticos | Estado peruano, así como la justicia penal. Son considerados como aquellos actos ilegales que se realizan mediante el uso de TIC´s con la finalidad de robar información personal y privada. | relación de la seguridad de la información digital con la configuración de los delitos informáticos con la finalidad de Determinar la relación entre las variables. | Desafíos en la tipificación | Budapest |
| | | | | Código Penal |
| | | | | Ley 30096 |
| | | | Derecho comparado | España |
| | | | | México |
| | | | | Colombia |

[4]

*Nota.* Elaboración propia

## 3.4. Población y Muestra.

### *3.4.1. Población*

Para Mamani (2024) la población dentro de un trabajo de investigación cualquier se distingue por ser el conjunto de elementos que comparten una característica específica para posterior análisis, la cual puede ser situaciones, personas, o unidades como los animales, objetos, eventos, etc. Además de acuerdo al enfoque de una investigación pueden darse dos tipos de poblaciones diferentes: la finita y la infinita. (p.147)

Por tal razón, en concordancia con la cita anterior, es que la presente investigación, tendrá una población la cual estará compuesta estará por 50 personas, las cuales principalmente serán ciudadanos, abogados especialistas en derecho penal y profesionales en la tecnología de la información.

En ese sentido entonces, nuestra población estaría constituida de la siguiente manera:

**Tabla 2**

*Muestra de la investigación*

| | **Muestra** |
|---|---|
| a. Ciudadanos comunes | 20 |
| b. Especialistas en tecnología de al información | 15 |
| c. Abogados especialistas en penal | 15 |
| **Total** | **50** |

*Fuente. Elaboración Propia*

### *3.4.2. Muestra:*

Para Zúñiga (2023) ésta es considerada como un parte, un conjunto separado de la población, normalmente seleccionada de tal modo que ponga de manifiesto las propiedades de la población.

En base a los criterios de la investigación, debemos de tener en cuenta que los juristas experimentados en el derecho familiar y jueces de familia, aquellos que serán encuestados, deberán tener estudios profesionales en derecho concluidos, lo que en cierta medida conllevaría a que la persona encuestada, reconozca la importancia de nuestra investigación, así como la oportunidad de brindarnos una respuesta correctamente fundamentada.

## 3.5. Instrumentos

- ***Formato de Encuestas***

  Se caracteriza por contener preguntas y opciones de respuestas previamente establecidas, para que los encargados de investigación, así como el autor o titular de la investigación pueda emplearlos a conseguir lo requerido, es decir, a los objetivos

planteados al inicio de la investigación.

- ***Guía de Cuestionario***

Una guía de cuestionario es uno de los instrumentos más utilizados por los autores, pues, al tener un esquema sobre las preguntas previamente redactadas, por interrogantes escritas, predefinidas, secuenciadas y separadas por capítulos o temática específica, es que este mismo, obtendrá una información específica y direccionada a la obtención de respuestas claras ayudando a la resolución del problema general.

- ***Ficha bibliográfica***

Básicamente, es un documento usado para la recopilación de datos de las normas legales, penales, de libros, revistas, periódicos, trabajos de investigación e Internet relacionados con las variables en estudio, es decir, al finalizar, esta contendrá toda la información principal que se usará para una investigación cualquiera.

## 3.6. Procedimientos

Una vez desarrollado los antecedentes y las bases teóricas de nuestra investigación, corresponde entonces, la aplicación tanto de las técnicas como de los instrumentos de recopilación de investigación con respecto al tema en desarrollo. En ese sentido, se tomará en cuenta, la señalización de los pasas a implementar con cada una de estos mecanismos, es decir, como es que se van a utilizar, con quienes se va a trabajar y con qué población se emplearán (cabe resaltar que esto se aplica en el uso de las encuestas y la muestra a considerar para el desarrollo de las mismas). Continuando, corresponderá el uso de los instrumentos de medición y las guías de cuestionario. Finalmente, se procederá a puntualizar cada una de las técnicas empleadas para el análisis de cada uno de los datos e información obtenida mediante cada uno de estos mecanismos, los cuales direccionarán a la solución de la problemática, así también

como el cumplimiento de cada uno de los objetivos trazados previamente.

## 3.7. Análisis de Datos

Para el desarrollo de un buen análisis es que se aplicarán las siguientes técnicas:

- **Análisis documental**

Muchos autores acotan que el análisis documental más que una técnica esto es considerado como un método o una estrategia empleada con la finalidad de adquirir datos de normas, libros, tesis, manuales, reglamentos, memorias, informes, etc. Esto último permite demostrar una de las grandes ventajas del análisis documental, que es tener un respaldo demostrativo, recurriendo a las fuentes que fueron medidos por su validez, entre los que se escogió en la realidad y lo que se plantea en la teoría.

Ahora bien, los instrumentos del análisis documentario más utilizados son los cuadros y tablas, los cuales son tratados mediante el procesador estadístico, en donde se hará uso a los programas computarizados más adecuados.

Finalmente, el análisis nacional, como internacional mediante el estudio del derecho comparado también serán temas de enfoque dentro del tema de estudio en este proyecto.

- **Encuesta**

Para Catacora (2024) el uso de las encuestas permite obtener la uniformidad y comparabilidad de la información recaba con la opinión de la población. Además, es considerada como una técnica que conlleva al interrogatorio en un cuestionario dirigido a la población de estudio, por la cual se caracteriza por tener preguntas previamente redactadas.

Ahora bien, teniendo en cuenta que la encuesta está direccionada a la población o muestra de estudio, es necesario resaltar que, el objetivo principal, es conocer la

opinión o los estados de aceptación sobre situaciones específicas las cuales deberán estar enfocadas en el tema de estudio, generando así, respuestas coherentes y especificas los cuales permitirán al autor, realizar un análisis estadístico.

**Tabla 3**

*Preguntas vinculadas a la encuesta*

| ITEM | PREGUNTAS | ESCALAS DE MEDICIÓN | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| 1 | ¿Considera que la seguridad de la información digital es una prioridad en su entorno laboral o diario? | | | | | |
| 2 | ¿Considera usted que el marco legal peruano actual es adecuado para enfrentar lo delitos informáticos? | | | | | |
| 3 | ¿Considera usted que las políticas y medidas de protección implementadas tanto por organismos públicos como privados, son realmente eficaces para combatir los delitos informáticos? | | | | | |
| 4 | ¿Considera que la falta de consciencia sobre la seguridad digital tanto en operador de la justicia como en ciudadanos contribuye al aumento de este tipo de delitos en Lima Metropolitana? | | | | | |

| | |
|---|---|
| **5** | ¿Considera que el conocimiento sobre la seguridad de la información digital en la población de Lima Metropolitana es suficiente para prevenir delitos informáticos? |
| **6** | ¿Considera que el fortalecimiento de la seguridad de la información digital debería ser la máxima prioridad tanto en la política pública como en la práctica del derecho penal en el Perú? |
| **7** | ¿Considera usted que la cooperación entre especialistas en derecho penal y en tecnología de la información es esencial para enfrentar eficazmente los delitos informáticos en el contexto legal peruano? |
| **8** | ¿Considera que la justicia penal está preparada para enfrentar los desafíos de los delitos informáticos relacionados con el fraude, la suplantación y los malware? |
| 9 | ¿Considera que la implementación de nuevas tecnologías como la inteligencia artificial y el análisis forense digital es importante para la resolución de casos de delitos informáticos en el derecho penal peruano? |
| 10 | ¿Ha sido alguna vez víctima de un delito informático? |

*Fuente. Elaboración Propia*

- **Juicio de Expertos**

Para Raeburn (2025) el juicio de expertos es entendido como aquella opinión personal pero debidamente detallada por parte de expertos en el tema de investigación, los cuales pueden ser consultores externos, miembros de algún equipo interno,

especialistas en áreas específicas, que permitan al autor, obtener una información sustentada, evidencias, juicios, o en todo caso, valoraciones sobre un tema determinado a partir de los conocimientos otorgados por los expertos. (p.78)

- **Técnicas de Análisis estadísticos**

  - ✓ ***Análisis de correlaciones***

    Para Mamani (2024) el análisis correlacional dentro de una investigación refiere a la relación entre las dos variables (en este caso cuantitativas) dependiente e independiente. (p.134)

    En pocas palabras, el objetivo principal, es determinar si existe o no relación entre las variables, es decir, si los cambios en una de las variables están o no influidos por la otra.

  - ✓ ***Análisis de regresión***

    Esta consiste en ser una técnica estadística que se caracteriza por calcular relación entre dos variables prediciendo sus valores. Además de esto, permite al autor ajustar los datos de la investigación, generando así la cual es la importancia de las variables y como es que estas interactúan entre sí.

  - ✓ ***Visualización de datos***

    La visualización de datos es considerada por muchos como una de las técnicas de análisis de datos más utilizadas y de gran relevancia, esto debido, por lo fácil que resulta a través de un gráfico o imagen detectar patrones en los datos. Es especialmente útil cuando se busca entender grandes volúmenes de información de forma rápida y simplificada.

  - ✓ ***Validez***

    Sabemos que los instrumentos que son empleados en toda investigación para

la recolección de datos deben contar básicamente con dos características: la validez y la confiabilidad. Ahora bien, nuestro punto de enfoque es el primero, por lo tanto, podemos indicar que, con respecto a los instrumentos, estos son válidos cuando mide correctamente aquello que se intenta medir, es el grado con que el instrumento es capaz de lograr los objetivos planteados en la investigación.

A través de los instrumentos, sabemos que se obtienen resultados, en ese sentido, tenemos que, mediante su publicación titulada "El protocolo de investigación VII. Validez y confiabilidad de las mediciones", Villasís (2018) sostiene que el validez, hablando en términos de investigación, hace referencia a lo que es verdadero o falso con respecto a los resultados, es decir, para que los resultados obtenidos dentro de un proyecto, este debe estar libre de errores, los cuales son evidencia de los problemas metodológicos empleados por el autor, y de los cuales pueden categorizarse en tres tipos: los sesgos de selección, los sesgos en la medición y finalmente, los sesgos de confusión.

De igual manera, Marqués (2018) sostiene que, un trabajo de investigación puede considerase no válido debido a diferentes cuestiones, dentro de las cuales se encuentran, los errores sistemáticos que comúnmente son denominados como sesgos, los errores aleatorios, los cuales están relacionados con la confiabilidad, la consistencia, la reproducción de la información obtenida, así también como la precisión y la exactitud al momento de plasmar las ideas recolectadas. Ahora bien, estos factores, según el autor, no se pueden eliminar, pero si se pueden disminuir mediante el uso de diferentes técnicas, como el parafraseo, la reducción o aumento de la información para tener resultados más preciso.

- ✓ ***Procesamiento de datos***

De acuerdo al desarrollo de la presente investigación, podemos indicar

que, los instrumentos de procesamiento de datos, son los siguientes:

**Google Forms**

Los formularios de Google son una herramienta disponible de Google Works pace, mediante la cual se pueden crear diversos tipos de formularios. También se pueden realizar encuestas, test de opciones múltiples, ventas, gastos, y otras distintas opciones.

Google en este caso, nos da un acceso a una herramienta que nos puede servir de mucha ayuda durante toda nuestra vida universitaria, y después. Este formulario se puede adecuar de acuerdo a nuestras múltiples necesidades. Facilitando la opción de poder extraer los resultados, convirtiéndolos en cuadros estadísticos en una hoja de cálculo (Excel).

- ✓ ***Escala de Likert***

Para Matas (2018) este instrumento de medición de resultados es considerado como una herramienta psicométrica, en la cual el encuestado, por voluntad propia, debe indicar su postura de acuerdo o descuerdo sobre una pregunta o afirmación realizada por otra persona, en este caso el autor de una investigación, lo que se realiza mediante una escala ordenada y unidimensional.

De acuerdo a nuestra perspectiva, podemos indicar que, la escala de Likert es una herramienta que ha venido siendo usado por todos los investigadores que utilizan la técnica de investigación "encuesta o cuestionario", con el objetivo de analizar las actitudes y fundamentos de las personas participantes en las encuestas, mediante posturas de acuerdo, desacuerdo o en todo caso neutra.

En ese sentido, debido al enfoque de nuestra investigación, es que, en nuestro cuestionario se emplearon un total de 10 preguntas cerradas, cada una con 5 alternativas, las cuales fueron basadas en la Escala de Likert, la cual

se muestra a continuación.

***Tabla 4***

*Niveles para la Escala de Likert*

| Evaluación | Puntaje |
|---|---|
| Totalmente de acuerdo | 1 |
| De acuerdo | 2 |
| Ni de acuerdo, ni en desacuerdo | 3 |
| En desacuerdo | 4 |
| Totalmente en desacuerdo | 5 |

*Fuente. Elaboración Propia*

- ✓ ***Alfa de Cronbach***

De acuerdo a Oviedo & Campos (2020) sostiene que, debido a que el proceso de validación de una escala se caracteriza por ser un proceso largo y costoso es que se nace la herramienta del alfa de Cronbach, la cual es una forma más simple y empleada por autores, debido a que la misma mide la consistencia interna, o en pocas palabras, evalúa los ítems que forman una escala, los cuales pueden ser de una encuesta o el cuestionario.

Ahora bien, al ser menos costosa y más sencilla de utilizar, es que encontramos ciertas ventajas en esta herramienta, de la cual podemos resaltar la capacidad para estimar cuánto mejorará (o empeorará) la fiabilidad de la prueba si excluye un elemento en particular.

La ecuación del coeficiente α está representada de la siguiente forma:

$$\alpha = [K / (K - 1)] * [1 - (\Sigma\sigma\_i^2 / \sigma\_T^2)]$$

En donde:

- Alfa (α): Coeficiente del Alfa de Cronbach
- K: Número de ítems del instrumento
- $\sigma\_i^2$: Varianza del ítem de i
- $\sigma\_T^2$: Varianza total del test (Suma de todos los Ítems)

### 3.8. Consideraciones Éticas

De acuerdo a un informe publicado por el Ministerio de Ciencia e Innovación, de la mano con las unidades por el Gobierno de España (2019), se llegó a la conclusión que, la ética dentro de cualquier tipo de investigación exige la práctica del respeto y la consideración de la protección de datos, privacidad y confidencialidad de otros autores.

En ese sentido, consideramos que todo trabajo debe ser original, y por esta razón, la información plasmada será objetiva, lo que conlleva al respeto de la confidencialidad de sus datos personales. Asimismo, en respeto a los demás autores, es que se empleó el estilo APA, tomando en cuenta, las citas, así como las referencias bibliográficas, reconociendo el derecho a la propiedad intelectual tal y como lo señala la normativa peruana.

# IV. RESULTADOS

## 4.1 Resultados de la investigación

La muestra utilizada en la presente tesis está conformada por 50 personas, la cual ha sido compuesta de la siguiente manera:

| Muestra | |
|---|---|
| Ciudadanos comunes | 20 |
| Especialistas en tecnología de al información | 15 |
| Abogados especialistas en penal | 15 |
| **Total** | **50** |

*Fuente. Elaboración Propia*

La encuesta fue realizada a una población la cual estará conformada por 50 personas. De esta cantidad, la mayoría de los encuestados serán principalmente ciudadanos comunes con la finalidad de determinar si estos han sido víctimas de algún delito informático, así mismo, nuestro cuestionario estará dirigido a abogados especialistas en la rama del derecho penal, así también como especialistas en tecnología de la información.

## 4.2. Análisis e interpretación de resultados

Una vez culminado la encuesta con cada uno de los miembros de nuestra muestra previamente seleccionada, es que se ha podido llegar a los siguientes resultados, los cuales se muestran a continuación.

**Pregunta 1.**

¿Considera que la seguridad de la información digital es una prioridad en su entorno laboral o diario?

**Tabla 5**

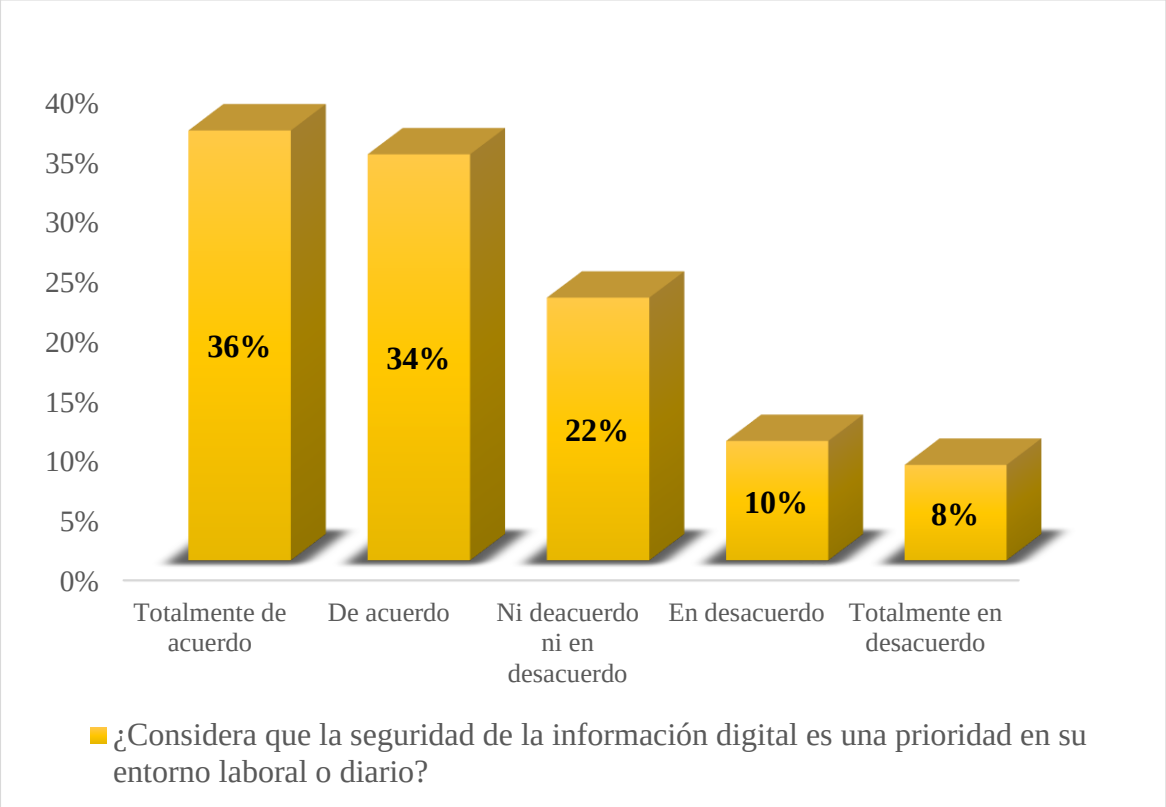
*La información digital como prioridad en el entorno*

| | Frecuencia | Porcentaje |
|---|---|---|
| Totalmente De Acuerdo | 18 | 36% |
| De Acuerdo | 12 | 24% |
| Ni Desacuerdo Ni En Desacuerdo | 11 | 22% |
| En Desacuerdo | 5 | 10% |
| Totalmente En Desacuerdo | 4 | 8% |
| Total | 50 | 100% |

*Nota.* Elaboración propia

**Figura 1**

*La información digital como prioridad en el entorno*



*Nota.* Elaboración propia

**Interpretación**

Con respecto a la pregunta 1, tenemos que el 36% de la población encuestada respondió totalmente de acuerdo, el 24% optó por la opción de acuerdo, el 22% respondió ni de acuerdo ni en desacuerdo, el 10% selecciono la opción en desacuerdo, y finalmente, el 8% marcó la alternativa de totalmente en desacuerdo.

**Pregunta 2.**

¿Considera usted que el marco legal peruano actual es adecuado para enfrentar lo delitos informáticos?

**Tabla 6**

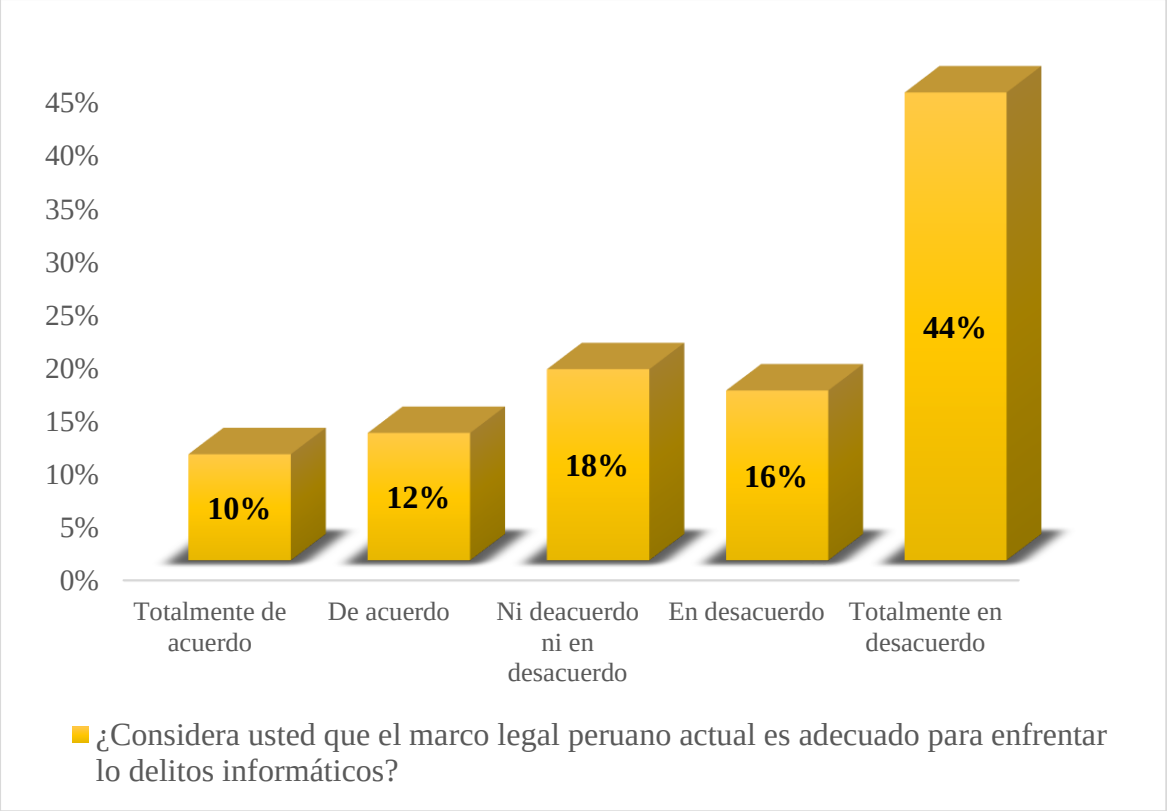
*El marco legal peruano actual como instrumento adecuado para enfrentar los delitos informáticos*

| | Frecuencia | Porcentaje |
|---|---|---|
| Totalmente de acuerdo | 5 | 10% |
| De acuerdo | 6 | 12% |
| Ni desacuerdo ni en desacuerdo | 9 | 18% |
| En desacuerdo | 8 | 16% |
| Totalmente en desacuerdo | 22 | 44% |
| Total | 50 | 100% |

*Nota.* Elaboración propia

**Figura 2**

*El marco legal peruano actual como instrumento adecuado para enfrentar los delitos informáticos*




*Nota.* Elaboración propia

**Interpretación**

Con respecto a la pregunta 2, se obtuvo que, el 10% de la muestra encuestada tomó como respuesta la opción totalmente de acuerdo, el 12% respondió en de acuerdo, el 18. % seleccionó la alternativa ni de acuerdo ni en desacuerdo, el 16% marcó en desacuerdo, y finalmente, casi del más de la mitad de los encuestados, el 44% optó por la opción totalmente en desacuerdo.

**Pregunta 3**

¿Considera usted que las políticas y medidas de protección implementadas tanto por organismos públicos como privados, son realmente eficaces para combatir los delitos informáticos?

**Tabla 7**

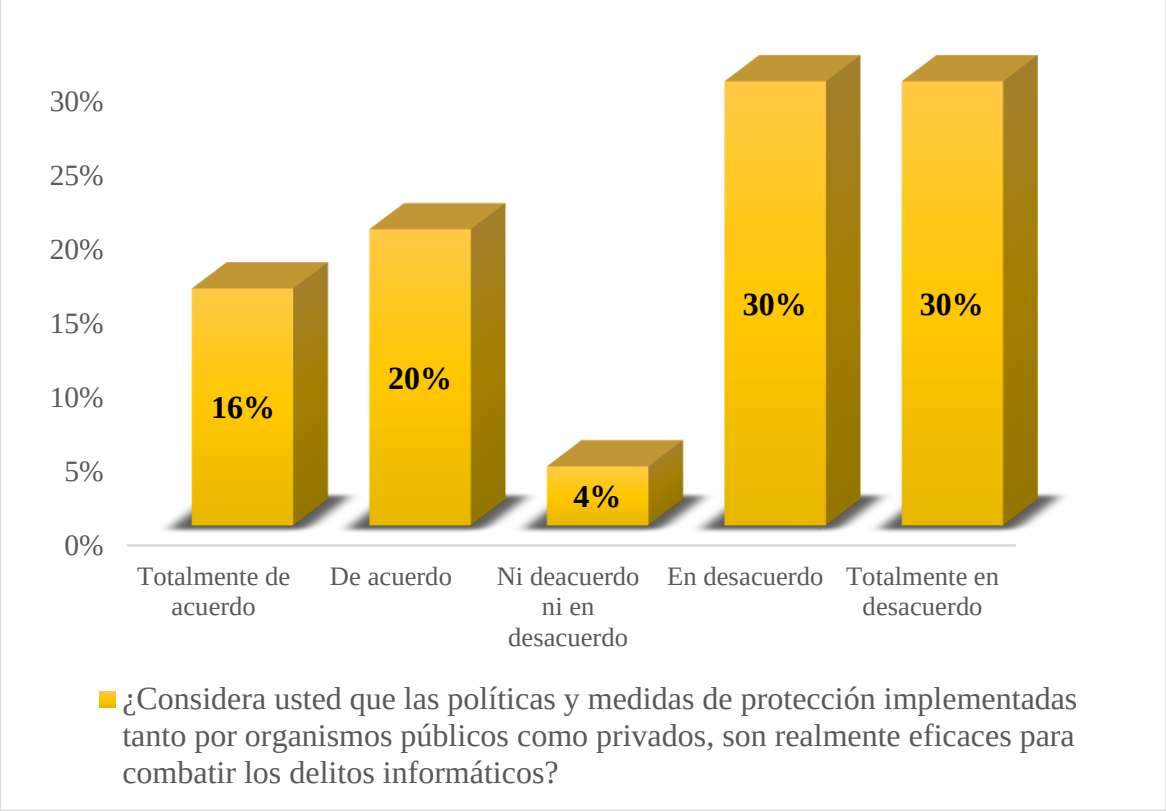
*Las políticas, medidas de protección implementadas y su eficacia*

| | Frecuencia | Porcentaje |
|---|---|---|
| Totalmente de acuerdo | 8 | 16% |
| De acuerdo | 10 | 20% |
| Ni de acuerdo, ni en desacuerdo | 2 | 4% |
| En desacuerdo | 15 | 30% |
| Totalmente en desacuerdo | 15 | 30% |
| Total | 50 | 100% |

*Nota.* Elaboración propia

**Figura 3**

*Las políticas, medidas de protección implementadas y su eficacia*




*Nota.* Elaboración propia

**Interpretación**

Con respecto a la pregunta 3 como parte de los resultados obtenidos, se concluye que, el 16% respondió totalmente de acuerdo, el 20% seleccionó como respuesta la opción de acuerdo, el 4% optó por la alternativa ni de acuerdo ni en desacuerdo, el 30% marcó en desacuerdo, y finalmente, el 30% de los encuestados tomó como respuesta totalmente en desacuerdo.

**Pregunta 4**

¿Considera que la falta de consciencia sobre la seguridad digital tanto en operador de la justicia como en ciudadanos contribuye al aumento de este tipo de delitos en Lima Metropolitana?

**Tabla 8**

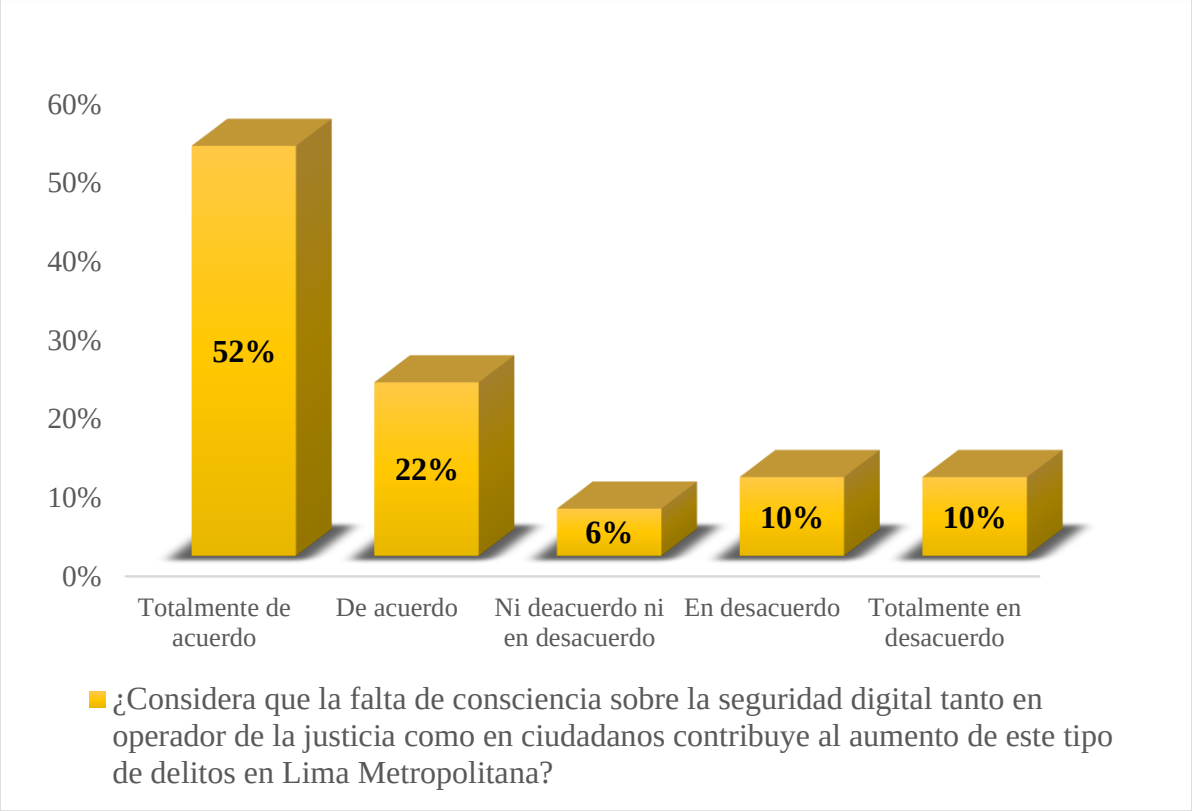
*La falta de consciencia sobre la seguridad digital*

| | Frecuencia | Porcentaje |
|---|---|---|
| Totalmente de acuerdo | 26 | 52% |
| De acuerdo | 11 | 22% |
| Ni de acuerdo, ni en desacuerdo | 3 | 6% |
| En desacuerdo | 5 | 10% |
| Totalmente en desacuerdo | 5 | 10% |
| Total | 50 | 100% |

*Nota.* Elaboración propia

**Figura 4**

*La falta de consciencia sobre la seguridad digital*




*Nota.* Elaboración propia

**Interpretación**

Con respecto a la pregunta 4, la cual fue enfocado sobre la falta de consciencia sobre la seguridad digital, y en concordancia con los resultados alcanzados, entonces se tiene que, el 52% respondió totalmente de acuerdo, el 22% marcó de acuerdo, el 6% optó por ni de acuerdo ni en desacuerdo, el 10% seleccionó en desacuerdo, y finalmente, el 10% de la muestra encuesta tomó como respuesta a la pregunta planteada la opción totalmente en desacuerdo.

**Pregunta 5.**

¿Considera que el conocimiento sobre la seguridad de la información digital en la población de Lima Metropolitana es suficiente para prevenir delitos informáticos?

**Tabla 9**

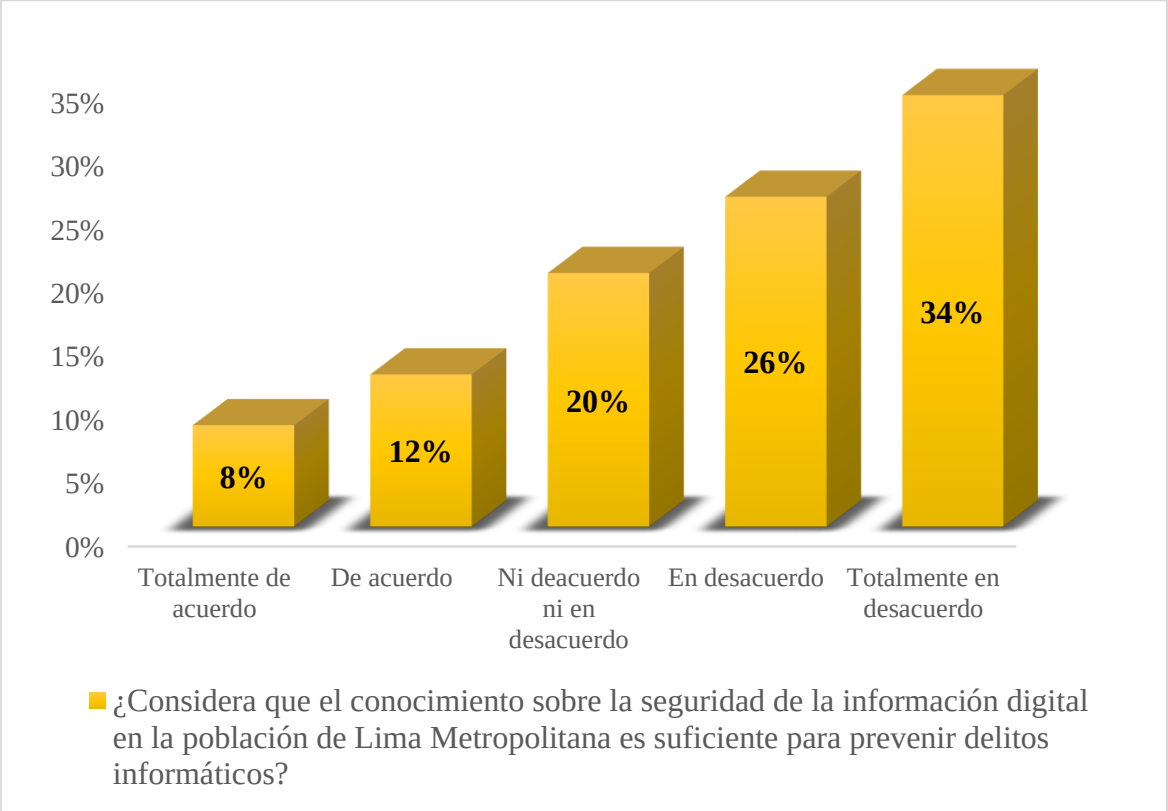
*El conocimiento sobre la seguridad de la información digital en la población de Lima Metropolitana*

| | Frecuencia | Porcentaje |
|---|---|---|
| Totalmente de acuerdo | 4 | 8% |
| De acuerdo | 6 | 12% |
| Ni de acuerdo, ni en desacuerdo | 10 | 20% |
| En desacuerdo | 13 | 26% |
| Totalmente en desacuerdo | 17 | 34% |
| Total | 50 | 100% |

*Nota.* Elaboración propia

**Figura 5**

*El conocimiento sobre la seguridad de la información digital en la población de Lima Metropolitana*




*Nota.* Elaboración propia

**Interpretación**

Con respecto a la pregunta 5, la cual estuvo direccionada conocimiento de las medidas de seguridad de la información digital en Lima Metropolitana, se puede concluir con respecto a las resultados recabados que, el 8% respondió totalmente de acuerdo, el 12% marcó la alternativa de acuerdo, el 20% tomó la opción de ni de acuerdo ni en desacuerdo, el 26% optó por en desacuerdo, y finalmente, el 34% del total de los encuestados seleccionó como respuesta totalmente en desacuerdo.

**Pregunta 6.**

¿Considera que el fortalecimiento de la seguridad de la información digital debería ser la máxima prioridad tanto en la política pública como en la práctica del derecho penal en el Perú?

**Tabla 10**

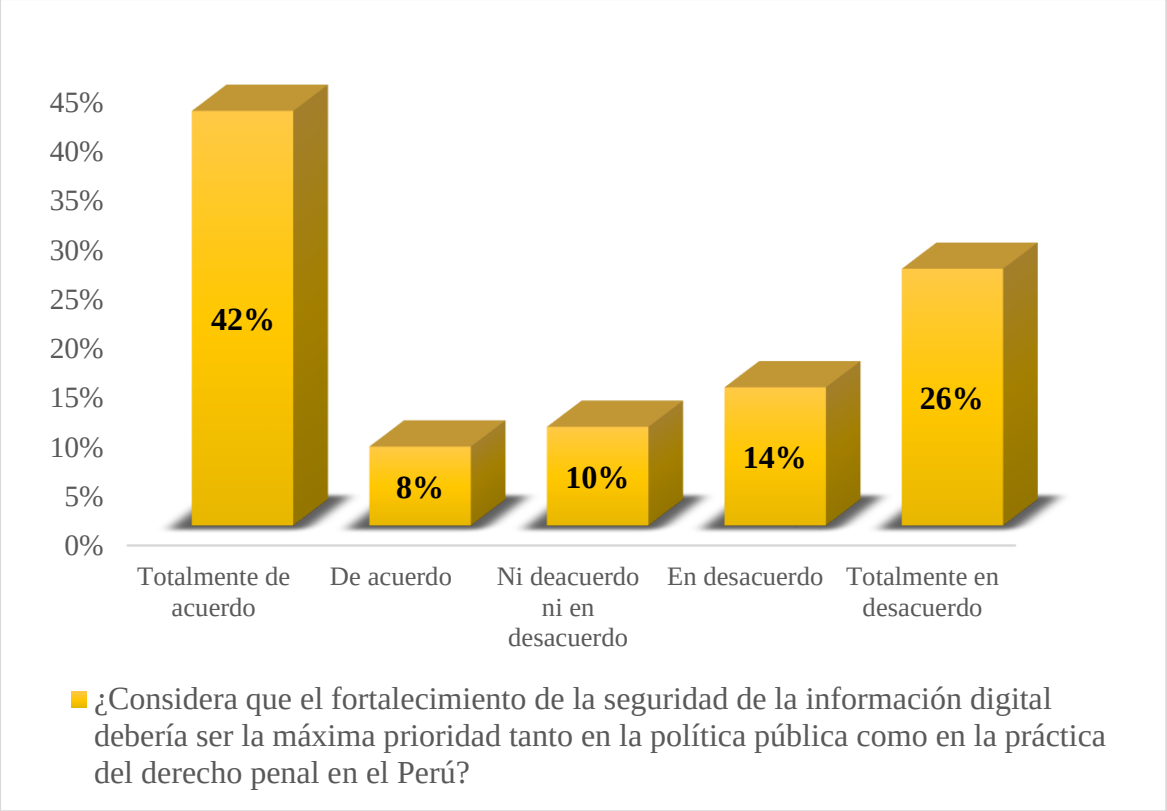
*El fortalecimiento de la seguridad de la información digital como máxima prioridad*

| | Frecuencia | Porcentaje |
|---|---|---|
| Totalmente de acuerdo | 21 | 42% |
| De acuerdo | 4 | 8% |
| Ni de acuerdo, ni en desacuerdo | 5 | 10% |
| En desacuerdo | 7 | 14% |
| Totalmente en desacuerdo | 13 | 26% |
| Total | 50 | 100% |

*Nota.* Elaboración propia

**Figura 6**

*El fortalecimiento de la seguridad de la información digital como máxima prioridad*




*Nota.* Elaboración propia

**Interpretación**

Con respecto a la pregunta 6, la cual está enfocada en el fortalecimiento de la seguridad de la información digital como máxima prioridad, se obtuvieron como resultados finales que, el 42% respondió totalmente de acuerdo, el 8% optó por la opción de acuerdo, el 10% marcó la alternativa ni de acuerdo ni en desacuerdo, el 14% tomó como respuesta en desacuerdo, y finalmente, el 26% seleccionó la opción totalmente en desacuerdo.

**Pregunta 7**

¿Considera usted que la cooperación entre especialistas en derecho penal y en tecnología de la información es esencial para enfrentar eficazmente los delitos informáticos en el contexto legal peruano?

**Tabla 11**

*La cooperación entre especialistas en derecho penal y en tecnología de la información como*

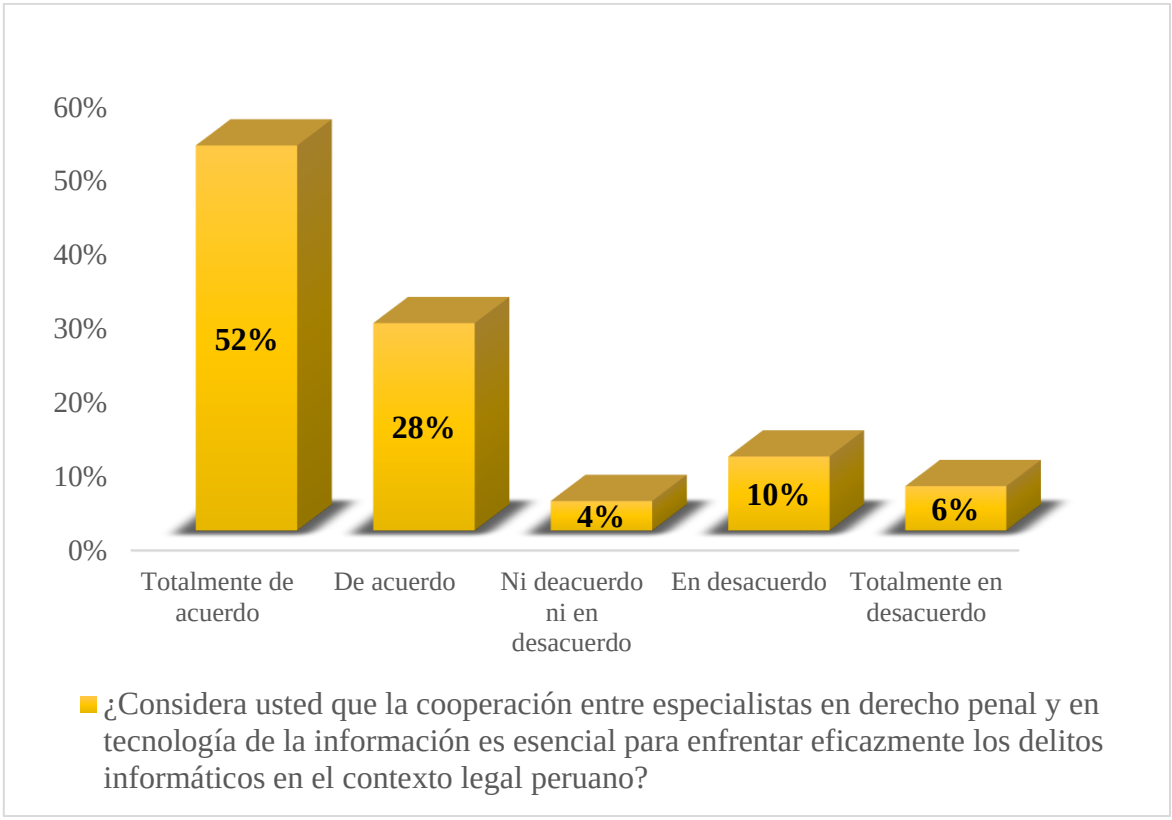
*aspecto esencial*

| | Frecuencia | Porcentaje |
|---|---|---|
| Totalmente de acuerdo | 26 | 52% |
| De acuerdo | 14 | 28% |
| Ni de acuerdo, ni en desacuerdo | 2 | 4% |
| En desacuerdo | 5 | 10% |
| Totalmente en desacuerdo | 3 | 6% |
| Total | 50 | 100% |

*Nota.* Elaboración propia

**Figura 7**

*La cooperación entre especialistas en derecho penal y en tecnología de la información como aspecto esencial*



*Nota.* Elaboración propia

**Interpretación**

Con respecto a la pregunta 7, la cual está encaminado a la cooperación entre los abogados especialistas en derecho penal y tecnología de la información, se obtuvo como resultados finales que, el 52% respondió totalmente de acuerdo, el 28% marcó la opción de acuerdo, el 4% optó por la alternativa ni de acuerdo ni en desacuerdo, el 10% tomó como respuesta en desacuerdo, y finalmente, el 60% de los encuestados seleccionó la opción totalmente en desacuerdo.

**Pregunta 8.**

¿Considera que la justicia penal está preparada para enfrentar los desafíos de los delitos informáticos relacionados con el fraude, la suplantación y los malware?

**Tabla 12**

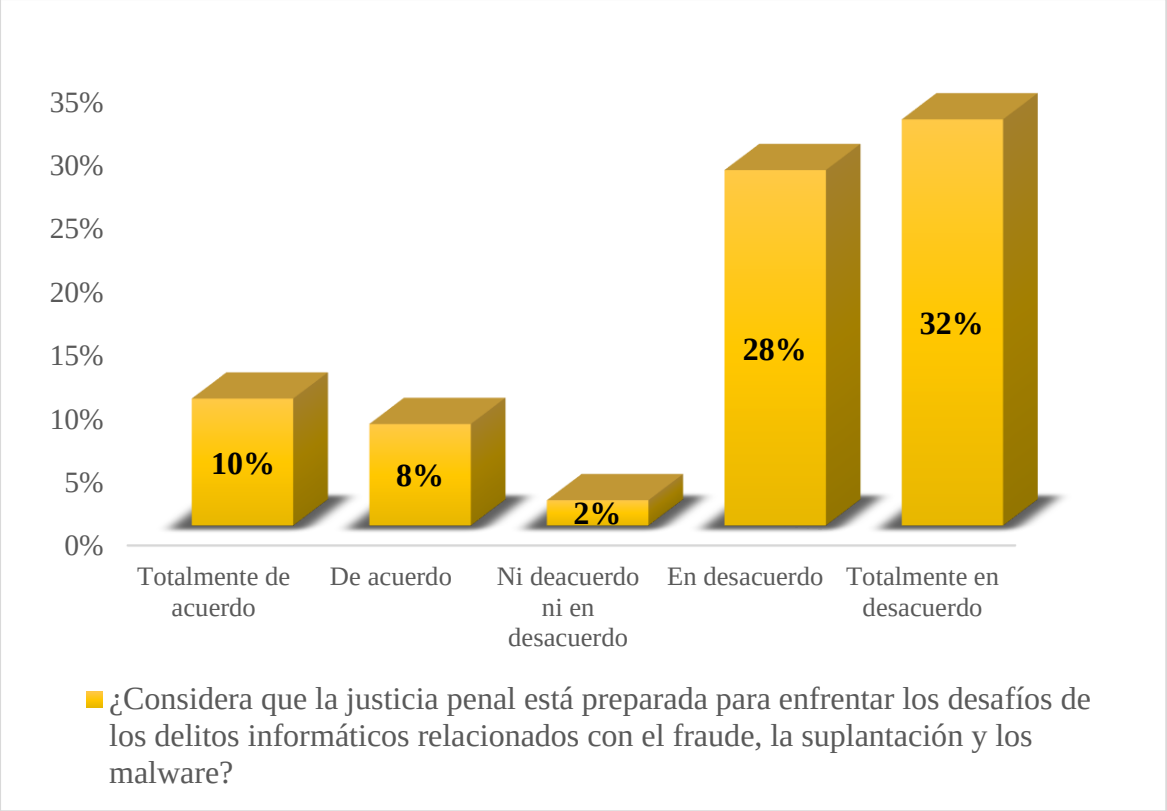
*La justicia penal y los desafíos de los delitos informáticos*

| | Frecuencia | Porcentaje |
|---|---|---|
| Totalmente de acuerdo | 5 | 10% |
| De acuerdo | 4 | 8% |
| Ni de acuerdo, ni en desacuerdo | 1 | 2% |
| En desacuerdo | 14 | 28% |
| Totalmente en desacuerdo | 26 | 32% |
| Total | 50 | 100% |

*Nota.* Elaboración propia

**Figura 8**

*La justicia penal y los desafíos de los delitos informáticos*




*Nota.* Elaboración propia

**Interpretación**

Con respecto a la pregunta 8, tenemos como resultados que, el 10% de la población encuestada respondió totalmente de acuerdo, el 8% marcó la alternativa de acuerdo, el 2% tomó como alternativa ni de acuerdo ni en desacuerdo, el 28% optó por la opción en desacuerdo, y finalmente, el 52% seleccionó como respuesta la opción totalmente en desacuerdo.

**Pregunta 9.**

¿Considera que la implementación de nuevas tecnologías como la inteligencia artificial y el análisis forense digital es importante para la resolución de casos de delitos informáticos en el derecho penal peruano?

**Tabla 13**

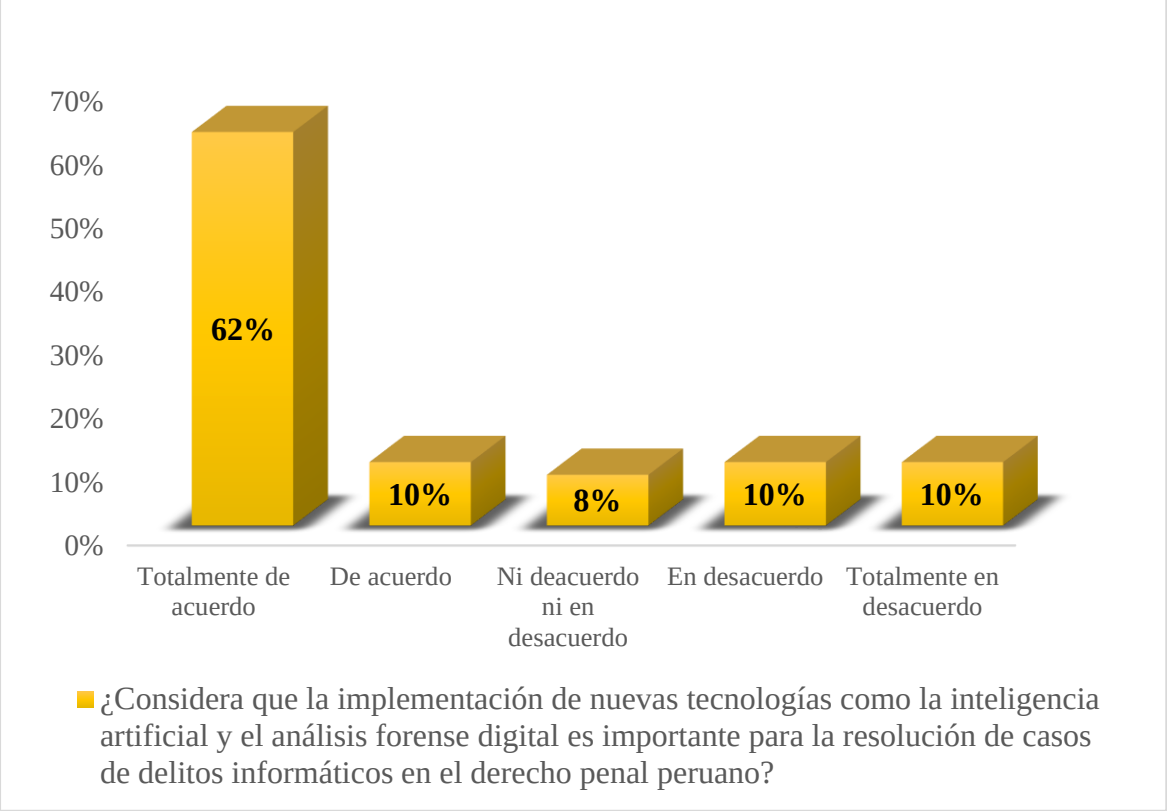
*La necesidad de la implementación de nuevas tecnologías*

| | Frecuencia | Porcentaje |
|---|---|---|
| Totalmente de acuerdo | 31 | 62% |
| De acuerdo | 5 | 10% |
| Ni de acuerdo, ni en desacuerdo | 4 | 8% |
| En desacuerdo | 5 | 10% |
| Totalmente en desacuerdo | 5 | 10% |
| Total | 50 | 100% |

*Nota.* Elaboración propia

**Figura 9**

*La necesidad de la implementación de nuevas tecnologías*




*Nota.* Elaboración propia

**Interpretación**

Con respecto a la pregunta 9, la cual está enfocada en la implementación de nuevas tecnologías para la resolución de casos de delitos informáticos, y en concordancia con los resultados obtenidos a partir de la encuesta realizada, tenemos como resultados que, el 62% respondió totalmente de acuerdo, el 10% marcó la opción de acuerdo, el 8% optó por la alternativa ni de acuerdo ni en desacuerdo, el 10% tomó la opción de en desacuerdo, y finalmente, el 10% de la población encuestada selecciono como respuesta final la opción totalmente en desacuerdo.

**Pregunta 10.**

¿Ha sido alguna vez víctima de un delito informático?

**Tabla 14**

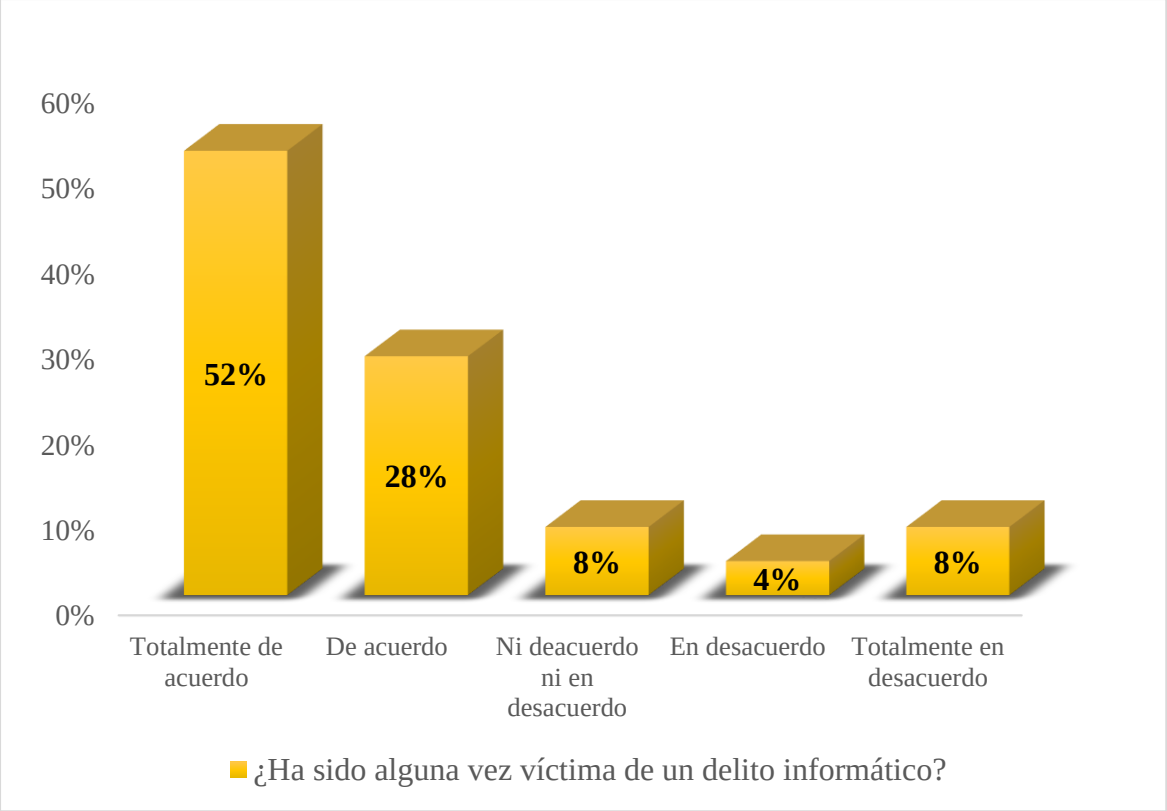
*Cantidad de personas que han sido víctima de delitos informáticos*

| | Frecuencia | Porcentaje |
|---|---|---|
| Totalmente de acuerdo | 26 | 52% |
| De acuerdo | 14 | 28% |
| Ni de acuerdo, ni en desacuerdo | 4 | 8% |
| En desacuerdo | 2 | 4% |
| Totalmente en desacuerdo | 4 | 8% |
| Total | 50 | 100% |

*Nota.* Elaboración propia

**Figura 10**

*Cantidad de personas que han sido víctima de delitos informáticos*




*Nota.* Elaboración propia

**Interpretación**

Con respecto a la pregunta 10, la cual estuvo en caminada a determinar si la muestra encuestada fue víctima alguna vez de delitos informáticos, es que se llegó a los siguientes resultados, teniendo que, el 52% respondió totalmente de acuerdo, el 28% marcó la opción de acuerdo, el 8% tomó como respuesta ni de acuerdo ni en desacuerdo, el 4% optó por la alternativa en desacuerdo, y finalmente, el 8% de la población encuestada selecciono como respuesta totalmente en desacuerdo.

# V. DISCUSIÓN DE RESULTADOS

A partir de los resultados obtenidos se puede concluir que, en primera, los delitos informáticos son uno de los problemas que afecta a Lima Metropolitana, y de ahí es que donde radica la importancia de la seguridad de la información, en ese sentido, es necesario que el Estado Peruano, de la mano con los organismos estatales involucrados y en colaboración con otras instituciones internacionales, ponga en marcha nuevas políticas públicas que se direccionen únicamente en la protección de los datos personales de millones de usuarios peruanos que se encuentran en la red. Así mismo es necesario que se saneen los vacíos procesales y legales con respecto con la tipificación de los delitos informáticos, pues de acuerdo a lo desarrollado, en la actualidad contamos con una única norma enfocada en este tema, la Ley 30096 y sus modificatorias, lo cual no permite una correcta tipificación de la gran cantidad de delitos informáticos, lo cual da paso a una mayor vulnerabilidad con respecto a la seguridad de la información.

Ahora bien, con respecto a la primera pregunta, se puede concluir que la mayoría de los encuestados, los cual representa al 36% comparten la idea con respecto a la seguridad de la información digital como una prioridad dentro de su entorno laboral o diario. Con respecto a la segunda pregunta, se puede concluir que, un poco menos de la mitad de la muestra encuesta están totalmente en desacuerdo con respecto al marco legal peruano actual sobre los delitos informáticos.

Ahora bien, siguiendo con la tercera pregunta se tiene que, la mayoría de los encuestados muestran postura firme sobre la ineficacia de las políticas y medidas de protección las cuales son implementadas tanto por los organismos públicos como privados contra la lucha de los delitos informáticos. De la cuarta pregunta se deduce que, más de la

mitad de la población encuesta muestra de total de acuerdo con respecto a la falta de consciencia sobre la importancia de la seguridad digital tanto en operadores de la justicia como

en ciudadanos contribuyendo así, al aumento en la presencia de los delitos informáticos.

De igual manera, continuando con la pregunta número cinco, se puede concluir que, más de la mitad de los encuestados consideran que el conocimiento sobre la seguridad de la información digital en la población de Lima Metropolitana no es suficiente para prevenir este tipo de delitos. Así mismo, de la pregunta número seis, se puede concluir que, en total, el 40% de la población encuestada, consideran que el fortalecimiento de la seguridad de la información digital no debería ser la máxima prioridad tanto en la política pública como en la práctica del derecho penal en el Perú.

Por otro lado, con respecto a la séptima pregunta, se deduce que, más del 80% de los encuestados mostraron su postura afirmativa con respecto a la cooperación que debería haber entre los especialistas en el derecho penal y en la tecnología de la información como un plus para hacer frente eficazmente a los delitos informáticos. De la pregunta número ocho, se tiene que, más de la mitad de todos los encuestados mostraron una postura en desacuerdo sobre la justicia penal actual peruana para hacer frente a los desafíos de los delitos informáticos como el fraude, la suplantación, los malware, etc.

Con respecto a la novena pregunta, más del 70% de toda la población que realizó esta encuesta en total de acuerdo con respecto a la implementación de nuevas tecnologías como la inteligencia artificial y el análisis forense para la resolución de casos de estos delitos. Y finalmente, respecto a la pregunta diez, se concluye que, la mayoría ha sido al menos una vez de algún tipo de delito informático.

# VI. CONCLUSIONES

- Se puede concluir que, la seguridad de la información digital es un elemento clave para la configuración de los delitos informáticos, esto debido a que, dentro del territorio peruano, existen pocos mecanismos de protección a la seguridad de la información, y además, los pocos que hay en la actualidad se caracterizan por ser ineficientes permitiendo que, para los malhechores cada vez sea fácil acceder a millones de datos personales que se encuentran en Internet o diversos sistemas informáticos, obteniendo así información o bases de datos de áreas sencillas como el Wi-fi, información en Facebook de una gran cantidad de usuarios en Facebook, datos que se encuentran en ordenadores, hasta las tan cuidadas cuentas bancarias, de los cuales, de acuerdo a los resultados obtenidos, la mayoría de los encuestados ha sido víctima.

- De igual manera, podemos concluir que, las amenazas a la seguridad de la información digital juegan desempañan un papel fundamental en la proliferación de los delitos informáticos. En ese sentido, el phishing, el malware, el Smishing, la suplantación de identidad, los spams, las redes inalámbricas inseguras y los ataques por Wi-fi hasta la ignorancia de la poca seguridad en línea, forman parte de las mayores amenazas en nuestro país. Además, el desarrollo rápido de nuevas tecnologías y la dependencia a estas, sumada a la fata de una cultura sólida de seguridad digital, facilita la comisión de estos delitos que, muchas veces quedan impunes debido a las limitaciones del marco legal y la falta de capacitación y formación de los operadores del sistema judicial en materia tecnológica.

- Podemos concluir también que, la normativa penal peruana ha evolucionado significativamente con respecto a la tipificación de los delitos informáticos tomando en cuenta la seguridad de la información digital, esto último debido a los constantes avances

sobre las TIC´s y la digitalización en las actividades comúnmente desarrolladas, los cuales, lamentablemente, se ha convertido en una ventana abierta para el desarrollo de los delitos informáticos. En ese sentido, como parte de la normativa peruana con respecto a nuestra problemática tenemos: el Código Penal de 1991 el cual regulaba el acceso y la copia ilícita de datos y el delito informático como agravante del delito del hurto. De igual manera, está la Ley actual 30096 o la Ley de los delitos informáticos, la cual ha sido modificada por la Ley 30171 y finalmente, como última normativa peruana influyente en la configuración de delitos informáticos tenemos la ratificación del Convenio de Budapest en el 2019.

- Finalmente, podemos concluir que, en la actualidad, el derecho penal peruano presenta desafíos en la tipificación y la sanción de delitos informáticos relacionados a la seguridad de la información digital, de las cuales podemos que, hasta el momento, contamos con la Ley 30096 y su modificatoria, así como el Convenio de Budapest como únicas fuentes normativas especializadas en la tipificación de delitos informáticos, a pesar de ello, estos aún están revestidos de algunos vacíos legales los cuales básicamente se deben a que las mismas no están adaptadas a las constantes evoluciones de las innovaciones tecnológicas, así mismo, otro de los grandes desafíos por superar es la falta de cooperación internacional legal la cual es necesaria para la sanción de los delitos informáticos, sino también para una mayor protección de la seguridad de la información digital.

# VII. RECOMENDACIONES

- Es necesario que el Estado busque , mediante la colaboración de organismos públicos como privados, busque implementar nuevas medidas y estrategias flexibles dirigidas exclusivamente a la protección de la información digital, tomando en cuenta la evolución de las tecnologías de la información, así también como la actualización de las constantes amenazas, y las cuales deben darse mediante la relación de las nuevas tecnologías de información con las políticas públicas destinadas a salvaguardar los derechos fundamentales de las personas, tales como el fortalecimiento del uso de contraseñas, exigiendo a los usuarios el cambio periódico de contraseñas, el desarrollo implementación de TIC´s para la autenticación de los usuarios, así también como la constante actualización de los software y los sistema de seguridad de las bases o almacenadores de datos.

- El Estado está en la responsabilidad de exigir tanto los organismos como públicos como los privados contar con un área especializada en informática, y como consiguiente a esto, contar con profesionales en informática o tecnología de la información deben recibir capacitación y formación constante sobre la prevención, la identificación, la respuesta y la recuperación de datos ante posibles nuevas amenazas, es decir, esto incluye, saber cómo actuar ante ellas, así como establecer un marco procedimental en caso de datos perdidos o robados, cómo es que dará su recuperación y en consecuencia de ello, las medidas legales que se tomarán en cuenta ante estas situación, además de, como es que esto se informará a los usuarios.

- Es necesario que las autoridades estatales analicen la actualización y la adecuación de la norma vigente respecto de los delitos informáticos de acuerdo a los constantes

avances tecnológicos y las normas formas de ciberdelincuencia, todo lo anterior es necesario para recopilar todas las amenazas tecnológicas y conforme a ello, actuar para disminuir las cifras alarmantes, así también es indispensable para sanear los vacíos legales existentes hasta la actualidad los cuales, para los ciberdelincuentes significa una puerta abierta para la libertad, dejando impune muchos delitos.

- Los poderes del Estado peruano deben estar disponibles al avance y desarrollo de una reforma legal dinámica los cuales no solo abarque las nuevas modalidades de delitos informáticos, sino también que sea flexible e incluya otros aspectos que son esenciales para la superación de los desafíos dentro de la tipificación y la sanción de los delitos informáticos, como es la cooperación internacional, no solo en ámbito legal normativo con respecto a la delitos informáticos y medidas para la seguridad de la información, sino también que se enfoque en la esfera de investigación y medidas que permitan la extradición de los delincuentes. De igual manera, es necesario la constante capacitación de los operadores de justicia peruana, tanto jueces, fiscales, así como abogados dentro del área de la ciberseguridad y la informática forense y finalmente, es necesario la creación de unidades especializadas en delitos informáticos los cuales deben contar con recursos tecnológicos adecuados los cuales permitan detectar y analizar los delitos informáticos de manera eficaz.

# VIII. REFERENCIAS

Acosta, M., Benavides, M., García, N. (2020) Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. [Revista de la Universidad del Zulia]

Alcalá y Meléndez (2023) Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas. [Revista de Tecnología y Sociedad]

Bascur (2023) Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459, Primera Parte – Universidad Autónoma de Chile. Recuperado de https://rej.uchile.cl/index.php/RECEJ/article/view/67885/75898

Carranza, J (2022) El delito de Estafa Informática en el Salvador" – Universidad de El Salvador. Obtenido de https://repositorio.ues.edu.sv/server/api/core/bitstreams/13bf6a3d-3297-465c-856b-8f4319803332/content

Chávez, E (2018) El delito contra Datos y Sistemas Informáticos en el derecho fundamental a la Intimidad Personal en la Corte Superior de Justicia de Lima Norte, 2017 – Universidad Nacional Federico Villareal. Recuperado el 08 de febrero del 2025 de https://repositorio.unfv.edu.pe/bitstream/handle/20.500.13084/2704/CHAVEZ%20RODRIGUEZ%20ELIAS%20GILBERTO%20-%20DOCTORADO.pdf?sequence=1&isAllowed=y

Contento, J (2023) La problemática de los Delitos Informáticos en el Ecuador, su persecución y capacidad preventiva de la legislación ecuatoriana en contraste con el Derecho Comparado – Universidad Nacional de Loja. Recuperado el 09 de febrero del 2025 de https://dspace.unl.edu.ec/jspui/handle/123456789/28000

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

El Peruano (2023) ¡Cuidado con los fraudes informáticos! Estas son las modalidades más denunciadas en Perú. https://www.elperuano.pe/noticia/216043-cuidado-con-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-en-peru

Gaceta Parlamentaria (2023) Iniciativa con Proyecto de Decreto por el que se expide de Ley Federal de Ciberseguridad. [Cámara de Diputados de México.]

Gamba Velandia, J (2019) El delito informático en el marco jurídico colombiano y el derecho comparado: Caso de la transferencia no consentida de Activos [Universidad Exterando de Colombia] Obtenido de https://bdigital.uexternado.edu.co/server/api/core/bitstreams/2e7e30f3-4a1f-45f6-b59a-dae6012b7210/content

Gómez (2021) Aspectos Procesales de los delitos informáticos y tecnológicos – Universidad Rey Juan Carlos. Recuperado el 9 de febrero del 2025. Obtenido de https://www.educacion.gob.es/teseo/imprimirFicheroTesis.do?idFichero=hnKQ7suiXOI%3D

Hincho, E (2023) Gobierno digital y transparencia de información en las Instituciones educativas de la UGEL Tambopata, 2022. – Universidad César Vallejo. Obtenido de https://hdl.handle.net/20.500.12692/109274

Jurado del Águila, M (2020) La Ciberseguridad en el Marco Europeo. El caso de España. [Universidad de Almería]. Obtenido de https://repositorio.ual.es/bitstream/handle/10835/9544/JURADO%20DEL%20AGUILA%2c%20MARINA.pdf?sequence=1&isAllowed=y

Observatorio CEPLAN (2024) Incremento del Ciberdelito. https://observatorio.ceplan.gob.pe/ficha/t85

ONU (s.f) Normas internacionales relativas a la privacidad digital. Oficina de Alto

Comisionado de las Naciones Unidas para los Derechos Humanos.

Osco, M (2019) La admisibilidad y el valor probatorio de la evidencia digital en el Sistema Jurídico Peruano 2018 – Universidad César Vallejo. Recuperado el 08 de febrero del 2025 de https://hdl.handle.net/20.500.12692/26623

Paletta, F (2022) Competencias digitales en información y documentación: El impacto de la transformación digital en el mercado laboral – Universidad Carlos III de Madrid. Obtenido de http://hdl.handle.net/10016/36384

Peña, M. (2023). Delitos Cibernéticos [Tesis de maestría, Universidad Libre de Colombia]. Repositorio Institucional UNILIBRE. https://hdl.handle.net/10901/24774

Portugal, J (2024) Delitos Informáticos y la Evidencia Digital en el Proceso Penal Peruano 2023 – Universidad Privada de San Carlos de Puno. Recuperado el 08 de febrero del 2025 de https://repositorio.upsc.edu.pe/bitstream/handle/UPSC/775/Jerry_Kent_PORTUGAL_ROMAN.pdf?sequence=1&isAllowed=y

Ramírez (2022) *La importancia de la seguridad de la información en el sector público en Colombia.* Revista Ibérica de Sistemas e Tecnología de Información.

Román, E (2020) Modificación legislativa de la Ley Legislativa 30096 de Delitos Informáticos para su eficacia contra la Ciberdelincuencia en la Ciudad de Chiclayo – Universidad Señor de Sipán. Recuperado de https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/10463/Roman%20Cruz%20Eucario%20Hector.pdf?sequence=1&isAllowed=y

Torres, C (2017) *Sociedad de la Información y brecha digital en España (25°ed.).* Panorama Social

Unión Europea (s.f) ¿Cómo refuerza la UE su ciberseguridad? [Consejo Europeo – Consejo de la Unión Europea].

Urdanegui, A (2023) Los delitos informáticos y la vulneración del derecho fundamental de Protección de Datos en Lima Metropolitana – Universidad Autónoma del Perú. Recuperado el 8 de febrero del 2025de https://repositorio.autonoma.edu.pe/bitstream/handle/20.500.13067/2999/Urdanegui%20Rangel%2c%20Anabeliza.pdf?sequence=1&isAllowed=y

# IX. ANEXOS

## ANEXO A: MATRIZ DE CONSISTENCIA

| Formulación de Problemas | Formulación de Objetivos | Formulación de Hipótesis | Variables e Indicadores | Metodología |
|---|---|---|---|---|
| **Problema General** | **Objetivos General** | **Hipótesis General** | **Variable** | **Tipo de Investigación:** |
| ¿De qué manera la seguridad de la información digital impacta en la configuración de los delitos informáticos en el derecho penal peruano en Lima Metropolitana 2023? | Determinar las formas en que la seguridad de la información digital impacta en la configuración de los delitos informáticos en el derecho penal peruano. | La configuración de los delitos informáticos en el derecho penal peruano se ve determinada por falta o la insuficiencia de la seguridad de la información digital, facilitando que cada vez más los ciberdelincuentes actúen con más frecuencia. | **Independiente:** La Seguridad de la Información digital. ***Dimensiones:*** - Legislaciones normativas - Características de la información digital | Este estudio de investigación es de tipo aplicada. Además de acuerdo a sus características, es que este estudio posee un nivel de estudio tipo descriptivo, de corte correlacional y explicativo, pues se buscará proporcionar a los lectores una representación detallada de los hechos enfocados en la investigación, determinando la relación entre las variables planteadas, así como especificando su vínculo, es decir, explicando cómo es que una influye en la |

| **Problemas Específicos** | **Objetivos Específicos** | **Hipótesis Especificas** | - Amenazas a la seguridad de la información digital | otra. Además, el espacio temporal utilizado será el 2023. |
|---|---|---|---|---|
| ¿Cuáles son las principales amenazas a la seguridad de la información digital que influyen en la configuración de delitos informáticos en el Perú? | Establecer las principales amenazas la seguridad de la información digital que influyen en la configuración de delitos informáticos en el Perú. | Las principales amenazas a la seguridad de la información digital en el Perú como el malware y el phishing, tienen un impacto significativo en la configuración de los delitos informáticos, aumentando la incidencia de delitos cibernéticos. | **Variable Dependiente:** La configuración de los delitos informáticos. | **Nivel de la Investigación:** Esta es una investigación de Nivel Descriptiva, de Corte correlacional y Explicativo, además, es que se va determinar y analizar el vínculo y los efectos de las variables. En ese sentido, para Zúñiga (2023) la variable independiente produce efectos sobre la variable dependiente. |
| ¿Cómo ha evolucionado la normativa penal peruana para abordar | Definir la evolución de la normativa penal peruana para abordar los delitos | La normativa penal peruana ha evolucionado de manera insuficiente para abordar los delitos informáticos, lo que ha | ***Dimensiones:*** -Legislación normativa -Desafío en la tipificación | **Método de Investigación:** Cuantitativa, Medina (2023) sostiene que es un proceso sistemático y organizado la cual es empleo por diversos autores para responder a la problemática de la investigación. A pesar de |

| | | | | |
|---|---|---|---|---|
| los delitos informáticos en relación con la seguridad de la información digital? | informáticos en relación con la seguridad de la información digital. | llevado a una desactualización en la legislación frente a las nuevas amenazas a la seguridad de la información digital. | -Derecho Comparado | esto, es erróneo creer que el método incluye únicamente la problemática, sino que también abarca la recopilación, así como el análisis de datos, las conclusiones obtenidas y las recomendaciones respecto de estas últimas. |
| ¿Qué desafíos enfrenta el derecho penal peruano en la tipificación y sanción de delitos informáticos relacionados con la seguridad de la información digital | Establecer los desafíos que enfrenta el derecho penal peruano en la tipificación y sanción de delitos informáticos relacionados con la seguridad de la información digital. | El derecho penal peruano enfrenta desafíos significativos en la tipificación y sanción de delitos informáticos, debido a la falta de capacitación en ciberseguridad de los operadores de justicia y a la dificultad de prueba en entornos digitales. | | **Diseño de la Investigación**<br>El diseño empleado es de tipo no experimental descriptivo, según Zúñiga (2023) se caracteriza por la recopilación de información de acuerdo a la realidad, sin dejando de lado las variables. Además, también es descriptiva, pues permite realizar la observación, descripción y análisis de cada una de ellas. |

## ANEXO B: INSTRUMENTO DE RECOLECCIÓN DE DATOS

## CUESTIONARIO

## UNIVERSIDAD NACIONAL FEDERICO VILLARREAL

"LA SEGURIDAD DE LA INFORMACIÓN DIGITAL Y SU IMPACTO EN LA CONFIGURACIÓN DE DELITOS INFORMÁTICOS EN EL DERECHO PENAL PERUANO EN LIMA METROPOLITANA 2023"

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

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

| Evaluación | Puntaje |
|---|---|
| Totalmente de acuerdo | 1 |
| De acuerdo | 2 |
| Ni de acuerdo, ni en desacuerdo | 3 |
| En desacuerdo | 4 |
| Totalmente en desacuerdo | 5 |

*Fuente. Elaboración Propia*

| ITEM | PREGUNTAS | ESCALAS DE MEDICIÓN | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| 1 | ¿Considera que la seguridad de la información digital es una prioridad en su entorno laboral o diario? | | | | | |
| 2 | ¿Considera usted que el marco legal peruano actual es adecuado para enfrentar lo delitos informáticos? | | | | | |
| 3 | ¿Considera usted que las políticas y medidas de protección implementadas tanto por organismos públicos como privados, son realmente eficaces para combatir los delitos informáticos? | | | | | |
| 4 | ¿Considera que la falta de consciencia sobre la seguridad digital tanto en operador de la justicia como en ciudadanos contribuye al aumento de este tipo de delitos en Lima Metropolitana? | | | | | |
| 5 | ¿Considera que el conocimiento sobre la seguridad de la información digital en la población de Lima Metropolitana es suficiente para prevenir delitos informáticos? | | | | | |
| 6 | ¿Considera que el fortalecimiento de la seguridad de la información digital debería ser la máxima prioridad tanto en la política pública como en la práctica del derecho penal en el Perú? | | | | | |

| | |
|---|---|
| **7** | ¿Considera usted que la cooperación entre especialistas en derecho penal y en tecnología de la información es esencial para enfrentar eficazmente los delitos informáticos en el contexto legal peruano? |
| **8** | ¿Considera que la justicia penal está preparada para enfrentar los desafíos de los delitos informáticos relacionados con el fraude, la suplantación y los malware? |
| 9 | ¿Considera que la implementación de nuevas tecnologías como la inteligencia artificial y el análisis forense digital es importante para la resolución de casos de delitos informáticos en el derecho penal peruano? |
| 10 | ¿Ha sido alguna vez víctima de un delito informático? |

## ANEXO C: VALIDACIÓN Y CONFIABILIDAD DEL INSTRUMENTO

Después de revisar el instrumento del Plan de Tesis denominado: ““LA SEGURIDAD DE LA INFORMACIÓN DIGITAL Y SU IMPACTO EN LA CONFIGURACIÓN DE DELITOSINFORMÁTICOS EN EL DERECHO PENAL PERUANO EN LIMA METROPOLITANA 2023” la calificación es la que se muestra a continuación:

| **Nº** | **PREGUNTA** | **0%** | **0%** | **0%** | **0%** | **0%** | **0%** |
|---|---|---|---|---|---|---|---|
| | ¿En qué porcentaje se logrará constatar la Hipótesis con este instrumento? | | | | | | |
| | ¿En qué porcentaje considera que las preguntas están referidas a las variables, sub-variables e indicadores de la investigación? | | | | | | |
| | ¿Qué porcentaje de las interrogantes planteadas son suficientes para lograr el objetivo general de la investigación? | | | | | | |
| | ¿En qué porcentaje, las preguntas son de fácil comprensión? | | | | | | |
| | ¿Qué porcentaje de preguntas siguen una secuencia lógica? | | | | | | |
| | ¿En qué porcentaje se obtendrán datos similares con esta prueba aplicándolo en otras muestras? | | | | | | |

## ANEXO D: VALIDACIÓN DE INSTRUMENTO

1. **DATOS GENERALES**
   1.1. Apellido y nombres: López Figueroa Mario Luis
   1.2. Cargo e Institución donde labora: Escuela de Posgrado de la Universidad Federico Villarreal
   1.3. Nombre del instrumento motivo de la evaluación: Encuesta
   1.4. Autor de instrumento: Sangama Huarmiyuri, Cheryl

**ASPECTOS DE VALIDACIÓN**

| Criterios | Indicadores | No cumple con su aplicación | | | | | Cumple con su aplicación | | | | | Si cumple con su aplicación | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 40 | 45 | 50 | 55 | 60 | 65 | 70 | 75 | 80 | 85 | 90 | 95 | 100 |
| 1.Claridad | Esta formulado con lenguaje apropiado | | | | | | | | | | | | | **x** |
| 2.Objetividad | Se expresa la realidad como es, indica calidad de objetivo y la adecuación al objeto investigado | | | | | | | | | | | | **x** | |
| 3.Actualidad | Este acorde a los aportes recientes al derecho | | | | | | | | | | | | | **x** |
| 4.Organizacional | Existe una organización lógica | | | | | | | | | | | | | **x** |
| 5.Suficiencia | Cumple con los aspectos metodológicos | | | | | | | | | | | | **x** | |
| 6.Internacionalidad | Esta adecuado para valorar las categorías | | | | | | | | | | | **x** | | |
| 7.Coherencia | Se respalda en fundamentos técnicos y | | | | | | | | | | | **x** | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | científicos | | | | | | | | | | | | | |
| 8.Coherencia | Existe coherencia entre los problemas, objetivos, supuestos, basados en los aspectos teóricos y científicos | | | | | | | | | | | **x** | | |
| 9.Metodología | El instrumento responde al objetivo, diseño, tipo de la investigación. | | | | | | | | | | | | | **x** |
| 10.Pertinencia | El instrumento tiene sentido frente a un problema crucial, está situado en una población, es interdisciplinaria , tiene relevancia global y asume responsablement e las consecuencias de sus hallazgos | | | | | | | | | | | | **x** | |

**OPCIÓN DE APLICABILIDAD**

- El instrumento cumple con los requisitos de para su aplicación CUMPLE
- El instrumento cumple en parte con los requisitos para su aplicación CUMPLE
- El instrumento no cumple con los requisitos para su aplicación CUMPLE

PROMEDIO DE VALORACIÓN 95.5

Firma

**Nombre:** Mario Luis López Figueroa

**DNI: 06024323**

# VALIDACIÓN DE INSTRUMENTO

## 1. DATOS GENERALES

1.1.Apellido y nombres: Martínez Letona Pedro Antonio
1.2.Cargo e Institución donde labora: Escuela de Posgrado de la Universidad Federico Villarreal
1.3.Nombre del instrumento motivo de la evaluación: Encuesta
1.4.Autor de instrumento: Sangama Huarmiyuri, Cheryl

## ASPECTOS DE VALIDACIÓN

| Criterios | Indicadores | No cumple con su aplicación | | | | | Cumple con su aplicación | | | | | Si cumple con su aplicación | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 40 | 45 | 50 | 55 | 60 | 65 | 70 | 75 | 80 | 85 | 90 | 95 | 100 |
| 1.Claridad | Esta formulado con lenguaje apropiado | | | | | | | | | | | **x** | | |
| 2.Objetividad | Se expresa la realidad como es, indica calidad de objetivo y la adecuación al objeto investigado | | | | | | | | | | | | **x** | |
| 3.Actualidad | Este acorde a los aportes recientes al derecho | | | | | | | | | | | **x** | | |
| 4.Organizacional | Existe una organización lógica | | | | | | | | | | | | | **x** |
| 5.Suficiencia | Cumple con los aspectos metodológicos | | | | | | | | | | | | **x** | |
| 6.Internacionalidad | Esta adecuado para valorar las categorías | | | | | | | | | | | **x** | | |
| 7.Coherencia | Se respalda en fundamentos técnicos y | | | | | | | | | | | **x** | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | científicos | | | | | | | | | | | | | |
| 8.Coherencia | Existe coherencia entre los problemas, objetivos, supuestos, basados en los aspectos teóricos y científicos | | | | | | | | | | | **x** | | |
| 9.Metodología | El instrumento responde al objetivo, diseño, tipo de la investigación. | | | | | | | | | | | **x** | | |
| 10.Pertinencia | El instrumento tiene sentido frente a un problema crucial, está situado en una población, es interdisciplinaria , tiene relevancia global y asume responsablement e las consecuencias de sus hallazgos | | | | | | | | | | | **x** | | |

**OPCIÓN DE APLICABILIDAD**

- El instrumento cumple con los requisitos de para su aplicación CUMPLE
- El instrumento cumple en parte con los requisitos para su aplicación CUMPLE
- El instrumento no cumple con los requisitos para su aplicación CUMPLE

PROMEDIO DE VALORACIÓN 94.5

……..

**Firma**

**Nombre:** Pedro Antonio Martinez Letona

**DNI:** 07943841

# ANEXO E: ALFA DE CONBRACH

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | | | | | | |
| 2 | | | LFA DE CRONBAC | | | | | | | | | | |
| 3 | Nº | SUJETOS | PREG. 1 | PREG. 2 | PREG. 3 | PREG. 4 | PREG. 5 | PREG. 6 | PREG. 7 | PREG. 8 | PREG. 9 | PREG. 10 | |
| 4 | 1 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 5 | 2 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 6 | 3 | x | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 20 |
| 7 | 4 | x | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 30 |
| 8 | 5 | x | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 40 |
| 9 | 6 | x | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 50 |
| 10 | 7 | x | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 30 |
| 11 | 8 | x | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 20 |
| 12 | 9 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 13 | 10 | x | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 20 |
| 14 | 11 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 15 | 12 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 16 | 13 | x | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 20 |
| 17 | 14 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 18 | 15 | x | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 20 |
| 19 | 16 | x | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 30 |
| 20 | 17 | x | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 50 |
| 21 | 18 | x | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 40 |
| 22 | 19 | x | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 30 |
| 23 | 20 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 24 | 21 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 25 | 22 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 26 | 23 | x | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 20 |
| 27 | 24 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 28 | 25 | x | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 30 |
| 29 | 26 | x | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 20 |
| 30 | 27 | x | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 20 |
| 31 | 28 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 32 | 29 | x | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 20 |
| 33 | 30 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 34 | 31 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 35 | 32 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 36 | 33 | x | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 40 |
| 37 | 34 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 38 | 35 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 39 | 36 | x | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 20 |
| 40 | 37 | x | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 20 |
| 41 | 38 | x | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 30 |
| 42 | 39 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 43 | 40 | x | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 |
| 44 | | | 1.35 | 1.35 | 1.35 | 1.35 | 1.35 | 1.35 | 1.35 | 1.35 | 1.35 | 1.35 | |
| 45 | | | | | | | | | | | | | |

**FORMULA**

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum Vi}{Vt}\right]$$

| | |
|---|---|
| K | 11 |
| Σ | 13.50 |
| V. TOTAL | 135 |

| ULTADO VALOR ALFA DE CRONB |
|---|
| 1 |