



**Autónoma**  
Universidad Autónoma del Perú

**FACULTAD DE DERECHO**  
**ESCUELA PROFESIONAL DE DERECHO**

**TESIS**

“LA IMPUNIDAD DE LOS HACKERS Y EL TRATAMIENTO DE DATOS PERSONALES  
DE LAS ENTIDADES FINANCIERAS, LIMA METROPOLITANA, 2022”

**PARA OBTENER EL TÍTULO DE**  
**ABOGADO**

**AUTORES**

EDSON JOSECARLO PALACIOS VALENCIA

ORCID: 0000-0002-4125-6307

MARÍA ROXANA NEYRA AREDO

ORCID: 0000-0001-8098-2216

**ASESOR**

MG. URBIZAGASTEGUI SILVESTRE, VICTOR MANUEL

ORCID: 0000-0002-3849-3299

**LÍNEA DE INVESTIGACIÓN**

PERSONA, SOCIEDAD, EMPRESA Y ESTADO

**LIMA, PERÚ, JULIO 2024**



**CC BY**

<https://creativecommons.org/licenses/by/4.0/>

*Esta licencia permite a otros distribuir, mezclar, ajustar y construir a partir de su obra, incluso con fines comerciales, siempre que le sea reconocida la autoría de la creación original. Esta es la licencia más servicial de las ofrecidas. Recomendada para una máxima difusión y utilización de los materiales sujetos a la licencia.*

## Referencia bibliográfica

Neyra Aredo, M. R., & Palacios Valencia, E. J. (2022). *La Impunidad de los Hackers y el Tratamiento de Datos Personales de las Entidades Financieras, Lima Metropolitana, 2022* [Tesis de pregrado, Universidad Autónoma del Perú]. Repositorio de la Universidad Autónoma del Perú.

## HOJA DE METADATOS

Datos del autor	
Nombres y apellidos	Maria Roxana Neyra Aredo
Tipo de documento de identidad	DNI
Número de documento de identidad	43020086
URL de ORCID	<a href="https://orcid.org/0000-0001-8098-2216">https://orcid.org/0000-0001-8098-2216</a>
Datos del autor	
Nombres y apellidos	Edson Josecarlo Palacios Valencia
Tipo de documento de identidad	DNI
Número de documento de identidad	70889885
URL de ORCID	<a href="https://orcid.org/0000-0002-4125-6307">https://orcid.org/0000-0002-4125-6307</a>
Datos del asesor	
Nombres y apellidos	Victor Manuel Urbizagastegui Silvestre
Tipo de documento de identidad	DNI
Número de documento de identidad	41072118
URL de ORCID	<a href="https://orcid.org/0000-0002-3849-3299">https://orcid.org/0000-0002-3849-3299</a>
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Yurela Kosett Yunkor Romero
Tipo de documento	DNI
Número de documento de identidad	20118250
Secretario del jurado	
Nombres y apellidos	Rafael Americo Torres Sotelo
Tipo de documento	DNI
Número de documento de identidad	21812076
Vocal del jurado	
Nombres y apellidos	Judith Beatriz Garcia Galindo
Tipo de documento	DNI
Número de documento de identidad	10179290

<b>Datos de la investigación</b>	
<b>Título de la investigación</b>	La Impunidad de los Hackers y el Tratamiento de Datos Personales de las Entidades Financieras, Lima Metropolitana, 2022.
<b>Línea de investigación Institucional</b>	Persona, Sociedad, Empresa y Estado
<b>Línea de investigación del Programa</b>	Enfoque Interdisciplinario de la Ciencia Jurídica
<b>Línea de acción RSU</b>	Salud y Bienestar
<b>URL de disciplinas OCDE</b>	<a href="https://purl.org/pe-repo/ocde/ford#5.05.01">https://purl.org/pe-repo/ocde/ford#5.05.01</a>

**FACULTAD DE DERECHO**  
**ESCUELA PROFESIONAL DE DERECHO**  
**ACTA DE SUSTENTACIÓN DE TESIS**

En la ciudad de Lima, el jurado de sustentación de tesis conformado por: la DRA. YURELA KOSETT YUNKOR ROMERO como presidenta, el MG. RAFAEL AMERICO TORRES SOTELO como secretario y la DRA. JUDITH BEATRIZ GARCIA GALINDO como vocal, reunidos en acto público para dictaminar la tesis titulada:

**LA IMPUNIDAD DE LOS HACKERS Y EL TRATAMIENTO DE DATOS  
PERSONALES DE LAS ENTIDADES FINANCIERAS, LIMA ,METROPOLITANA,  
2022.**

Presentado por el bachiller:  
**EDSON JOSECARLO PALACIOS VALENCIA**

Para obtener el **Título Profesional de Abogado**; luego de escuchar la sustentación de la misma y resueltas las preguntas del jurado se procedió a la calificación individual, obteniendo el dictamen de **Aprobado** con una calificación de **DOCE (12)**.

En fe de lo cual firman los miembros del jurado, el 04 de diciembre del 2024



**PRESIDENTE**  
DRA. YURELA KOSETT  
YUNKOR ROMERO



**SECRETARIO**  
MG. RAFAEL AMERICO  
TORRES SOTELO



**VOCAL**  
DRA. JUDITH BEATRIZ  
GARCIA GALINDO

**FACULTAD DE DERECHO**  
**ESCUELA PROFESIONAL DE DERECHO**  
**ACTA DE SUSTENTACIÓN DE TESIS**

En la ciudad de Lima, el jurado de sustentación de tesis conformado por: la DRA. YURELA KOSETT YUNKOR ROMERO como presidenta, el MG. RAFAEL AMERICO TORRES SOTELO como secretario y la DRA. JUDITH BEATRIZ GARCIA GALINDO como vocal, reunidos en acto público para dictaminar la tesis titulada:

**LA IMPUNIDAD DE LOS HACKERS Y EL TRATAMIENTO DE DATOS  
PERSONALES DE LAS ENTIDADES FINANCIERAS, LIMA ,METROPOLITANA,  
2022.**

Presentado por la bachiller:  
**MARIA ROXANA NEYRA AREDO**

Para obtener el **Título Profesional de Abogada**; luego de escuchar la sustentación de la misma y resueltas las preguntas del jurado se procedió a la calificación individual, obteniendo el dictamen de **Aprobado** con una calificación de **DOCE (12)**.

En fe de lo cual firman los miembros del jurado, el 04 de diciembre del 2024



**PRESIDENTE**  
DRA. YURELA KOSSET  
YUNKOR ROMERO



**SECRETARIO**  
MG. RAFAEL AMERICO  
TORRES SOTELO



**VOCAL**  
DRA. JUDITH BEATRIZ  
GARCIA GALINDO

## ACTA DE APROBACIÓN DE ORIGINALIDAD

Yo Víctor Manuel Urbizagastegui Silvestre docente de la Facultad de Derecho de la Escuela Profesional de Derecho de la Universidad Autónoma del Perú, en mi condición de Asesor de la tesis titulada:

**La Impunidad de los Hackers y el Tratamiento de Datos Personales de las Entidades Financieras, Lima Metropolitana, 2022.**

De los bachilleres Maria Roxana Neyra Aredo y Edson Josecarlo Palacios Valencia, certifico que la tesis tiene un índice de similitud de 18% verificable en el reporte de similitud del software Turnitin que se adjunta.

El suscrito revisó y analizó dicho reporte a lo que concluyó que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Autónoma del Perú.

Lima, 10 de diciembre de 2024



---

Víctor Manuel Urbizagastegui Silvestre

DNI: 41072118





## **DEDICATORIA**

La siguiente tesis va dedicada a mis familiares, que viene siendo mi soporte en toda la etapa de mi carrera, a mis docentes, que me han permitido poder adquirir conocimientos.

**Edson Josecarlo Palacios Valencia**

La siguiente tesis va dedicada a mi familia y docentes que me han permitido poder adquirir conocimientos no solo basados en mi carrera, sino también, de su experiencia profesional.

**María Roxana Neyra Aredo**

## **AGRADECIMIENTOS**

Agradecer a mi centro de estudios, la Universidad Autónoma del Perú, que me acogió durante esta hermosa etapa estudiantil, brindándome sus instalaciones, maestros y material de estudio que me nutren de conocimientos para poder desarrollarme como futuro profesional; a mi asesor de tesis el Dr. Víctor Manuel Urbizagastegui Silvestre, por sus constantes recomendaciones, apoyo, guía y orientación al desarrollo de trabajo de investigación.

**Edson Josecarlo Palacios Valencia**

Agradezco a mi asesor de tesis el Dr. Víctor Manuel Urbizagastegui Silvestre, por sus constantes recomendaciones, apoyo, guía y orientación a mi desarrollo de trabajo de investigación; a mis familiares, que son mi motivo de seguir avanzando y para finalizar doy gracias a aquellas personas que me motivaron a poder realizar y concluir este importante trabajo de investigación para poder culminar mi carrera.

**María Roxana Neyra Aredo**

## INDICE

<b>DEDICATORIA</b> .....	2
<b>AGRADECIMIENTOS</b> .....	3
<b>LISTA DE TABLAS</b> .....	5
<b>LISTA DE FIGURAS</b> .....	6
<b>RESUMEN</b> .....	7
<b>ABSTRACT</b> .....	8
<b>CAPITULO I: INTRODUCCIÓN</b> .....	9
<b>CAPÍTULO II: METODOLOGÍA</b> .....	10
2.1. Tipo y diseño de investigación .....	35
2.2. Población, muestra y muestreo.....	35
2.3. Hipótesis. ....	35
2.4. Variables y Operacionalización .....	37
2.5. Técnicas e instrumentos de recolección de datos, validez y confiabilidad.....	37
2.6. Procedimientos.....	38
2.7. Análisis de Datos.....	38
2.8. Aspecto Ético .....	38
<b>CAPITULO III: RESULTADOS</b> .....	39
<b>CAPITULO IV: DISCUSIÓN</b> .....	49
<b>CAPITULO V: CONCLUSIONES</b> .....	50
<b>CAPITULO VI: RECOMENDACIONES</b> .....	56
<b>REFERENCIAS</b>	
<b>ANEXOS</b>	

## LISTA DE TABLAS

Tabla 1	Tabla de variables y dimensiones
Tabla 2	Descripción de la pregunta 1 de la variable Impunidad de los hackers
Tabla 3	Descripción de la pregunta 2 de la variable Impunidad de los hackers
Tabla 4	Descripción de la pregunta 3 de la variable Impunidad de los hackers
Tabla 5	Descripción de la pregunta 4 de la variable Tratamiento de datos personales
Tabla 6	Descripción de la pregunta 5 de la variable Tratamiento de datos personales
Tabla 7	Descripción de la pregunta 6 de la variable Tratamiento de datos personales
Tabla 8	Descripción de la pregunta 7 de la variable 1
Tabla 9	Descripción de la pregunta 8 de la variable 2
Tabla 10	Descripción de la pregunta 9 de la variable 1
Tabla 11	Para el objetivo general: La impunidad de los hackers se relaciona significativamente con el tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022
Tabla 12	Para el objetivo específico 1: La impunidad de los hackers se relaciona significativamente con el acceso tratamiento
Tabla 13	Para el objetivo específico 2: La impunidad de los hackers se relaciona significativamente con el acceso tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022

**LISTA DE FIGURAS**

- Figura 1 De la primera pregunta de la primera variable
- Figura 2 De la segunda pregunta de la primera variable
- Figura 3 De la tercera pregunta de la primera variable
- Figura 4 De la cuarta pregunta de la segunda variable
- Figura 5 De la quinta pregunta de la segunda variable
- Figura 6 De la sexta pregunta de la segunda variable
- Figura 7 De la séptima pregunta de la variable 1
- Figura 8 De la octava pregunta de la variable 2
- Figura 9 De la novena pregunta de la variable 02

**LA IMPUNIDAD DE LOS HACKERS Y EL TRATAMIENTO DE DATOS  
PERSONALES DE LAS ENTIDADES FINANCIERAS, LIMA METROPOLITANA, 2022**

**MARÍA ROXANA NEYRA AREDO  
EDSON JOSECARLO PALACIOS VALENCIA**

**UNIVERSIDAD AUTÓNOMA DEL PERÚ**

**RESUMEN**

En la presente tesis: la impunidad de los hackers y el tratamiento de datos personales de las entidades financieras, Lima Metropolitana 2022. Técnica usada es la encuesta y utilizaremos uno de los instrumentos para recopilar datos del cuestionario, donde la población y muestra estará constituida por 60 ciudadanos de Lima Metropolitana. El objeto de nuestra tesis es Determinar, de qué manera la impunidad de los hackers se relaciona con el tratamiento de datos personales de las entidades financieras de Lima Metropolitana 2022. Para la obtener efectos, hemos recurrido a diversas investigaciones doctrinarias y legislativas tanto nacionales e internacionales. Como una de las conclusiones tenemos que los resultados muestran que la impunidad de los hackers si se relaciona significativamente con el tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022 en este sentido si se cumplió con conocer que la impunidad de los hackers se relaciona significativamente con el tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.

**Palabras clave:** impunidad, delitos informáticos, hackers, tratamiento de datos personales

**THE IMPUNITY OF HACKERS AND THE PROCESSING OF PERSONAL DATA OF  
FINANCIAL ENTITIES, METROPOLITAN LIMA, 2022**

**MARÍA ROXANA NEYRA AREDO**

**EDSON JOSECARLO PALACIOS VALENCIA**

**UNIVERSIDAD AUTÓNOMA DEL PERÚ**

**ABSTRACT**

In this thesis: the impunity of hackers and the processing of personal data of financial entities, Metropolitan Lima 2022. The technique used is the survey and we will use one of the instruments to collect data from the questionnaire, where the population and sample will consist of 60 citizens of Metropolitan Lima. The object of our thesis is to determine how the impunity of hackers is related to the processing of personal data of the financial entities of Metropolitan Lima 2022. To obtain effects, we have resorted to various doctrinal and legislative investigations, both national and international. As one of the conclusions, we have that the results show that the impunity of hackers is significantly related to the processing of personal data of financial entities, Metropolitan Lima, 2022. In this sense, it was true to know that the impunity of hackers is significantly related to the processing of personal data of financial entities, Metropolitan Lima, 2022.

**Keywords:** impunity, computer crimes, hackers, processing of personal data

# **CAPÍTULO I: INTRODUCCIÓN**



En la presente investigación, abordaremos “La Impunidad de los Hackers y el Tratamiento de Datos Personales de las Entidades Financieras, Lima Metropolitana, 2022” que hoy en día, muchos ciudadanos se han visto afectados por los hackers, quienes vulneran el derecho a la identidad personal y suplantan sus identidades. De esta manera, los hackers, logran obtener beneficios económicos, debido a que, al usurpar la identidad de ciertas personas, logran solicitar y obtener créditos personales, ya sean por compras en línea, o por la obtención de créditos personales, puesto que las entidades financieras, solicitan datos personales de los clientes, que, los mismos hackers ya lo obtuvieron.

No se puede subestimar el impacto social de los ciberataques a las entidades financieras, ya que pueden provocar daños importantes a su reputación, lo que se traduce en una posible pérdida de clientes y de cuota de mercado. Esto, a su vez, puede tener efectos perjudiciales sobre la estabilidad y rentabilidad de sus negocios. Ser víctima de un ciberataque importante exponen vulnerabilidades que pueden erosionar la confianza no sólo entre socios comerciales como bancos, instituciones financieras, proveedores y distribuidores, sino también entre clientes que pueden dudar en establecer o mantener una relación con una organización que ha experimentado tal ataque. un ataque (Hernández, 2005).

Las entidades financieras también experimentan importantes consecuencias económicas, incluidas pérdidas financieras y gastos adicionales, que impactan en gran medida sus operaciones. Estos gastos abarcan diversos aspectos como la adquisición de software y sistemas digitales, orientación tecnológica especializada, así como la contratación de personal (Olivares, 2024).

Peralta & Limones, reconocidos autores de Cultura Organizacional y Liderazgo, describe tres niveles distintos de cultura organizacional. El nivel inicial abarca las creencias inconscientes arraigadas dentro de la organización. El segundo nivel comprende los valores, la misión, la estrategia, los procesos cognitivos y el conocimiento de la organización. Por último, el tercer nivel engloba las normas, rituales, hábitos y lenguajes empleados dentro de la organización (Peralta & Limones, 2023). Sin embargo, estos elementos niveles de la cultura organizacional se a ver severamente afectados cuando los piratas informáticos violan con éxito la medida de seguridad que salvaguardan los datos personales de los clientes.

Cuando se trata del ámbito de la tecnología y la ciencia, los piratas informáticos emplean una variedad de software malicioso, incluidos virus, troyanos, ransomware y software espía, para infiltrarse en los sistemas y robar información confidencial o infligir daños. Vale la pena señalar que estas son sólo algunas de las tácticas empleadas por los piratas informáticos, ya que sus métodos y estrategias evolucionan constantemente. Para cuidarse contra estos ataques, es imperativo poner en marcha medidas de seguridad sólidas, como la implementación de contraseñas con eficacia, actualizar periódicamente el software y los sistemas, educar a los empleados sobre la seguridad en línea y emplear herramientas de seguridad como firewalls y programas antivirus. Mantener la conciencia y permanecer siempre alerta son cruciales para defenderse contra las amenazas de los piratas informáticos en el panorama digital actual (Peña, 2020).

Los delitos informáticos no solo se conocen desde ahora, ello inició desde los años 60 por la fobia infundida de la literatura de antaño relacionada en recopilar y almacenar

datos personales. Se puede obtener como referente el libro de 1984 de George Orwell, actor más conocido como omnipresente Gran Hermano, donde puede controlar y monitorear las vivencias de los individuos por medio de diferentes tecnologías. La determinación "delito informático" comenzó a manifestarse inicialmente desde que se pudieron publicar secciones periodísticas sobre ciertos delitos fundamentales sucedidos en esos tiempos, luego de un periodo a este tipo de hechos se los conoció como "ciberpunk". Desde 1970 empezaron a registrarse varios hechos de delitos informáticos, causando enormes pérdidas en el sector privado, siendo tales: como vigilancia informática, robo de software, avería y usurpación. Desde principios de la década de 1980, los delitos informáticos se dieron a conocer a medida que el número de casos de fraude aumentaba rápidamente y las organizaciones internacionales tomaron cartas en el asunto y abordaron el problema (Acosta, Benavides, & Garcia, 2020).

En el mundo se ha evidenciado el incremento y suma importancia relevante en cara a la población. El solo hecho de ofrecer servicios que permitan que los usuarios se les simplifiquen las cosas en un momento determinado, sobre todo para comunicarse e informarse, lo hace una herramienta útil y en muchos casos, necesaria (Marquez & Mousalli, 2016).

Resulta increíble la posibilidad de acceder a tanta información, tan diversa y tan pública, a la mano de cualquier usuario, en la historia de la humanidad (Trejo, 2006). Hoy en día, existe una gran variedad de contenidos al respecto, tales como wikis, bibliotecas virtuales, chat, correo electrónico, videoconferencias, firmas electrónicas, foros, blogs, robótica, entre otros, que facilitan cualquier tipo de interacción masiva, sin tomar en consideración edad, género o nivel económico, que se apoyan en estos contenidos para

entretenerse, socializar, buscar información desde la comodidad de la casa, oficina o cualquier ambiente donde exista la conexión (Marquez & Mousalli, 2016).

El aumento exponencial de los peligros cibernéticos ha sido sustancial. Por ejemplo, la aparición de ataques de ransomware se triplicó en 2021 y 2022 en comparación con el año anterior, lo que subraya la importancia de la ciberseguridad para las instituciones financieras. El informe de Sophes revela que un asombroso 65% de las organizaciones financieras fueron víctimas de ataques de ransomware en 2024, lo que significa un aumento notable con respecto a años anteriores (Melo, 2021)

A nivel nacional, Según directiva de la Superintendencia de Banca, Seguros y AFP (SBS), las empresas que operan en el sector financiero y tienen presencia en línea ahora deben establecer un programa integral de ciberseguridad. Esto implica garantizar una protección sólida contra amenazas potenciales, identificar rápidamente cualquier incidente, responder rápidamente y recuperarse de cualquier interrupción tecnológica que pueda surgir. Además, las instituciones financieras están obligadas a notificar oportunamente a la SBS en caso de cualquiera de los siguientes eventos: pérdida o robo de información de la empresa o de clientes, casos de fraude interno o externo, cualquier incidente que potencialmente pueda dañar la reputación o imagen de la empresa, así como cualquier interrupción en las operaciones normales.

Asimismo, la (DIVINDAT), manifestó que pudieron investigar 1,188 denuncias sobre quebrantamientos cibernéticos esto relacionados al fraude de los mismos y a la suplantación de identidad. Si el problema persistiera y no se llegaría a una solución frente a este tipo de delitos, se incrementaría el índice de porcentaje de personas afectadas, perjudicando su récord crediticio y posibles procesos judiciales por partes de la entidades

financieras, por la cual, buscaremos métodos de alternativas de solución, para combatir y contrarrestar estos tipos de delitos; con la implementación de juzgados especializados en delitos cibernéticos; asimismo, proponer que las entidades financieras, utilicen nuevos mecanismos de verificación de datos personales, como el uso obligatorio de huellas dactilares, asimismo, el reconocimiento facial; como problema general, tenemos la siguiente pregunta: ¿Cómo la impunidad de los hackers se relaciona con el tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022?; como problemas específicos tenemos las siguientes preguntas: ¿Cómo la impunidad de los hackers se relaciona con la extracción de tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022?; ¿Cómo la impunidad de los hackers se relaciona con el acceso tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022?

La presente investigación, es realizada, debido a las constantes denuncias públicas que hemos podido observar y advertir en nuestra ciudad de Lima Metropolitana. En cuanto a la justificación teórica del presente trabajo que se está realizando, nos basamos en un análisis cuyos conceptos tienen carácter de doctrina, jurisprudencias y datos de estadística en cara a los delitos informáticos como son la vulneración de los derechos reconocidos a la privacidad personal, donde todo ello nos conlleva a ofrecer un mejor análisis de los distintos patrones de delitos informáticos, resaltando los hechos delincuenciales que van en oposición al principio y derecho de la vida privada, en la localidad de Lima – Metropolitana; en cuanto a nuestra justificación metodológica, la presente investigación, nos permitirá generar un análisis sobre este problema que se tiene en la actualidad, dándole un énfasis netamente jurídico; el cual se relaciona con los

materiales bibliográficos buscados; que llevarán como pilar a posteriores trabajos de investigación de este problema que atraviesa la sociedad, aplicando el método científico para su elaboración; asimismo, es relevante socialmente, puesto que gracias a las especializaciones existentes, la exposición digital y la cooperación internacional se puede dar a conocer fácilmente a los “delincuentes informáticos”, por lo que trascenderá en mejora de la ciudadanía sobre la dirección de justicia. Por cuanto, está presente investigación, tiene como objetivo brindar alternativas de solución, tanto como a las entidades financieras y asimismo a la ciudadanía.

**Objetivo General:** Determinar, de qué manera la impunidad de los hackers se relaciona con el tratamiento de datos personales de las entidades financieras de Lima Metropolitana 2022.

**Objetivos Específicos:**

- Determinar, cómo la impunidad de los hackers se relaciona con la extracción de datos personales de las entidades financieras, Lima Metropolitana, 2022.
- Determinar, cómo la impunidad de los hackers se relaciona con el acceso al tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.

En cuanto a las limitaciones que estamos obteniendo en la presente elaboración de nuestra tesis, son: la búsqueda de antecedentes bibliográficos, el tiempo de ejecución de la presente tesis, el horario laboral, la escasa información de datos relacionados con nuestras variables.

Como antecedentes internacionales: se realizan con mucha más frecuencia en Colombia, por su gran evolución y origen de la era digital, el área de la informática tele comunicativa. Es así que podemos observar el avance de los métodos, técnicas o

herramientas de aplicativos a dispositivos hardware que fueron creados para dar facilidad a los robos cibernéticos, que cada vez se incrementa con las diversas maniobras criminales al atentar contra la confidencialidad de la población, de tal manera que vulneran los bienes que no deben ser tocados, así como los de valor económico de la población que vienen siendo víctimas de los ataques o delitos informáticos. Por lo que con la presente investigación demuestra que aún falta normatividad en Colombia que logre abarcar todos los ámbitos de seguridad informática y que pueda sancionar correctamente este tipo de incidentes, que dejan daños en todos los entornos de desarrollo y crecimiento del país.

(Zambrano, 2023), en su tesis titulada *“Ciberdelitos y las dificultades que tiene la justicia para prevenir y sancionar estos actos delictivos”*, hace referencia que la ciberdelincuencia incluye aquellos delitos cometidos contra la seguridad de las computadoras y sistemas de información, buscando acceder de forma no autorizada a un dispositivo, o bloquear el acceso del usuario legítimo. Se puede decir que un ciberdelincuente viene ser aquel tipo que detecta los puntos débiles de algunos medios sociales: tales son la sustracción de información, extorsión, ventilación de algunas informaciones confidenciales, repartimiento de obscenidad infantil, entre otros. Asimismo, aprovechando la red de equipos conectados, sea de forma pública o privada, o por medio de un sistema informático, busque vulnerar todo lo relacionado con la confidencialidad, así como la integridad y también la disponibilidad de los sistemas informáticos, además del empleo de los sistemas, redes y datos de forma fraudulenta.

(Peña, 2007), en su artículo titulado *“Estudio dogmático de los delitos de cohecho y sus perspectivas políticos criminales”*, menciona que las conductas realizadas por el

sujeto activo en esta clase de delito abarcan diferentes tipos de atentados en contra de diferentes bienes jurídicos protegidos según el caso. Ejemplo de ello, a primera vista, al patrimonio, este tipo de proceder afecta a las proximidades personales, y; otro provecho jurídico quien se ve afectado de manera directa como también a la protección nacional. Suelen ser comportamientos destinados y van contrarias a la reserva, plenitud y disponibilidad del sistema informática, medios sociales o referencia, así como el exceso de algunos sistemas. A ello, se debe agregar una característica esencial de los delitos informáticos, tomando en cuenta que los mismos son una forma conductual de crimen transnacional, es decir que puede ser cometido en cualquier parte del mundo y afectar a una persona a un grupo de personas o países diferentes y lejanos del lugar del cometimiento físico del mismo (Zambrano, 2023)

La finalidad es de comparar la impresión que trae la putrefacción y también la inmunidad que contiene vulneraciones a derechos fundamentales. Por esto, pudieron realizar distintos ejemplos de estadísticas. Se visualizó que hay algunas categorías de vulneraciones para algunos derechos fundamentales que están incluidos en actos de putrefacción. Algunas de las medidas que ni la acción de putrefacción ni esas vulneraciones sean sancionadas, las impunidades se transforman en un entorno donde se promueve al ejecutor a dirigirse con las mismas acciones de putrefacción, lo que logra generar distintas vulneraciones a los derechos humanos. Cuando la corrupción y la impunidad se conjugan, ambas se convierten en patrones estructurales de violaciones a los derechos humanos (Ortiz & Vasquez, 2021).

(Trejo, 2006); en este proyecto culminante, se exploran los puntos focales de la ciberseguridad en la industria financiera actual, con el objetivo de obtener información



sobre su trayectoria futura. Para lograr esto, se lleva a cabo un examen del panorama cibernético actual, que proporciona una aclaración de varios tipos de amenazas y vulnerabilidades. La comprensión de los elementos más significativos es posible examinando el panorama actual de las ciberamenazas, los individuos responsables de su creación y los patrones que han surgido en los últimos años. Las implicaciones de la ciberseguridad para las empresas y las repercusiones resultantes son consideraciones importantes. Además, el análisis de la ciberseguridad en las instituciones es el eje central del trabajo, a incluir las medidas implementadas por las empresas para combatir los ataques. La seguridad de los datos es de suma importancia, como lo demuestra este estudio en el ámbito financiero. Las cuentas bancarias, debido a la información sensible que contienen, son muy buscadas por los ciberatacantes. Como resultado, el enfoque principal de este trabajo es abordar los desafíos y obstáculos asociados con la seguridad de estas cuentas. En relación con la seguridad de las instituciones financieras, ha habido avances notables. La defensa de la organización puede fortalecerse abordando los aspectos técnicos y humanos de la ciberseguridad, lo que implica capacitar y desarrollar a los empleados. Además, se reconoce la importancia del Director de Seguridad de la Compañía (CISO). El propósito de este esfuerzo es prever el futuro basándose en la información disponible y los esfuerzos colaborativos de su equipo. ¿Se adaptará el campo de la ciberseguridad en sincronía con el panorama en constante evolución de las amenazas cibernéticas, o es capaz de prever y contrarrestar estas amenazas de forma preventiva?

(Acosta, Benavides, & Garcia, 2020) En su investigación señala que el uso indebido de la tecnología para realizar actividades ilícitas, como violar la privacidad de

las personas y manipular o extraer datos de servidores y dispositivos, constituye delitos informáticos. El propósito de este estudio es encontrar las principales categorías de delitos informáticos que plantean riesgos para la sociedad, las empresas y los gobiernos. Esta investigación adopta una combinación de enfoques confirmatorios y exploratorios, profundizando en teorías y leyes relevantes. Los hallazgos subrayan la importancia de identificar diversos delitos informáticos y reconocer vulnerabilidades en la seguridad de la red para mitigar su proliferación. En definitiva, los delitos informáticos engloban ilícitas realizadas a través del ciberespacio, con el objetivo de causar daño, desprestigiar o extorsionar a personas que utilizan medios electrónicos y redes de Internet.

Como antecedentes nacionales: (Álvarez & Montoya, 2020); en la labor de investigador de título "*Sombras de la normativa que propone el aumento de la ciberdelincuencia*" el cual se realizó en la U.N.J.F.S.C.H –Perú. Con la obtención del nombre profesional Abogado, Llegó a algunas determinaciones: Que el ejercicio actual de la norma vigente establece la ciberdelincuencia en Lima 2015, contraviniendo en varias discusiones debido a que es una ventana para su estricta sanción que incide de manera resalta en la forma de cómo se le da dicha protección a la ciudadanía, su negativa atribución puede causar un lamentable impacto social. De igual forma se logró indicar que si en el día a día se genera tantas faltas, se devendría en ilegal, y por lo mismo se podría genera en inconstitucionalidad. Esto genera que una gran parte afecte la Constitución. Señalar también la evidente falta de conocimiento informático que es un factor determinante en el desconcierto de las vulneraciones informáticas de la humanidad, los trabajadores de justicia cada día deberían de tener mayor conocimiento tecnológico de información. En nuestra actualidad es un poco riesgoso hacer negocios

vía Web ya que los instrumentos legales no garantizan con un adecuado marco legal para su efectividad.

(Arapa et al.,2024) señala en su trabajo *“Implementación de programas de cumplimiento en ciberseguridad como una práctica de buen gobierno corporativo en las entidades que forman parte del sistema financiero peruano”* para la Pontificia Universidad Católica del Perú ,que a pesar de las numerosas oportunidades y avances que brinda la tecnología, ciertas industrias como el comercio minorista, el consumo y las finanzas han experimentado importantes impactos negativos debido al aumento de los ciberataques. Como resultado, se ha vuelto crucial que las entidades dentro del sistema financiero peruano establezcan diferentes programas para cumplir con la ciberseguridad como parte de sus prácticas de gobierno corporativo. Este sector, al ser muy susceptible a este tipo de incidentes, desempeña un papel vital en la economía de nuestro país. Para comprender plenamente la complejidad de este tema, este estudio tiene como objetivo explorar conceptos clave y extraer ideas de experiencias en otros países. Al examinar la gravedad y las consecuencias de los ciberataques, podemos comprender mejor las medidas esenciales que se pueden implementar en nuestro propio país. Dada la ausencia de regulaciones nacionales relacionadas con la ciberseguridad en el sistema financiero peruano, es crucial establecer programas con cumplimientos de ciberseguridad en todas las entidades relevantes. Para garantizar la implementación de prácticas sólidas de gobierno corporativo, se deben considerar e incorporar ciertos elementos clave en las operaciones de estas instituciones financieras.

(Brito, 2023) manifestó en su estudio *“Mejoramiento de la seguridad de la información para reducir los ciberataques del tipo phishing en una entidad financiera”*,

realizada para la Universidad Tecnológica del Perú; donde se plantea como objetivo general mejorar la seguridad de la información y mitigar los ciberataques de phishing dentro de una institución financiera. Para conseguir este objetivo se utiliza medidas con metodología descriptiva y no experimental. La implementación de la plataforma Gophish se utiliza para reforzar la seguridad de la información y combatir los ciberataques de phishing. Para evaluar la efectividad de esta implementación, se realiza un análisis de los antes y el después de una campaña de phishing. Como resultado, hay una reducción significativa del 40% en la cantidad de personas que hacen clic en enlaces de correo electrónico de phishing. Esta reducción se considera satisfactoria, ya que el objetivo final es minimizar este número al máximo. Además, hay una notable disminución del 67,36% en el número de usuarios que, sin saberlo, proporcionan información a través de formularios de correo electrónico fraudulentos de phishing. Esta reducción se considera válida, ya que la intención es evitar que cualquier usuario sea víctima de ataques de phishing y revelar información sensible como nombres de usuario y contraseñas. Además, hay un aumento sustancial del 57,14% en el número de usuarios que denuncian correos electrónicos de phishing. Este aumento se considera un progreso positivo, ya que se espera que más usuarios informen proactivamente de estos casos al encontrar correos electrónicos de phishing.

(Cruz, 2017); en su investigación sobre: "Los Hackers: Delito Informático frente al Código Penal Peruano", para obtener el título profesional de Abogado, de la Universidad Nacional Santiago Antúnez de Mayolo. Huaraz-Ancash-Perú, indica que la finalidad de esta investigación que se ha tomado como referente, es de evidenciar de huecos legales en nuestro ordenamiento penasl vigente, precisamente en transmisiones de signos

electrónicos comercial, para de esta manera tener definido la significación de forma jurídica, disminuir esta forma de asitas, disminuyendo el choque que perjudica a la humanidad de manera amplia y manera específica en las garantías fundamentales, dando a conocer mejoras para su modificación.

En relación a los antecedentes locales, se tiene el estudio de (Bustillos & Rojas, 2023) quien sostiene que en el Perú existen estándares establecidos para abordar los delitos informáticos y el cibercrimen. Estas regulaciones incluyen la regla de neutralidad de la red, que permite bloquear nombres de dominio y aplicaciones informáticas maliciosas. Además, este trabajo destaca casos específicos relacionados con estos temas.

La normativa en Perú en materia de ciberseguridad y seguridad de la información, junto con la utilización de la geolocalización en la investigación de actividades delictivas específicas. Mediante la utilización de la biometría de huellas dactilares, se pueden poner de relieve casos destacados relacionados con la lucha contra el cibercrimen y la delincuencia, incluidos el caso Pirate Bay, el caso Picap y un caso de robo de identidad

(Dávila, 2018); el propósito de este trabajo señala es examinar los efectos de los delitos cibernéticos en la gestión operativa, financiera y la reputación institucional de los principales bancos de Lima Metropolitana, específicamente BCP y BBVA, durante los últimos cinco años. Estos delitos ocurren predominantemente en el ámbito digital, lo que dificulta que las instituciones financieras los controlen por completo. La hipótesis inicial sugiere que ha habido cambios en los procesos operativos y una mayor inversión en tecnologías de la información para la ciberseguridad, lo que ha resultado en una pérdida de credibilidad y daño a la imagen de bancos destacados en el Perú, como el BBVA

Banco. Continental y el BCP de Lima Metropolitana. También se descubrió que, si bien ambos bancos reconocen el aumento de los delitos cibernéticos, no han asignado un presupuesto sustancial para la ciberseguridad. Aunque ha habido cierto crecimiento anual, todavía es insuficiente en comparación con los esfuerzos de los bancos de otros países.

Cuando se habla del concepto de delito, este implica inherentemente la presencia de un estado de criminalidad o la violación de las leyes, que en última instancia atenta contra la integridad de los demás (Duque et al., 2017). En este contexto particular, el crimen organizado ha experimentado crecimiento y desarrollo a lo largo del tiempo, en gran medida debido a la evolución general del sistema y la expansión de las redes criminales a través de las fronteras. La gama de actividades delictivas es amplia y puede variar dependiendo de factores como la ubicación, las oportunidades y otras variables, lo que permite su proliferación en numerosos países. Según Espinoza (2022), existe una notoria tendencia hacia actos delictivos dirigidos al sector empresarial, ya que éste se convierte en un objetivo prioritario para individuos con tendencias antisociales, muchas veces explotando las vulnerabilidades dentro de los sistemas de seguridad de las organizaciones.

La llegada de la modernización ha revolucionado la forma en que se gestiona la información, utilizando procesadores informáticos para almacenar grandes cantidades de datos y permitiendo un acceso rápido y eficiente. Esta información abarca varias categorías, como personal, comercial, financiera y corporativa, lo que la convierte en un objetivo atractivo para individuos conocidos como delincuentes informáticos que buscan explotarla para su propio beneficio. Estos delincuentes emplean tácticas como el

chantaje, la difamación e incluso el secuestro de información robada. Nuestra era actual se caracteriza por cambios rápidos y constantes (Acosta, Benavides&García,2020). En este contexto, Peña (2007) explica que en el pasado podíamos estar seguros de que muy pocas personas, si es que había alguna, podrían acceder a información sobre nuestra vida privada a través de Internet.

Según Zambrano (2023), los datos informáticos se han transformado en parte general de la vida diaria de las personas, lo que ha aumentado su importancia. En consecuencia, este valor elevado también conlleva un mayor riesgo. Existen personas que se centran únicamente en cometer delitos cibernéticos, ya sea para beneficio personal o para crear titulares sensacionalistas en torno a un incidente en particular.

El delito informático, como se mencionó anteriormente, es una forma de actividad delictiva que surge de los avances tecnológicos. Impregna varios aspectos de la vida cotidiana, particularmente dentro de organizaciones y corporaciones que deben asignar importantes recursos financieros para salvar su información. Sin embargo, es crucial no pasar por alto los vacíos legales que surgen en relación con estos temas, ya que tienen el potencial de comprometer la integridad, la ética y el intelecto de personas y empresas (Acosta, Benavides & García, 2020). El doctor Brito (2023) sostiene que estos vacíos legales dan lugar a lo que combinados se conocen como “paraísos informáticos” o “paraísos cibernéticos”, que ocurren cuando una entidad específica explota las deficiencias en las regulaciones o leyes relativas a los delitos informáticos.

Según Dávila (2018), un asombroso 95% de los delitos relacionados con la cibernética en Madrid, España, siguen sin resolverse. Esta alarmante estadística está respaldada por datos del Ministerio del Interior, que enfatizan las importantes

implicaciones nacionales y globales del ciberdelito. No sólo representa una intimidación para la sociedad y la economía, sino que también pone en riesgo en la mayoría de la población, poniendo en peligro la infraestructura personal, financiera y, lo más importante, la infraestructura crítica.

La falta de medidas de ciberseguridad es un factor recurrente que contribuye a la ocurrencia de ciberdelitos y su impunidad. Este problema ha atraído la atención mundial, lo que ha llevado a los gobiernos y de todo el mundo a reconocer la importancia de proteger los datos informáticos e implementar medidas de seguridad efectivas. La impunidad de estos crímenes debe abordarse desde perspectivas legales, éticas y de seguridad. Las organizaciones han enfrentado desafíos para salvar sus bases de datos, lo que las coloca en desventaja y crea oportunidades para los ciberdelincuentes. Al priorizar el cumplimiento de estándares y parámetros legales, podemos brindar apoyo a quienes se encuentran vulnerables ante esta situación (Acosta, Benavides & García,2020).

En cuanto al tratamiento de los datos personales le asiste el derecho a la intimidad de estos, según Trejo (2006), la intimidad abarca las circunstancias, cosas, experiencias, sentimientos y comportamientos que un individuo desea mantener en privado, con la libertad de elegir quién tiene acceso a ellos. Este derecho a la privacidad impone a los demás la obligación de respetarla y sólo puede vulnerarse en casos justificados cuando exista un propósito lícito para su divulgación. Por otro lado, Peña (2007) define el derecho a la privacidad o intimidad como el derecho humano que permite a los individuos, ya sean físicos o morales, excluir o negar a otros el conocimiento de su vida personal. Los individuos también tienen el poder de determinar hasta qué punto pueden compartir



aspectos de su vida personal con otros. Este derecho se divide además en varias dimensiones, entre ellas la inviolabilidad del domicilio, la correspondencia, la protección contra escuchas telefónicas, la propia imagen y la privacidad en el ámbito de las tecnologías de la información o la libertad informática. Existen derechos similares a la vida íntima en otros sistemas jurídicos, conocidos como "privacidad" en el derecho anglosajón, "vie intime" en el derecho francés y "riservatezza" en el derecho italiano.

Según el Comité Jurídico Interamericano de la Organización de los Estados Americanos, los Principios Actualizados sobre Privacidad y Protección de Datos Personales, como instrumento interamericano de derecho indicativo, pretenden servir a los Estados miembros como punto de referencia para fortalecer sus respectivos derechos legales. marcos en la materia, y orientar el desarrollo colectivo de la región hacia una protección armoniosa y efectiva de los datos personales:

1.-Multas Legítimos y Lealtad: El procedimiento de datos personales debe basarse en la aprobación previa, libre, informado e inequívoco del sujeto a la que pertenecen.

2.-Transparencias y Consentimientos: La recopilación de datos personales debe realizarse solamente con propósitos legítimos y por métodos lícitos. Además, la confidencialidad de los datos debe ser respetada, evitando su divulgación, uso o acceso por terceros sin la aprobación explícito del titular, salvo que lo permita la ley.

3.-Relevancia y Necesidad: Solo deben recopilarse aquellos datos personales que sean adecuados, pertinentes y estrictamente necesarios para cumplir con los propósitos de su procesamiento.

4.-Tratamiento y Conservación Limitados: La data personal deben ser procesados y almacenados exclusivamente para fines legítimos y compatibles con los objetivos para los que fueron originalmente recolectados.

5.-Seguridad de los datos: Es fundamental garantizar la privacidad, completitud y disposición de la data personal a través de medidas técnicas, administrativas y organizativas adecuadas. Estas salvaguardas deben prevenir el acceso, uso o procesamiento no autorizado, así como la privación, devastación, deterioro o difusión, incluso en caso de incidentes de naturaleza accidental.

6.-Acceso, Rectificación, Cancelación, Oposición y Portabilidad: Se deben implementar mecanismos rápidos, simples y eficaces que faciliten a los titulares de los datos personales ejercer sus derechos. Esto incluye acceder a sus datos, solicitar correcciones, eliminarlos, oponerse a su tratamiento y, cuando corresponda, trasladar sus datos a otro responsable.

7.-Exactitud de los datos: La data personal tienen que sostenerse correctos, íntegros y vigentes según lo requieran los propósitos de su procesamiento, asegurando que su autenticidad no se vea comprometida.

8. Acceso, Rectificación, Cancelación, Oposición y Portabilidad: Es esencial contar con procedimientos accesibles, dinámicos, sencillos y eficaces que permitan a las personas cuyos datos han sido recopilados ejercer sus derechos. Esto incluye solicitar el ingreso, corrección, supresión, disensión al tratamiento y, cuando aplique, la transferibilidad de sus datos personales. Por regla general, el ejercicio de estos derechos debe ser gratuito. Si es necesario limitar alguno de estos derechos, dichas restricciones

deben estar claramente especificadas en la legislación nacional y alinearse con las normas internacionales aplicables.

9.-Datos Personales Sensibles: Los datos personales sensibles, aquellos cuya mala utilización podrían generar afectaciones significativas, deben ser definidos de manera precisa y protegidos con rigor por las disposiciones legales nacionales correspondientes.

10.-Responsabilidades: Los encargados del manejo de datos personales deben establecer medidas adecuadas de primacía y protección, considerando la sensibilidad de los datos. Esto incluye mostrar el acatamiento de los principios mediante estrategias técnicas y organizativas efectivas, auditorías regulares y colaboración con las autoridades que protegen los datos cuando se requiera.

11.- Considerando la importancia del intercambio de datos personales para el desarrollo económico y social, los Estados integrantes deben colaborar para facilitar el movimiento internacional de datos hacia países que garanticen un nivel pertinente de protección, conforme a estos principios. Asimismo, deben promover la creación de procedimientos que aseguren que las entidades responsables del tratamiento de datos en múltiples jurisdicciones, o que transfieran datos a otros países, puedan salvaguardar su cumplimiento y asumir responsabilidad efectiva por ello.

12.-Excepciones: Una exceptuación a estos principios debe estar claramente especificada en la legislación nacional, ser comunicada al público y limitarse a circunstancias justificadas. Estas pueden incluir motivos relacionados con la soberanía, la seguridad nacional, la seguridad pública, la salvaguarda de la salud pública, la

contienda al crimen, el acatamiento de normativas, otras exenciones de orden público o intereses públicos específicos.

13.- Autoridades de Protección de Datos: Los Estados Miembros deben crear órganos de supervisión autónomos con recursos adecuados, adaptados al sistema constitucional, organizativa y administrativa de cada país. Estos organismos tendrán la tarea de supervisar y fomentar la protección de datos personales en cumplimiento con estos principios. Asimismo, se debe alentar la cooperación entre dichos organismos para garantizar una protección efectiva y coordinada.

### **Variable 1: Hackers**

Es una irregularidad que puede existir sobre todo en el ámbito político y ordenamiento social. Al no existir algunas vivencias sociales y legales de carencia de dispensa, que incluye que en todas las sociedades que se anotan delitos no sancionados y de usuarios impunes que se roban la forma de los sistemas justicieros. De tal forma que la impunidad casi todas las veces es difícil de poder medirlo, pues de la misma manera se logra crear una relación de inputs y outputs del sistema judicial que son reportes que ingresan en el sistema en contra de resoluciones de condenas acertadas que generan los mismos sistemas al calcular muchas faltas o vulneraciones denunciadas, por lo que se puede preestablecer una absoluta tasa de inmunidad para los otros” (Romero, 2018).

Los sistemas de investigación modernos tienden a basarse cada día más en criterios de persecución selectiva (pautas de oportunidad legalmente establecidas), como respuesta a la realidad de la sobrecarga de trabajo de la justicia penal que se ha manifestado durante muchos años y que es una de las causas más directas de

impunidad” (Zambrano, 2023). Así también hace mención que, el deseo de reducir cifras de impunidad, no debería implicar o despojar a los justiciables de sus derechos fundamentales, según las máximas de un Estado Constitucional de derecho (Sabillon, 2018).

Si nos detenemos a revisar la definición de hacker, encontraremos autores como (Hernandez, 2005) quien lo detalla como un individuo que estudia un sistema (informático) para comprenderlo tan profundamente, que pueda ser capaz de modificarlo de distintas formas, en su mayoría creativas. Por su parte, (Trejo, 2006) señala que el hacker resuelve problemas en formas inimaginables comparado con aquellos que se circunscriben en resolverlos pensando en metodologías convencionales.

Incluso (Svintsytskyi, 2022) describe el término hacker, como aquella persona que programa de manera entusiasta y aprende a detalle los sistemas de cómputo. Asimismo, hacker es un sujeto que tiene una mayor habilidad en conocimientos digitales, esto es, explora cada cosa, la estructura operativa, las programaciones, arquitectura de PC, sistemas de medios de comunicación de información, entre otros. Su fin fundamental es investigar y demostrar que se conoce.

Por lo que se preguntan, ¿por qué se vienen ganando la fama de ser individuos que están fuera de la legislación? La solución más simplificada es por la autorización. Es por ello que los hackers al penetrar los diversos sistemas de información sin que sus propietarios puedan tener conocimiento al respecto, y caen en lo ilícito, realizada su fechoría la información obtenida, se emplea para cometer actos criminales. A pesar de ello, no todos los hackers siguen esa línea de acción.

Base Legal: Ley de Delitos Informáticos Ley N° 30096. Esta define **hackers**: “son personas expertas que poseen conocimientos informáticos avanzados para acceder a un determinado sistema o dispositivo y realizar modificaciones desde adentro, principalmente destinadas a la seguridad informática y al desarrollo de técnicas para su mejora” (Pichincha, 2022).

### **Variable 2: Datos personales**

Operación o procedimiento técnico, automatizado o no, que nos puede permitir el registro, la elaboración, organización, almacenamiento, conservación, modificación, extracción, elaboración, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento de datos que facilite el acceso, correlación o interconexión de los datos personales (Roca, 2020).

El acceso es desde el punto de vista de los datos personales, es la acción de llegar a un lugar, asimismo, es un medio de autenticación, muy común en google, siendo desde su masificación, ha podido surgir una gran congestión de servicios que exigen la creación de una cuenta personal para gozar del mismo, con sus respectivos nombres de usuario y clave.

Dado que el mismo usuario se ve obligado a aportar datos personales importantes, como ser su domicilio o su número de tarjeta de crédito, es fundamental que la empresa le brinde la garantía de que nadie más que él podrá visualizarlos, así lo define (Romero, 2018).

### **Jurisprudencia**

Expediente N° 02839-2021-PHD/TC LIMA; Tal como puede aparecer en el petitorio de la demanda el objetivo del presente proceso constitucional va dirigido a que

el Ministerio del Interior pueda disponer la cancelación del Registro 12041435, que se ubica dentro del Sistema SIDPOL-PNP, a cargo de la Dirección de Criminalística de la PNP y se encuentra en el registro de denuncias realizadas en las comisarías, lo cual se considera que viene afectando el derecho a la intimidad personal y a la labor del demandante, puesto que una empresa privada podría tener acceso a dicho registro y transmitiéndolo a poder de terceros. Asimismo, se solicita que se condene al emplazado al pago de costas y costos del proceso (Zambrano, 2023).

### **Legislación**

Ley 30171 Ley que modifica la Ley 30096 Ley de Delitos Informáticos; Ley 29733, Ley de protección de datos personales y su reglamento, aprobado mediante el Decreto Supremo N° 003-2013-JUS.

Código Penal Peruano: El delito informático, art. 186°, inciso 3, párrafo 2; Código Penal Peruano: Decreto Legislativo N° 635: Delitos contra la Administración de Justicia.

### **Definición de términos básicos**

**Acceso:** Conjunto de técnicas usado al buscar, categorizar, modificar y acceder a la información que se encuentra en un sistema: bases de datos, bibliotecas, archivos, Internet.

**Bloqueo:** Indica la identificación y reserva de los mismos, adoptando de esta manera posibles técnicas y organizativa para poder impedir su tratamiento incluyente su visualización.

**Extracción:** Principalmente trata de recuperar varios tipos de datos de una o puede ser de varias fuentes.

**Entidades Financieras:** Empresa cuyo fin administra los fondos de sus inversionistas, estas entidades pueden ser los bancos, las cajas municipales o de ahorro, como también cooperativas.



## **CAPÍTULO II: METODOLOGÍA**

## 2.1. Tipo y diseño de investigación

El tipo de investigación de acuerdo con su enfoque la investigación es: Cuantitativa, porque, aplica la estadística, para cuantificar y decodificar los datos obtenidos, así también lo refiere (Hernandez, 2005): refiere que el enfoque cuantitativo, se fundamenta en un esquema deductivo y lógico, que busca formular preguntas de investigación e hipótesis para posteriormente probarlas.

El presente trabajo de investigación es de diseño no experimental, porque las variables no serán manipuladas, transaccional, porque los datos serán recogidos en un solo momento y descriptivo simple porque, este tipo de diseño permite señalar la manera de cómo se recogerán los datos de la muestra de estudio en un momento determinado,

Así también (Hernandez, 2005), nos refiere, que el diseño no experimental, se divide tomando en cuenta el tiempo durante se recolectan los datos, estos son: diseño transversal, donde se recolectan datos en un solo momento, en un tiempo único, su propósito, es describir variables y su incidencia de interrelación en un momento dado.

## 2.2. Población, muestra y muestreo

El universo poblacional está constituido por los 4,643,550 personas de 18 y más años de edad que tiene alguna cuenta en el sistema financiero (cuenta de ahorro o cuenta sueldo,) en Lima Metropolitana (SBS,2023).

Claro, para ajustar el tamaño de una muestra de 60 a una población finita de 4,643,550, se consideró conveniente usar la siguiente fórmula:

$$n_{finita} = \frac{n}{1 + \frac{n-1}{N_{total}}}$$

Donde:

n = tamaño de la muestra inicial (60 en este caso)

N total= tamaño total de la población (4,643,550 en este caso)

Sustituyendo los valores:

$$n_{\text{finita}} = \frac{60}{1 + \frac{60-1}{4,643,550}}$$

Primero, se calculó la fracción:

$$\frac{60-1}{4,643,550} = \frac{59}{4,643,550} \approx 0.0000127$$

Luego, se suma 1:

$$1 + 0.0000127 \approx 1.0000127$$

Finalmente, se dividió el tamaño de la muestra inicial por este valor:

$$n_{\text{finita}} = \frac{60}{1.0000127} \approx 59.999$$

Dado que el tamaño de la muestra ajustado para una población finita es casi igual al tamaño de la muestra original (60), se puede considerar que el tamaño de muestra ajustado sigue siendo aproximadamente 60 en este caso.

Esto se debe a que, dado el tamaño de la población (4,643,550) es mucho mayor que el tamaño de la muestra (60), el ajuste es mínimo y la diferencia es prácticamente insignificante.

### 2.3. Hipótesis

**General:** La impunidad de los hackers se relaciona significativamente con el tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.

**Específico:** La impunidad de los hackers se relaciona significativamente con el acceso tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.

La impunidad de los hackers se relaciona significativamente con la extracción de tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.

## 2.4. Variables y Operacionalización

**Tabla 1**

*Tabla de variables y sus dimensiones*

Variable	Dimensiones
Variable 1: Hackers	Amenaza
	Impunidad
Variable 2: Tratamiento de datos personales	Extracción
	Acceso

## 2.5. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

Las técnicas que usamos para la recolección de datos en la investigación, es mediante encuesta. Según (Hernandez, 2005) refiere que el método de cuestionario, es el más frecuente para la recolección de datos al consistir en un conjunto de preguntas respecto a una o más variables a medir. Se utilizó también el escalamiento tipo Likert, que sirve para medir las actitudes de los docentes.

El instrumento que se aplicó fue el cuestionario de preguntas, según (León et al., 2022); manifiestan que el cuestionario es el instrumento más utilizado para recabar datos y consta en un grupo de preguntas respecto a una o más variables a medir.

La validez de los datos se realizó mediante 4 juicios de expertos. Según (Hernandez, 2005) la validez de un test indica el grado de exactitud con el que mide el constructo teórico que pretende medir y si se puede utilizar con el fin previsto.

El presente trabajo científico obtuvo como resultado un cuestionario rediseñado y sometido a un análisis de fiabilidad, obteniéndose un Alfa de Cronbach de 0.905, considerando que tiene un excelente nivel de fiabilidad, y está enfocado en medir aspectos como el conocimiento, uso y actitud que los docentes presentan frente a la implementación de la tecnología en el proceso de enseñanza aprendizaje de las clases presenciales; según (León et al., 2022).

## **2.6. Procedimientos**

Se solicitó permiso al Gerente Municipal de Lima Metropolitana nos conceda poder realizar las encuestas en la jurisdicción de su cargo. El procedimiento que utilizaremos, será de ejecución mediante encuestas en la población de Lima Metropolitana, y éstas serán procesadas en el SPSS 26.

## **2.7. Análisis de Datos**

Los datos recogidos de las encuestas se realizaron mediante el software SPSS versión 26, previo volcado de la encuesta a una hoja de cálculo.

## **2.8. Aspecto Ético**

Se sujetó a las reglas de las normas Apa por lo que se respetó a los autores en citas y referencias.

Así mismo se sometió al reglamento de grados y títulos de la universidad Autónoma del Perú, por lo que cumple el porcentaje mínimo de similitud en el software tourniting (20%), se cumplió respetando los Derechos de Autor, citando de esta manera a autores, enlaces de páginas webs, aplicando los valores de honestidad y respeto.

## **CAPÍTULO III: RESULTADOS**

## Descripción de resultados de la técnica: Encuesta

A continuación, se señalará la información obtenida de la técnica de encuesta, teniendo en cuenta los objetivos propuestos en la presente investigación.

Los resultados de la técnica de encuesta vinculados al objetivo general se establecen de la siguiente manera:

### Tabla para los objetivos Generales

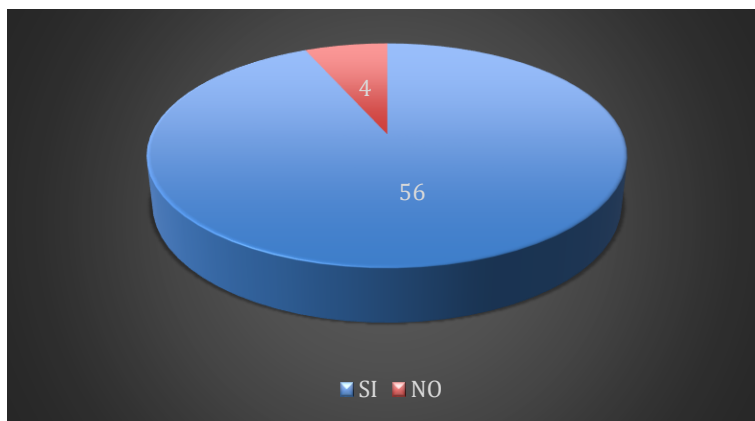
**Tabla 2**

*Descripción de la pregunta 1 de la variable Impunidad de los hackers*

1.- ¿Cree usted que la impunidad de los hackers se relaciona con el tratamiento de datos personales?		
	Frecuencia	Porcentaje
Si	56	93,3
No	4	6,7

**Figura 1**

*Frecuencia de la pregunta 1*



*Nota:* El gráfico representa la figura de los resultados de la primera pregunta de la primera variable

Se puede señalar que en la tabla número 1 de la figura número 1; 56 personas si creen que la impunidad de los hackers se relaciona con el tratamiento de datos personales; mientras que 04 Personas no creen que tenga relación con el tratamiento de datos personales.

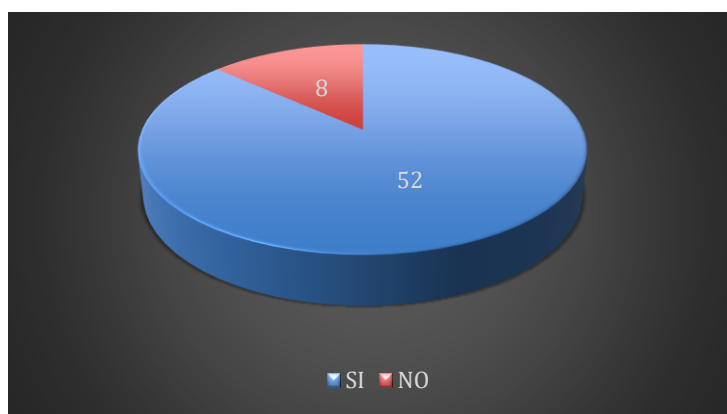
**Tabla 3**

*Descripción de la pregunta 2 de la variable Impunidad de los hackers*

2.- ¿Cree usted que la impunidad de los hackers se relaciona con las entidades financieras?		
	Frecuencia	Porcentaje
Si	52	86,7 %
No	8	13,3 %

**Figura 2**

*Frecuencia de la pregunta 2*



*Nota:* El gráfico representa la figura de los resultados de la segunda pregunta de la primera variable

Se puede señalar que en la tabla número 2 de la figura número 2; 52 personas si creen que la impunidad de los hackers se relaciona con las entidades financieras; mientras que 08 Personas no creen que tenga relación con las entidades financieras.

**Tabla 4**

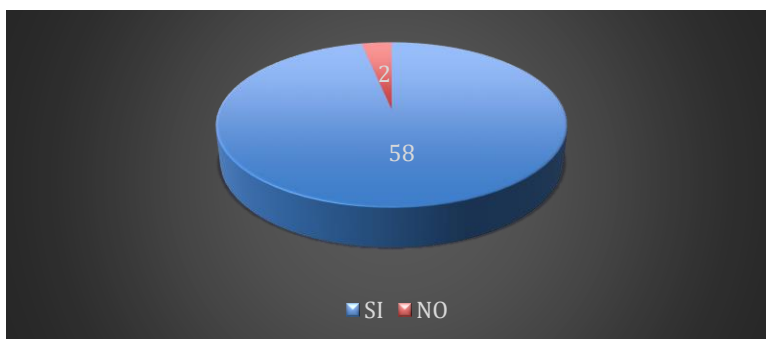
*Descripción de la pregunta 3 de la variable Impunidad de los hackers*

3.- ¿Cree usted que en el tiempo de pandemia que atravesaba el mundo, la impunidad de los hackers se vino incrementando de tal manera que ha perjudicado cada día más a la población?		
	Frecuencia	Porcentaje
Si	58	96,7 %
No	2	3,3 %



## Figura 4

### Frecuencia de la pregunta 3



Nota: El gráfico representa la figura de los resultados de la tercera pregunta de la primera variable

Se puede señalar que en la tabla número 3 de la figura número 3; 58 personas si creen que la impunidad de los hackers se ha incrementado mientras que 02 Personas no creen que se haya incrementado la impunidad de los hackers.

## Tabla 5

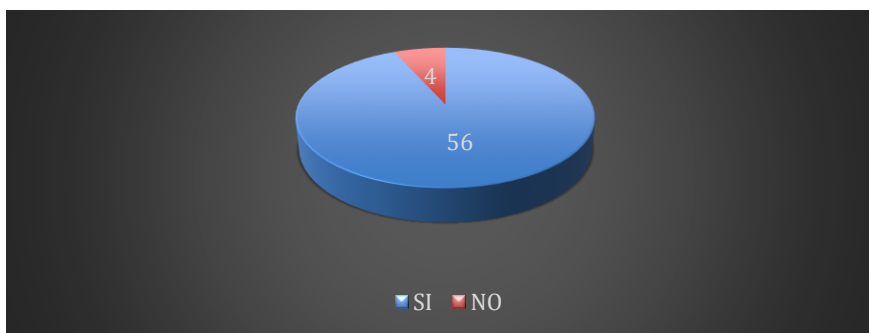
### Descripción de la pregunta 4 de la variable Tratamiento de datos personales

4.- ¿Considera Usted que la impunidad de los hackers se relaciona significativamente con el acceso de tratamiento de datos personales de las entidades financieras?

	Frecuencia	Porcentaje
Si	56	93,3 %
No	4	6,7 %

## Figura 6

### Frecuencia de la pregunta 4



Nota: El gráfico representa la figura de los resultados de la cuarta pregunta de la segunda variable

Se puede señalar que en la tabla número 4 de la figura número 4; 56 personas si creen que la impunidad de los hackers se relaciona significativamente con el acceso de tratamiento de datos personales de las entidades financieras mientras que 04 Personas no creen que se relaciona significativamente con el acceso de tratamiento de datos personales de las entidades financieras.

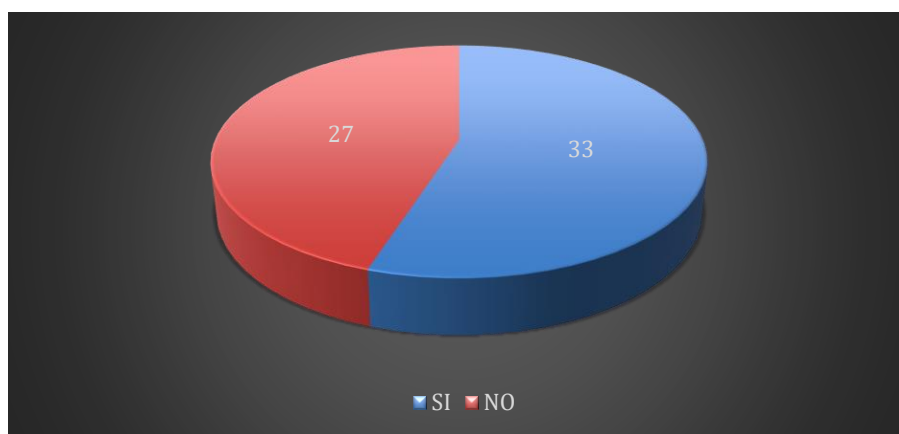
### Tabla 6

*Descripción de la pregunta 5 de la variable Tratamiento de datos personales*

5.- ¿Tiene Usted Conocimientos básicos sobre la relevancia del tratamiento de datos personales y el acceso a los mismos conocimientos que tienen los hackers a las entidades financieras?		
	Frecuencia	Porcentaje
Si	33	55%
No	27	45%

### Figura 5

*Frecuencia de la pregunta 5*



*Nota:* El gráfico representa la figura de los resultados de la quinta pregunta de la segunda variable

Se puede señalar que en la tabla número 5 de la figura número 5; 33 personas si tienen conocimientos básicos sobre la relevancia del tratamiento de datos personales y el acceso a los mismos conocimientos que tienen los hackers a las entidades financieras mientras que 27 Personas no tienen conocimientos básicos sobre la relevancia del

tratamiento de datos personales y el acceso a los mismos conocimientos que tienen los hackers a las entidades financieras.

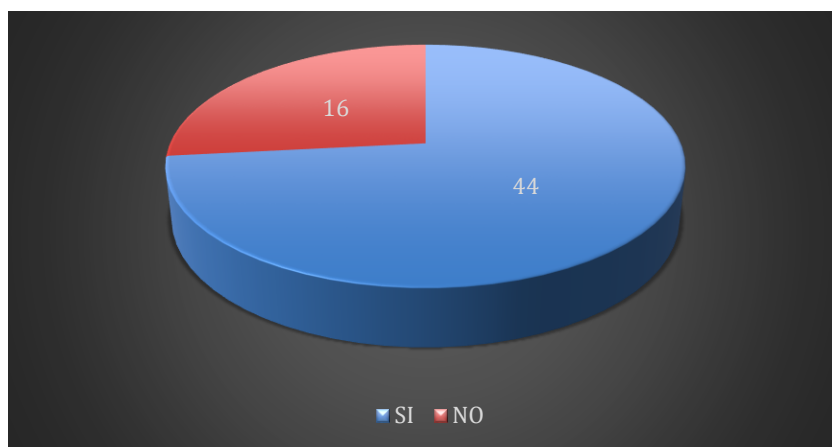
### Tabla 7

*Descripción de la pregunta 6 de la variable Tratamiento de datos personales.*

6.- ¿Considera Usted que los sistemas financieros no invierten en herramientas de seguridad para salvaguardar el acceso a los tratamientos de datos personales de sus clientes?		
	Frecuencia	Porcentaje
Si	44	73,3
No	16	26,7

### Figura 6

*Frecuencia de la pregunta 6*



*Nota:* El gráfico representa la figura de los resultados de la sexta pregunta de la segunda variable

Se puede señalar que en la tabla número 6 de la figura número 6; 44 personas si consideran que los sistemas financieros no invierten en herramientas de seguridad para salvaguardar el acceso a los tratamientos de datos personales de sus clientes mientras que 16 Personas no consideran que los sistemas financieros no invierten en herramientas de seguridad para salvaguardar el acceso a los tratamientos de datos personales de sus clientes.

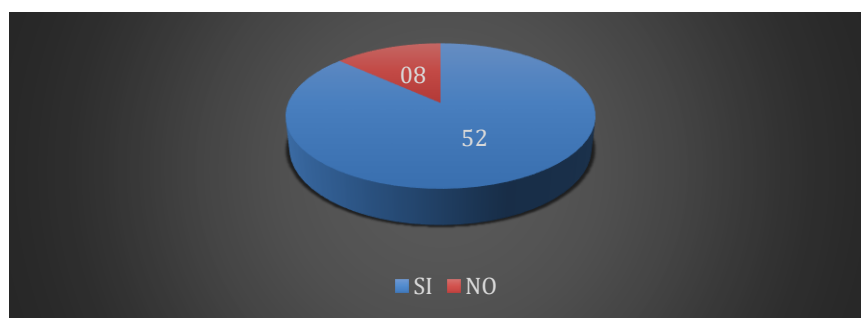
**Tabla 8**

*Descripción de la pregunta 7 de la variable 01*

7.- ¿Cree usted que la impunidad de los hackers se relaciona significativamente con la extracción de tratamiento de datos personales de las entidades financieras?		
	Frecuencia	Porcentaje
Si	52	86,7
No	8	13,3

**Figura 7**

*Frecuencia de la pregunta 7*



*Nota:* El gráfico representa la figura de los resultados de la séptima pregunta de la primera variable

Se puede señalar que en la tabla número 7 de la figura número 7; 52 personas si creen que la impunidad de los hackers se relaciona significativamente con la extracción de tratamiento de datos personales de las entidades financieras mientras que 08 Personas creen lo contrario,

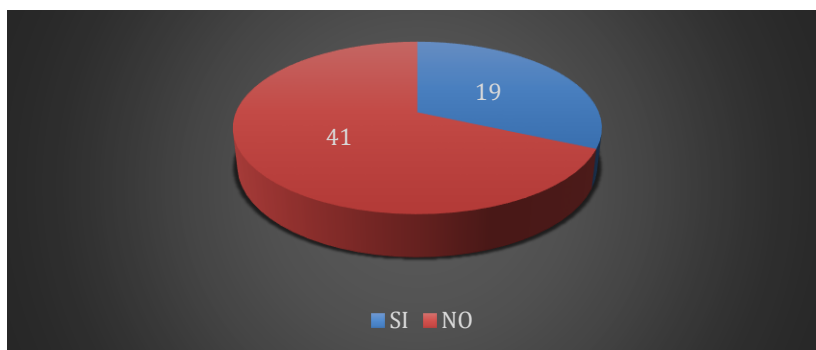
**Tabla 9**

*Descripción de la pregunta 8 de la variable 2*

8.- ¿Tenía conocimiento que algunas entidades financieras en tiempo de pandemia entregaban tarjetas de crédito a sus clientes tan solo con realizar consultas con los datos que figuraban en RENIEC? ¿Usted estaba de acuerdo con el mecanismo de solución de las mismas entidades para seguir adquiriendo clientes en tiempo de pandemia?		
	Frecuencia	Porcentaje
Si	19	68,3 %
No	41	31,7 %

## Figura 8

### Frecuencia de la pregunta 8



*Nota:* El gráfico representa la figura de los resultados de la octava pregunta de la segunda variable

Se puede señalar que en la tabla número 8 de la figura número 8; 19 personas si tenían conocimiento que algunas entidades financieras en tiempo de pandemia entregaban tarjetas de crédito a sus clientes tan solo con realizar consultas con los datos que figuraban en RENIEC y estaban de acuerdo con el mecanismo de solución de las mismas entidades para seguir adquiriendo clientes en tiempo de pandemia mientras que 41 personas no tenían conocimiento que algunas entidades financieras en tiempo de pandemia entregaban tarjetas de crédito a sus clientes tan solo con realizar consultas con los datos que figuraban en RENIEC y no estaban de acuerdo con el mecanismo de solución de las mismas entidades.

## Tabla 10

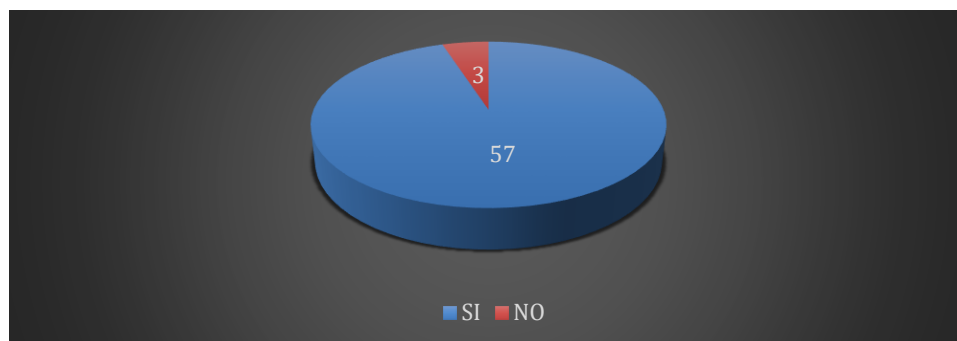
### Descripción de la pregunta 9 de la variable 1

9.- ¿Considera Usted que una gran parte de responsabilidad lo puede tener la SBS por no fiscalizar dichos sucesos y no realizar ninguna modificación para salvaguardar la tranquilidad y seguridad de sus clientes?

	Frecuencia	Porcentaje
Si	57	95%
No	3	5%

## Figura 9

### Frecuencia de la pregunta 9



*Nota:* El gráfico representa la figura de los resultados de la novena pregunta de la segunda variable

Se puede señalar que en la tabla número 9 de la figura número 9; 57 personas si consideran que una gran parte de responsabilidad lo puede tener la SBS por no fiscalizar dichos sucesos y no realizar ninguna modificación para salvaguardar la tranquilidad y seguridad de sus clientes mientras que 03 personas no consideran que una gran parte de responsabilidad lo puede tener la SBS

### Contrastación de Hipótesis:

#### Para la hipótesis general:

#### Tabla 11

*Para el objetivo general: La impunidad de los hackers se relaciona significativamente con el tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.*

<b>Chi cuadrado</b>			
(Bilateral)	Valor	Df	Significación asintótica
Chi cuadrado de Pearson	639.12	2	.000
Razón de verosimilitud			
Asociación lineal por lineal			
N° de caso válidos	60		

**Para la hipótesis específica:**

**Tabla 12**

*Para el objetivo específico 1: La impunidad de los hackers se relaciona significativamente con el acceso tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.*

<b>Chi cuadrado</b>			
(Bilateral)	Valor	Df	Significación asintótica
Chi cuadrado de Pearson	639.12	2	.000
Razón de verosimilitud			
Asociación lineal por lineal			
N° de caso válidos	60		

**Tabla 13**

*Para el objetivo específico 2: La impunidad de los hackers se relaciona significativamente con el acceso tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.*

<b>Chi cuadrado</b>			
(Bilateral)	Valor	Df	Significación asintótica
Chi cuadrado de Pearson	639.12	2	.000
Razón de verosimilitud			
Asociación lineal por lineal			
N° de caso válidos	60		

## **CAPÍTULO IV: DISCUSIÓN**



**Para el Objetivo General:**

Los resultados muestran que La impunidad de los hackers si se relaciona significativamente con el tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.

Este resultado coincide con (Matilde & Valencia, 2022); quien hace referencia que los comportamientos realizados por el sujeto activo en este tipo de delito, comprende diferentes estilos de atentados que van en contra de diferentes bienes jurídicos protegidos conforme sea el caso. Es así, en primer lugar, al patrimonio, esta conducta afecta a la seguridad de una persona, y; otro de los bienes jurídicos que se afectan de manera directa es el resguardo nacional. Al ser actos dirigidos contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes o datos, como los abusos a estos sistemas. A esto, se puede agregar una característica primordial de los abusos informáticos, teniendo en cuenta que estos son una forma cuya conducta es de crimen transnacional, que pudiera ser cometido en cualquier parte del mundo y de la misma forma, afectaría a una persona o grupos de personas, distintos países y lejanos del lugar del cometimiento físico del mismo.

Del mismo modo coincide con (Melo, 2021); tal y como señala en su trabajo de investigación titulada “Sombras de la normatividad que regula el incremento de la ciberdelincuencia” desarrollada en la Universidad Nacional José Faustino Sánchez Carrión de Huacho –Perú. Para la obtención del Título de Abogado, concluye que el ejercicio de nuestra normativa vigente, modifica la ciberdelincuencia en Lima 2015, y infringe en constates controversias, siendo una ventana amplia para su adecuada aplicación y por ende, interfiere de manera significativa en el proceder de como se le

concede la adecuada protección a la ciudadanía, siendo así, que su desfavorable aplicación causa un lamentable impacto a nuestra población. De la misma manera se puede establecer, que si en la práctica se generaran tantos errores judiciales se devendría en ilegal, y por ende se generarían actos inconstitucionales.

Del en base a la jurisprudencia tenemos como referencia a la 05484-2015 quien nos habla de las definiciones de los tratamientos de datos personales y todo lo relacionado sobre el mismo.

### **Para el Objetivo Específico 1:**

Los resultados muestran que La impunidad de los hackers si se relaciona significativamente con el acceso tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.

Este resultado coincide con (Muñoz, 2018); en relación a su investigación: "Los Hackers: Delito Informático frente al Código Penal Peruano", para obtener el título profesional de Abogado, de la Universidad Nacional Santiago Antúnez de Mayolo. Huaraz-Ancash-Perú, menciona que su objetivo general, es dar a conocer la existencia de numerosos vacíos legales en nuestro Código Penal, siendo las más deficientes, las telecomunicaciones de carácter electrónicas comerciales (la existencia de Hackers), para así poder establecer la relevancia de carácter jurídico, de reducir este tipo de aristas, minimizando el impacto perjudicial en la sociedad de modo amplio y de modo específico en los derechos bases, como el de la intimidad, postulando y mejoras para su regulación

Del mismo modo coincide con (Muñoz, 2018), en la tesis de investigación titulada: "Protección Penal de la Intimidad Personal en las Redes Sociales", de la Universidad del Altiplano. Puno-Perú, para obtener el título profesión de Derecho.

Nuestra investigación, se centra fundamentalmente en la era digital, el que advierte, un fenómeno tecnológico de las nuevas eras, y que estos avances tecnológicos, nos hace reflexionar; la falta de protección a la privacidad personal, se manifiesta, por el mal uso de manejo de las redes sociales en el País peruano. Tal es, que nuestra investigación, nos permitirá proponer una propuesta a la presente Ley de Delitos Informáticos, con la finalidad de reformar leyes penales, teniendo un método disuasivo, además podrá establecer acciones eximentes, que tengan supuestos, hacia la lesividad de la propia intimidad, al ser observado, a través de redes sociales.

En base a la jurisprudencia tenemos como referencia a la 2324-2013 quien nos habla de "El titular de los datos personales, tiene el pleno derecho a ser informado, que, sobre él, viene siendo objeto de tratamiento en bancos de datos de la administración pública".

### **Para el objetivo Específico 2:**

Los resultados muestran que La impunidad de los hackers si se relaciona significativamente con la extracción de tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.

Este resultado coincide con La finalidad es de comparar el incremento que la corrupción y la impunidad caen sobre las vulneraciones a derechos humanos. Por el cual, se llevaron a cabo distintos modelos estadísticos. Se visualizó que hay derechos humanos que se involucran mediante actos de corrupción. En la medida en que ni el acto de corrupción ni esa vulneración sean sancionados, la impunidad se transforma en un contexto que motiva al perpetrador a seguir teniendo los mismos actos de corrupción, lo que trae nuevas violaciones a derechos humanos. Cuando la corrupción y la impunidad

se conjugan, ambas se convierten en patrones estructurales de violaciones a los derechos humanos. (Ortiz & Vasquez, 2021)

Del mismo modo coincide con (Peña, 2007) en su investigación sobre: "Los Hackers: Delito Informático frente al Código Penal Peruano", para obtener el título profesional de Abogado, de la Universidad Nacional Santiago Antúnez de Mayolo. Huaraz-Ancash-Perú, hace énfasis que el objetivo general de nuestra investigación, tomada como guía, la existencia de diversos vacíos legales en nuestro Código Penal, siendo específicamente, las telecomunicaciones de tipo electrónicos comerciales (la existencia de Hackers).

En base a la jurisprudencia tenemos como referencia la 05121-2015 que refiere como tema puntual, salvaguardar el derecho a la protección de datos personales de las partes.

## **CAPITULO V: CONCLUSIONES**

**Primera.** – Los resultados muestran que la impunidad de los hackers si se relaciona significativamente con el tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022 en este sentido si se cumplió con precisar que la impunidad de los hackers se relaciona significativamente con el tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.

**Segunda.** Los resultados muestran que la impunidad de los hackers si se relaciona significativamente con el acceso de tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022, en este sentido si se cumplió con demostrar que la impunidad de los hackers se relaciona significativamente con el acceso tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.

**Tercera.** - Los resultados muestran que La impunidad de los hackers si se relaciona significativamente con la extracción de tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022, en este sentido si se cumplió con demostrar que la impunidad de los hackers se relaciona significativamente con la extracción de tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.

## **CAPITULO VI: RECOMENDACIONES**

**Primero.** - Se evidencian brechas legales en la ley N° 30171 que impiden sancionar los delitos informáticos en el Perú el 2015. Pese a los esfuerzos por considerarse que este dispositivo enmendaría los vacíos hallados en la ley 30096, se aprecia que, también existen vacíos en esta ley, como es sabido con los desarrollos tecnológicos continuos, se generan nuevas modalidades conformen evolucionan las tecnologías de información, por lo tanto, la tipicidad de estos nuevos delitos, requiere hacer las respectivas modificaciones a la ley vigente.

**Segundo.** - Asimismo, el Art. 3 de la LDI tipifica el Delito de atentado a la integridad de datos informáticos en las modalidades señaladas en el Convenio de Budapest., donde se sancionan conductas como dañar”, “borrar”, “deteriorar”, “alterar” o “suprimir”; por ende, se deben eliminar las modalidades de “introducir” y “hacer inaccesible” por convertirse en inútiles. Además, dicha ley no hace distinción de lo gravoso del daño ocasionado pese a las recomendaciones en el segundo párrafo del artículo 4 del Convenio de Budapest. Por lo que se recomienda que una adecuada tipificación debe precisar que se configura un acto ilícito siempre y cuando ocasionen un daño grave.

**Tercero.** - La figura del hacker mayormente se vincula al delito informático, como protagonista de infracciones al ámbito íntimo o privado de entidades o sujetos con el propósito de extorsionarlos o de ejecutar un comercio ilegal de datos. Pero, desde otra perspectiva más ética, el hacker, como experto en tecnología, puede devenir en un cooperante de gran importancia para prevenir e investigar estos delitos. Dada esta dualidad de enfoques, es pertinente proponer una regulación adecuada de esta actividad, a fin de regular y proteger su actuación en nuestro ordenamiento jurídico.



**Cuarto.** - Se requiere contar con un ciber comando y una estrategia definida en tópicos de desarrollo e implementación de ciberseguridad. En caso de webs, para que no se pueda filtrar ni sacar información de ellas. Las entidades públicas carecen de buena capacidad en seguridad de aplicaciones web. Debe formarse personal especializado en delitos informáticos en las Fuerzas Policiales, Ministerio Público y Poder Judicial, para enfrentar a los ciberdelincuentes.

**Quinto.** - Las entidades bancarias deben preparar y capacitar a su personal para aminorar el impacto de un ciber ataque dirigido, mediante plataformas capaces de detectar los Malwares de última generación y diseñando un plan de respuesta ante incidentes, para afrontar y minimizar la infección de ramoneares, troyanos y spyware.

**Sexto.** - Tener en cuenta la implementación en varios distritos de más áreas de control o fiscalización especializadas en denunciar este tipo de delitos que tengan por fin, la protección a las personas en casos de haber sido víctima de la vulneración o acceso a su información sin su consentimiento, ocasionándoles un daño económico

## **REFERENCIAS**

- Acosta, M.; Benavides, M. & García, C. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia*, 25(89), 351-368. <https://dialnet.unirioja.es/servlet/articulo?codigo=8890269>
- Álvarez, M. & Montoya, H. (2020). Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos. *Ingeniería y Desarrollo*, 38(2), 279-297. <https://doi.org/10.14482/inde.38.2.006.31>
- Arapa, J.; Cari, K.; Laura, J.; Laura, M.; Merma, R.; Tarapa, H. & Condori, R. (2024). Causas y consecuencias del incremento de los delitos informáticos en la ciudad de Puno 2023. *Revista de Derecho*, 9(1), 1-19. <https://revistas.unap.edu.pe/rd/index.php/rd/article/view/262/568>
- Brito, G. (2023). Cybersecurity in aeronautical maturity: a framework of reference. *Dyna*, 90(227), 24-34. <https://doi.org/10.15446/dyna.v90n227.107420>
- Bustillos, O. & Rojas, J. (2023). Cómo promueven los estados la ciberseguridad de las pymes. *Interfases*, 10(17), 21-37. <https://doi.org/10.26439/interfases2023.n017.6246>
- Cruz, L. (2017). La política brasileña de ciberseguridad como estrategia de liderazgo regional. URVIO. *Revista Latinoamericana de Estudios de Seguridad*, 12(20), 16-30. <https://doi.org/10.17141/urvio.20.2017.2576>
- Dávila, O. (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* [Tesis de pregrado, Universidad Nacional Federico Villa Real]. Repositorio de la Universidad Nacional Federico Villa Real.

<https://repositorio.unfv.edu.pe/bitstream/handle/20.500.13084/2704/CHAVEZ%20RODRIGUEZ%20ELIAS%20GILBERTO%20-%20DOCTORADO.pdf?sequence=1&isAllowed=y>

Duque, M.; Mena, A. & Tuapanta, J. (2017). Alfa de cronbach para validar un cuestionario de uso de tic en docentes universitarios. *Revista Descubre*, 10(12), 37-48.  
<https://core.ac.uk/download/pdf/234578641.pdf>

Espinoza, V. (2022). *Delitos Informáticos y Nuevas Modalidades Delictivas*. (1°ed.). Jurista Editores

Hernandez, L. (2005). El delito informático. *EGUZKILORE*, 23(34), 227- 243.  
<https://www.ehu.es/documents/1736829/2176697/18-Hernandez.indd.pdf>

León, E.; Tesillo, C.; Escobar, Y. & Godoy, L. (2022). Revisión de los avances y cambios en ciberseguridad en el Perú, para una transformación digital. *Innovación y Software*, 3(2), 109-120. <https://www.redalyc.org/articulo.oa?id=673870841009>

Marquez, N. K., & Mousalli, G. M. (2016). Internet, usos y riesgos. Una visión desde la formación de estudiantes, padres y docentes. *Revista Latinoamericana de Investigación en Organizaciones, Ambiente y Sociedad*, 9(12), 177–192.  
<https://doi.org/10.33571/teuken.v9n12a8>

Matilde, Y., & Valencia, L. (2022). Análisis bibliométrico de la producción científica sobre México en temas de ciberseguridad (2015-2020). *CIENCIA ergo-sum, Revista Científica Multidisciplinaria de Prospectiva*, 29(3), 1-14.  
<https://doi.org/10.30878/ces.v29n3a11>

Melo, S. (2021). *El principio de responsabilidad demostrada en el tratamiento de datos personales a través del comercio electrónico en Colombia* [Tesis de posgrado,

Universidad del Rosario, Bogotá]. Repositorio de la Universidad del Rosario, Bogotá. <https://repository.urosario.edu.co/server/api/core/bitstreams/ae888ed2-429c-4a6b-bc2c-d80fd247421e/content>

Muñoz, L. (2018). *Protección penal de la intimidad personal en las redes sociales* [Tesis de pregrado, Universidad Nacional del Altiplano]. Repositorio de la Universidad Nacional del Altiplano. [https://repositorio.unap.edu.pe/bitstream/handle/20.500.14082/9897/Mu%c3%b1oz\\_Quispe\\_Lenin\\_Leonir.pdf?sequence=1&isAllowed=y](https://repositorio.unap.edu.pe/bitstream/handle/20.500.14082/9897/Mu%c3%b1oz_Quispe_Lenin_Leonir.pdf?sequence=1&isAllowed=y)

Olivares, J. (2024). *Transparencia en la gestión pública y su relación contra el crimen organizado en la ciudad de Lima, 2022* [Tesis de pregrado, Universidad Nacional Federico Villareal]. Repositorio de la Universidad Nacional Federico Villareal. [https://repositorio.unfv.edu.pe/bitstream/handle/20.500.13084/9085/UNFV\\_EUP\\_G\\_Soriano\\_Olivares\\_Jonathan\\_Mestria\\_2024.pdf?sequence=1&isAllowed=y](https://repositorio.unfv.edu.pe/bitstream/handle/20.500.13084/9085/UNFV_EUP_G_Soriano_Olivares_Jonathan_Mestria_2024.pdf?sequence=1&isAllowed=y)

Ortiz, H. & Vasquez, D. (2021). Impunidad, corrupción y derechos humanos. *Revista de la Facultad Latinoamérica de Ciencias Sociales*, 29(57), 167-194. <https://dialnet.unirioja.es/servlet/articulo?codigo=7711708>

Peña, F. (2007). Estudio dogmático de los delitos de cohecho y sus perspectivas político criminales. *Revista Diálogo con la Jurisprudencia, Gaceta Jurídica*, 111(13), 189-200. <https://javierjimenezperu.wordpress.com/wp-content/uploads/2011/05/01-alonso-estudio-cohecho-1era-parte.pdf>

Peña, P. (2020). La protección de los datos personales como derecho fundamental: su autonomía y vigencia propia en el ordenamiento jurídico estatal. *Revista De La*

*Facultad de Derecho de México*, 70(278), 915–936. <https://doi.org/10.22201/fder.24488933e.2020.278-2.77065>

Peralta, J. & Limones, J. (2023), *Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación uruguaya desde un Enfoque de Ciberseguridad y delitos Informáticos* [Tesis de posgrado, Universidad Politécnica Salesiana]. Repositorio de la Universidad Politécnica Salesiana. <https://dspace.ups.edu.ec/bitstream/123456789/25184/4/UPS-CT010616.pdf>

Pichincha, B. (2022, 29 de agosto). ¿Qué hacen los hackers y qué tipos existen? Blog de Banco Pichincha. <https://www.pichincha.com/blog/que-es-un-hacker#:~:text=Los%20hackers%20son%20personas%20expertas,de%20t%C3%A9cnicas%20para%20su%20mejora>

Roca, A. (2020). El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado. *Revista de derecho político*, 10(108), 165-194. <https://dialnet.unirioja.es/servlet/articulo?codigo=7527690>

Romero, J. (2018). Conceptualización de una estrategia de ciberseguridad para la seguridad nacional de México. *Revista Internacional de Ciencias Sociales y Humanidades*, 28(2), 3-26. <https://www.redalyc.org/articulo.oa?id=65458498003>

Sabillon, R., (2018). A practical model for conducting comprehensive cybersecurity audits. *UTE Approach*, 9(1), 127-137. <https://doi.org/10.29019/enfoqueute.v9n1.214>

Svintsytskyi, A. (2022). The system of cybersecurity bodies in Ukraine. *General Scientific Magazine José María Córdova*, 20(38), 287-305. <https://doi.org/10.21830/19006586.903>

Trejo, R. (2006). *Viviendo en el Aleph. La sociedad de la información y sus laberintos*. (1° ed.). ESPAÑA: GEDISA.

Zambrano, A. (2023). *Ciberdelitos, y las dificultades que tiene la justicia para prevenir y sancionar estos actos delictivos* [Tesis de pregrado, Universidad Indoamericana].

Repositorio de la Universidad Indoamericana.

<https://repositorio.uti.edu.ec/bitstream/123456789/5512/1/ZAMBRANO%20VER>

[DUGO%20ALEX%20DARIO.pdf](https://repositorio.uti.edu.ec/bitstream/123456789/5512/1/ZAMBRANO%20VER)

## **ANEXOS**



## Anexo 1

Variable	Dimensiones
Variable 1 La impunidad de los hackers	Extracción
Variable 2 Tratamiento de datos personales	Interconexión Bloqueo

### Matriz de Consistencia

**Título:** “La impunidad de los hackers y el tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022”

Problema	Objetivos	Hipótesis
<p><b>General:</b> ¿Cómo la impunidad de los hackers se relaciona con el tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022?</p> <p><b>Específico</b> ¿Cómo la impunidad de los hackers se relaciona con la extracción de tratamiento de datos personales de las entidades</p>	<p><b>General:</b> Determinar, cómo la impunidad de los hackers se relaciona con el tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.</p> <p><b>Específico</b> Determinar, cómo la impunidad de los hackers se relaciona con la extracción de</p>	<p><b>General:</b> La impunidad de los hackers se relaciona directamente con el tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.</p> <p><b>Específico</b> La impunidad de los hackers se relaciona directamente con la extracción de tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.</p>

<p>financieras, Lima Metropolitana, 2022?</p> <p>¿Cómo la impunidad de los hackers se relaciona con el acceso tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022?</p>	<p>tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.</p> <p>Determinar, cómo la impunidad de los hackers se relaciona con el acceso tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.</p>	<p>La impunidad de los hackers se relaciona directamente con el acceso tratamiento de datos personales de las entidades financieras, Lima Metropolitana, 2022.</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------

Anexo 2  
Encuestas

**ENCUESTA**

**\*INSTRUCCIONES.-** La presente encuesta tiene por finalidad conocer e indicar mediante dos opciones sus respectivas respuestas, con la finalidad de poder contribuir con nuestra tesis titulada: **"La Impunidad de los hackers y el tratamiento de los datos personales en Lima metropolitana 2022"**. (Marcar con un X en el recuadro que crea conveniente).

Nombres y Apellidos: Julia Felipa Contreras Molero.....D.N.I. N° 099099061  
Edad: 67.....Distrito: J.C. García Naranjo 1936.....Dpto. 090.....Celvaldo de Lima.....

N°	PREGUNTAS	SI	NO
1	¿Cree usted que la impunidad de los hackers se relaciona con el tratamiento de datos personales?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	¿Cree usted que la impunidad de los hackers se relaciona con las entidades financieras?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	¿Cree usted que en el tiempo de pandemia que atravesaba el mundo, la impunidad de los hackers se vino incrementando de tal manera que ha perjudicado cada día más a la población?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	Considera usted que La impunidad de los hackers se relaciona significativamente con el acceso de tratamiento de datos personales de las entidades financieras?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	¿Tiene Usted conocimientos básicos sobre la relevancia del tratamiento de datos personales y el acceso a los mismos conocimientos que tienen los hackers a las entidades financieras?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6	Considera Usted que los sistemas financieros no invierten en herramientas de seguridad para salvaguardar el acceso a los tratamientos de datos personales de sus clientes ?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7	Considera usted que La impunidad de los hackers se significativamente con la extracción de tratamiento de datos personales de las entidades financieras?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8	Tenia conocimiento que algunas entidades financieras en tiempo de pandemia entregaban tarjetas de créditos a sus clientes tan solo con realizar consultas con los datos que figuraban en RENIEC. ¿Usted estaba de acuerdo con el mecanismo de solución de las mismas entidades para seguir adquiriendo clientes en tiempo de pandemia?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9	Considera Usted que una gran parte de responsabilidad lo puede tener la SBS por no fiscalizar dichos sucesos y no realizar ninguna modificación para salvaguardar la tranquilidad y seguridad de los clientes?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Julia Contreras  
Firma del encuestado




**ENCUESTA**

**\*INSTRUCCIONES.-** La presente encuesta tiene por finalidad conocer e indicar mediante dos opciones sus respectivas respuestas, con la finalidad de poder contribuir con nuestra tesis titulada: **"La impunidad de los hackers y el tratamiento de los datos personales en Lima metropolitana 2022"**. (Marcar con un X en el recuadro que crea conveniente).

Nombres y Apellidos: Andy Frank Pizarro Contreras D.N.I. N° 411423594

Edad: 42 Distrito: Villa María del Triunfo Jr. Unión 829

N°	PREGUNTAS	SI	NO
1	¿Cree usted que la impunidad de los hackers se relaciona con el tratamiento de datos personales?	X	
2	¿Cree usted que la impunidad de los hackers se relaciona con las entidades financieras?		X
3	¿Cree usted que en el tiempo de pandemia que atravesaba el mundo, la impunidad de los hackers se vino incrementando de tal manera que ha perjudicado cada día más a la población?	X	
4	Considera usted que La impunidad de los hackers se relaciona significativamente con el acceso de tratamiento de datos personales de las entidades financieras?	X	
5	¿Tiene Usted conocimientos básicos sobre la relevancia del tratamiento de datos personales y el acceso a los mismos conocimientos que tienen los hackers a las entidades financieras?		X
6	Considera Usted que los sistemas financieros no invierten en herramientas de seguridad para salvaguardar el acceso a los tratamientos de datos personales de sus clientes ?	X	
7	Considera usted que La impunidad de los hackers se significativamente con la extracción de tratamiento de datos personales de las entidades financieras?	X	
8	Tenía conocimiento que algunas entidades financieras en tiempo de pandemia entregaban tarjetas de créditos a sus clientes tan solo con realizar consultas con los datos que figuraban en RENIEC. ¿Usted estaba de acuerdo con el mecanismo de solución de las mismas entidades para seguir adquiriendo clientes en tiempo de pandemia?	X	
9	Considera Usted que una gran parte de responsabilidad lo puede tener la SBS por no fiscalizar dichos sucesos y no realizar ninguna modificación para salvaguardar la tranquilidad y seguridad de los clientes?	X	

  
 Firma del encuestado

**ENCUESTA**

**\*INSTRUCCIONES.-** La presente encuesta tiene por finalidad conocer e indicar mediante dos opciones sus respectivas respuestas, con la finalidad de poder contribuir con nuestra tesis titulada: **"La Impunidad de los hackers y el tratamiento de los datos personales en Lima metropolitana 2022"**. (Marcar con un X en el recuadro que crea conveniente).

Nombres y Apellidos: Cesar Augusto Champac Palacios ..... D.N.I. N° 10631288

Edad: 46 ..... Distrito: Villa el Salvador .....

N°	PREGUNTAS	SI	NO
1	¿Cree usted que la impunidad de los hackers se relaciona con el tratamiento de datos personales?	X	
2	¿Cree usted que la impunidad de los hackers se relaciona con las entidades financieras?	X	
3	¿Cree usted que en el tiempo de pandemia que atravesaba el mundo, la impunidad de los hackers se vino incrementando de tal manera que ha perjudicado cada día más a la población?	X	
4	Considera usted que La impunidad de los hackers se relaciona significativamente con el acceso de tratamiento de datos personales de las entidades financieras?	X	
5	¿Tiene Usted conocimientos básicos sobre la relevancia del tratamiento de datos personales y el acceso a los mismos conocimientos que tienen los hackers a las entidades financieras?		X
6	Considera Usted que los sistemas financieros no invierten en herramientas de seguridad para salvaguardar el acceso a los tratamientos de datos personales de sus clientes ?	X	
7	Considera usted que La impunidad de los hackers se relaciona significativamente con la extracción de tratamiento de datos personales de las entidades financieras?	X	
8	Tenia conocimiento que algunas entidades financieras en tiempo de pandemia entregaban tarjetas de créditos a sus clientes tan sólo con realizar consultas con los datos que figuraban en RENIEC. ¿Usted estaba de acuerdo con el mecanismo de solución de las mismas entidades para seguir adquiriendo clientes en tiempo de pandemia?	X	
9	Considera Usted que una gran parte de responsabilidad lo puede tener la SBS por no fiscalizar dichos sucesos y no realizar ninguna modificación para salvaguardar la tranquilidad y seguridad de los clientes?	X	

Cesar Augusto Champac

Firma del encuestado

**ENCUESTA**

**\*INSTRUCCIONES.-** La presente encuesta tiene por finalidad conocer e indicar mediante dos opciones sus respectivas respuestas, con la finalidad de poder contribuir con nuestra tesis titulada: **"La Impunidad de los hackers y el tratamiento de los datos personales en Lima metropolitana 2022"**. (Marcar con un X en el recuadro que crea conveniente).

Nombres y Apellidos: YANUQUIN ELENA VALENCIA JIMENEZ D.N.I.N° 42949332

Edad: 38 Distrito: VILLA EL SALVADOR

N°	PREGUNTAS	SI	NO
1	¿Cree usted que la impunidad de los hackers se relaciona con el tratamiento de datos personales?	X	
2	¿Cree usted que la impunidad de los hackers se relaciona con las entidades financieras?	X	
3	¿Cree usted que en el tiempo de pandemia que atravesaba el mundo, la impunidad de los hackers se vino incrementando de tal manera que ha perjudicado cada día más a la población?	X	
4	Considera usted que La impunidad de los hackers se relaciona significativamente con el acceso de tratamiento de datos personales de las entidades financieras?	X	
5	¿Tiene Usted conocimientos básicos sobre la relevancia del tratamiento de datos personales y el acceso a los mismos conocimientos que tienen los hackers a las entidades financieras?		X
6	Considera Usted que los sistemas financieros no invierten en herramientas de seguridad para salvaguardar el acceso a los tratamientos de datos personales de sus clientes ?	X	
7	Considera usted que La impunidad de los hackers se significativamente con la extracción de tratamiento de datos personales de las entidades financieras?	X	
8	Tenia conocimiento que algunas entidades financieras en tiempo de pandemia entregaban tarjetas de créditos a sus clientes tan solo con realizar consultas con los datos que figuraban en RENIEC. ¿Usted estaba de acuerdo con el mecanismo de solución de las mismas entidades para seguir adquiriendo clientes en tiempo de pandemia?	X	
9	Considera Usted que una gran parte de responsabilidad lo puede tener la SBS por no fiscalizar dichos sucesos y no realizar ninguna modificación para salvaguardar la tranquilidad y seguridad de los clientes?	X	

  
 Firma del encuestado

### Anexo 3

### Validación de Juicio de Experto 1

**CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE DEPENDENCIA ECONÓMICA**

N°	DIMENSIONES / ítems	Pertinencia <sup>1</sup>		Relevancia <sup>2</sup>		Claridad <sup>3</sup>		Suficiencia <sup>4</sup>		Sugerencias
		Si	No	Si	No	Si	No	Si	No	
<b>DIMENSIÓN 1: Amenaza</b>										
1	¿Cree usted que la impunidad de los hackers se relaciona con el tratamiento de datos personales?	X		X		X		X		
2	¿Cree usted que la impunidad de los hackers se relaciona con las entidades financieras?	X		X		X		X		
3	¿Cree usted que en el tiempo de pandemia que atravesaba el mundo, la impunidad de los hackers se vino incrementando de tal manera que ha perjudicado cada día más a la población?	X		X		X		X		
<b>DIMENSIÓN 2: Acceso</b>										
1	¿Considera usted que La impunidad de los hackers se relaciona significativamente con el acceso de tratamiento de datos personales de las entidades financieras?	X		X		X		X		
2	¿Tiene usted conocimientos básicos sobre la relevancia del tratamiento de datos personales y el acceso a los mismos conocimientos que tienen los hackers a las entidades financieras?	X		X		X		X		
3	¿Considera Usted que los sistemas financieros no invierten en herramientas de seguridad para salvaguardar el acceso a los tratamientos de datos personales de sus clientes ?	X		X		X		X		
<b>DIMENSIÓN 3: Extracción</b>										
1	¿Considera usted que La impunidad de los hackers se relaciona significativamente con la extracción de tratamiento de datos personales de las entidades financieras?	X		X		X		X		
2	Tenía conocimiento que algunas entidades financieras en tiempo de pandemia entregaban tarjetas de créditos a sus clientes tan solo con realizar consultas con los datos que figuraban en RENIEC. ¿Usted estaba de acuerdo con el mecanismo de solución de las mismas entidades para seguir adquiriendo clientes en tiempo de pandemia?	X		X		X		X		
3	¿considera usted que una gran parte de responsabilidad lo puede tener la SBS por no fiscalizar dichos sucesos y no realizar ninguna modificación para salvaguardar la tranquilidad y seguridad de los clientes?	X		X		X		X		

Observaciones (precisar si hay suficiencia<sup>4</sup>): LDS PREGUNTAS SON SUFICIENTES PARA LA INVESTIGACIÓN PROPUESTA.

Opinión de aplicabilidad:  Aplicable [X]     Aplicable después de corregir [ ]     No aplicable [ ]

Apellidos y nombres del juez validador: Dr Mg/ Abog: MARWAN JONAS LOAYZA DRISTA    DNI: 46369520

Especialidad del validador: DERECHO PENAL Y POLÍTICA CRIMINAL

Lima, 20 de 10 del 2023

<sup>1</sup>Pertinencia: El ítem corresponde al concepto teórico formulado.  
<sup>2</sup>Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo.  
<sup>3</sup>Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.  
<sup>4</sup>Suficiencia: Los ítems planteados son suficientes para medir la dimensión.

## Validación de Juicio de Experto 2

### CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE DEPENDENCIA ECONÓMICA

N°	DIMENSIONES / ítems	Pertinencia <sup>1</sup>		Relevancia <sup>2</sup>		Claridad <sup>3</sup>		Suficiencia <sup>4</sup>		Sugerencias
		Si	No	Si	No	Si	No	Si	No	
<b>DIMENSIÓN 1: Amenaza</b>										
1	¿Cree usted que la impunidad de los hackers se relaciona con el tratamiento de datos personales?	X		X		X		X		
2	¿Cree usted que la impunidad de los hackers se relaciona con las entidades financieras?	X		X		X		X		
3	¿Cree usted que en el tiempo de pandemia que atravesaba el mundo, la impunidad de los hackers se vino incrementando de tal manera que ha perjudicado cada día más a la población?	X		X		X		X		
<b>DIMENSIÓN 2: Acceso</b>										
1	¿Considera usted que La impunidad de los hackers se relaciona significativamente con el acceso de tratamiento de datos personales de las entidades financieras?	X		X		X		X		
2	¿Tiene usted conocimientos básicos sobre la relevancia del tratamiento de datos personales y el acceso a los mismos conocimientos que tienen los hackers a las entidades financieras?	X		X		X		X		
3	¿Considera Usted que los sistemas financieros no invierten en herramientas de seguridad para salvaguardar el acceso a los tratamientos de datos personales de sus clientes ?	X		X		X		X		
<b>DIMENSIÓN 3: Responsabilidad</b>										
1	¿Considera usted que La impunidad de los hackers se relaciona significativamente con la extracción de tratamiento de datos personales de las entidades financieras?	X		X		X		X		
2	Tenia conocimiento que algunas entidades financieras en tiempo de pandemia entregaban tarjetas de créditos a sus clientes tan solo con realizar consultas con los datos que figuraban en RENIEC. ¿Usted estaba de acuerdo con el mecanismo de solución de las mismas entidades para seguir adquiriendo clientes en tiempo de pandemia?	X		X		X		X		
3	¿considera usted que una gran parte de responsabilidad lo puede tener la SBS por no fiscalizar dichos sucesos y no realizar ninguna modificación para salvaguardar la tranquilidad y seguridad de los clientes?	X		X		X		X		

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad:  Aplicable [ ]  Aplicable después de corregir [ ]  No aplicable [ ]

Apellidos y nombres del juez validador: Dr. Mg. Abog. Ayber Yeaguirre Cerado, Axel

DNI: 44823980

Especialidad del validador: D: Corporativo

Lima, 20 de 10 del 2023

<sup>1</sup>Pertinencia: El ítem corresponde al concepto teórico formulado.

<sup>2</sup>Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo

<sup>3</sup>Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

<sup>4</sup>Suficiencia: Los ítems planteados son suficientes para medir la dimensión





## Validación de Juicio de Experto 3

### CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE DEPENDENCIA ECONÓMICA

N°	DIMENSIONES / ítems	Pertinencia <sup>1</sup>		Relevancia <sup>2</sup>		Claridad <sup>3</sup>		Suficiencia <sup>4</sup>		Sugerencias
		Si	No	Si	No	Si	No	Si	No	
<b>DIMENSIÓN 1: Amenaza</b>										
1	¿Cree usted que la impunidad de los hackers se relaciona con el tratamiento de datos personales?	X		X		X		X		
2	¿Cree usted que la impunidad de los hackers se relaciona con las entidades financieras?	X								
3	¿Cree usted que en el tiempo de pandemia que atravesaba el mundo, la impunidad de los hackers se vino incrementando de tal manera que ha perjudicado cada día más a la población?									
<b>DIMENSIÓN 2: Acceso</b>										
1	¿Considera usted que La impunidad de los hackers se relaciona significativamente con el acceso de tratamiento de datos personales de las entidades financieras?	X		X		X		X		
2	¿Tiene usted conocimientos básicos sobre la relevancia del tratamiento de datos personales y el acceso a los mismos conocimientos que tienen los hackers a las entidades financieras?	X		X		X				
3	¿Considera Usted que los sistemas financieros no invierten en herramientas de seguridad para salvaguardar el acceso a los tratamientos de datos personales de sus clientes ?	X								
<b>DIMENSIÓN 3: Responsabilidad</b>										
1	¿Considera usted que La impunidad de los hackers se relaciona significativamente con la extracción de tratamiento de datos personales de las entidades financieras?	X		X		X		X		
2	Tenía conocimiento que algunas entidades financieras en tiempo de pandemia entregaban tarjetas de créditos a sus clientes tan solo con realizar consultas con los datos que figuraban en RENIEC. ¿Usted estaba de acuerdo con el mecanismo de solución de las mismas entidades para seguir adquiriendo clientes en tiempo de pandemia?	X		X		X		X		
3	¿considera usted que una gran parte de responsabilidad lo puede tener la SBS por no fiscalizar dichos sucesos y no realizar ninguna modificación para salvaguardar la tranquilidad y seguridad de los clientes?	X		X		X		X		

Observaciones (precisar si hay suficiencia\*): \_\_\_\_\_

Opinión de aplicabilidad:  Aplicable [ ]  Aplicable después de corregir [ ]  No aplicable [ ]

Apellidos y nombres del juez validador: Dr. Mg/ Abog. Augusto Tapo Usamín

DNI: 03626802

Especialidad del validador: CIULLUSA

Lima, 20 de 10 del 2023

- <sup>1</sup>Pertinencia: El ítem corresponde al concepto teórico formulado.  
<sup>2</sup>Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo  
<sup>3</sup>Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo  
<sup>4</sup>Suficiencia: Los ítems planteados son suficientes para medir la dimensión



## Validación de Juicio de Experto 4

### CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE DEPENDENCIA ECONÓMICA

N°	DIMENSIONES / ítems	Pertinencia <sup>1</sup>		Relevancia <sup>2</sup>		Claridad <sup>3</sup>		Suficiencia <sup>4</sup>		Sugerencias
		Si	No	Si	No	Si	No	Si	No	
<b>DIMENSIÓN 1: Amenaza</b>										
1	¿Cree usted que la impunidad de los hackers se relaciona con el tratamiento de datos personales?	X		X		X		X		
2	¿Cree usted que la impunidad de los hackers se relaciona con las entidades financieras?	X		X		X		X		
3	¿Cree usted que en el tiempo de pandemia que atravesaba el mundo, la impunidad de los hackers se vino incrementando de tal manera que ha perjudicado cada día más a la población?	X		X		X		X		
<b>DIMENSIÓN 2: Acceso</b>										
1	¿Considera usted que La impunidad de los hackers se relaciona significativamente con el acceso de tratamiento de datos personales de las entidades financieras?	X		X		X		X		
2	¿Tiene usted conocimientos básicos sobre la relevancia del tratamiento de datos personales y el acceso a los mismos conocimientos que tienen los hackers a las entidades financieras?	X		X		X		X		
3	¿Considera Usted que los sistemas financieros no invierten en herramientas de seguridad para salvaguardar el acceso a los tratamientos de datos personales de sus clientes ?	X		X		X		X		
<b>DIMENSIÓN 3: Caso</b>										
1	¿Considera usted que La impunidad de los hackers se relaciona significativamente con la extracción de tratamiento de datos personales de las entidades financieras?	X		X		X		X		
2	Tenia conocimiento que algunas entidades financieras en tiempo de pandemia entregaban tarjetas de créditos a sus clientes tan solo con realizar consultas con los datos que figuraban en RENIEC. ¿Usted estaba de acuerdo con el mecanismo de solución de las mismas entidades para seguir adquiriendo clientes en tiempo de pandemia?	X		X		X		X		
3	¿considera usted que una gran parte de responsabilidad lo puede tener la SBS por no fiscalizar dichos sucesos y no realizar ninguna modificación para salvaguardar la tranquilidad y seguridad de los clientes?	X		X		X		X		

Observaciones (precisar si hay suficiencia\*): SI HAY SUFICIENCIA

Opinión de aplicabilidad: Aplicable     Aplicable después de corregir [ ]    No aplicable [ ]  
 Apellidos y nombres del juez validador: Dr. Mg/ Abog: WILFREDO GORDILLO BRICENO    DNI: 08337343  
 Especialidad del validador: DERECHO CIVIL

Lima, ... 20 ... de 10 ... del 2020

<sup>1</sup>Pertinencia: El ítem corresponde al concepto teórico formulado.  
<sup>2</sup>Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo  
<sup>3</sup>Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo  
<sup>4</sup>Suficiencia: Los ítems planteados son suficientes para medir la dimensión

