UNIVERSIDAD TECNOLÓGICA DE LOS ANDES

FACULTAD CIENCIAS JURÍDICAS, CONTABLES Y SOCIALES

ESCUELA PROFESIONAL DE DERECHO

Tesis

Implicancias de las nuevas técnicas de ciberdelincuencia en la protección de datos personales en el delito de estafa

Asesor:

Mgt. Herrera Pfuyo, Cornelio

Autora:

Peralta Salas, Yeshira

Para optar al Título Profesional de:

Abogado (a)

Cusco – Cusco - Perú

2025

UNIVERSIDAD TECNOLÓGICA DE LOS ANDES
FACULTAD DE CIENCIAS JURIDICAS CONTABLES Y SOCIALES
ESCUELA PROFESIONAL DE DERECHO

Acta N°: 034-2025

ACTA DE SUSTENTACIÓN DE TÍTULO PROFESIONAL

En la ciudad de Cusco, a los 12 días del mes de agosto del 2025, siendo las 11:15 horas, se reunieron los integrantes del Jurado designado por Resolución Sub Directoral N° 439-2025-UTEA-FCJCS-EPD-FC de la Escuela Profesional de Derecho, Facultad de Ciencias Jurídicas Contables y Sociales:

Presidente	:	Dra. Rodríguez Ayerbe, Kathie
Dictaminante	:	Mgt. Caceres Caceres, Angel
Replicante	:	Mgt. Salas Torres, Walter

Para evaluar la sustentación, en la modalidad de:

☒ Tesis ☐ Trabajo de suficiencia profesional

Titulada:

Implicancias de las nuevas técnicas de ciberdelincuencia en la protección de datos personales en el delito de estafa

Desarrollado por el (los) Bachiller (es):

Br.: Peralta Salas, Yeshira
(Apellidos y Nombres)

Br.: _____
(Apellidos y Nombres)

Para optar el Título Profesional de:

Abogado(a)
(Denominación del Título)

Concluido el acto, el Jurado dictaminó que el (la) (los) mencionado(a) (s) bachiller (es) fue (ron) APROBADO (S):

Por: Unanimidad
(Unanimidad o Mayoría) (*)

Emitiéndose el calificativo final de:

Bachiller (Apellidos y Nombres)	Calificación (**)
Br. Peralta Salas, Yeshira	Aprobado

Siendo las 12:45 horas concluyó la sesión, firmando los integrantes del Jurado.

Presidente: Dra. Rodríguez Ayerbe, Kathie
(Dr. Mg.). (Apellidos y Nombres) (Firma)

Dictaminante: Mgt. Caceres Caceres, Angel
(Dr. Mg.). (Apellidos y Nombres) (Firma)

Replicante: Mgt. Salas Torres, Walter
(Dr. Mg.). (Apellidos y Nombres) (Firma)

(*): **Mayoría:** Dos integrantes del jurado aprueban o desaprueban; **Unanimidad:** Todos los integrantes del Jurado aprueban o desaprueban, Art.18 RGGAT.
(**): 0 a 10: Desaprobado, 11 a 15: Aprobado, 16 a 18: Aprobado Notable, 19 y 20: Aprobado con Distinción, Art. 18 RGGAT.

5% Similitud general

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

Filtrado desde el informe

- Bibliografía
- Texto citado
- Coincidencias menores (menos de 15 palabras)

Fuentes principales

3% Fuentes de Internet
0% Publicaciones
4% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

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

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

Metadatos

Datos del Autor		
Apellidos y nombres	:	Peralta Salas, Yeshira
Tipo de Documento de Identidad	:	DNI
Número de Documento de Identidad	:	60508494
URL ORCID	:	https://orcid.org/0009-0005-2053-3706
Datos del Asesor		
Apellidos y nombres	:	Mgt. Herrera Pfuyo, Cornelio
Tipo de Documento de Identidad	:	DNI
Número de Documento de Identidad	:	23953105
URL ORCID	:	https://orcid.org/0000-0002-9721-8107
Datos de la Investigación		
Facultad	:	Ciencias Jurídicas, Contables y Sociales
Escuela Profesional	:	Derecho
Línea de Investigación	:	Derecho, Privado y Público
Rango de años en que se realizó la investigación	:	Febrero 2025 a agosto 2025
Fuente de financiamiento	:	Autofinanciado
Porcentaje de similitud	:	5%
URL OCDE	:	https://purl.org/pe-repo/ocde/ford#5.05.01

Dedicatoria

Dedico esta tesis a Dios quien con su infinito amor, bendición y acompañamiento me ha dado la fortaleza para enfrentar cada desafío en esta etapa.

A mí querida familia; en especial a mis padres, Alejandro y Antonia a quienes debo mi total gratitud por ser inspiración en mi vida, este logro es para ellos. A mis hermanos por su apoyo inquebrantable, colaboración e inspiración.

A todos mis perrunos rescatados por su amor y acompañamiento incondicional. Pero, sobre todo, a mi Pequeña, mi compañera de 4 patas por su ser mi soporte emocional en mis desvelos de etapa universitaria.

Peralta Salas, Yeshira

Agradecimientos

A la Universidad Tecnológica de los Andes, mi Hatun Yachay Wasi por brindarme los recursos necesarios para realizar el trabajo de investigación. A mis docentes de la filial Cusco quienes compartieron sus amplios conocimientos con el fin de forjar buenos profesionales.

A mi asesor Dr. Cornelio Herrera Pfuyo por su dedicación y guía como docente en la presente investigación.

A mis validadores y entrevistados quienes me orientaron al desarrollo de esta investigación, han sido pilares fundamentales en la dirección de la misma.

A mi familia por su constante apoyo incondicional.

A mis amistades por sus consejos.

Peralta Salas, Yeshira

Resumen

Este estudio tuvo como objetivo analizar las implicancias de las nuevas técnicas de ciberdelincuencia en la protección de datos personales dentro del delito de estafa. Para ello se empleó un enfoque cualitativo con diseño fenomenológico, utilizando entrevistas dirigidas a siete abogados especialistas en derecho penal con experiencia en datos personales y ciberdelincuencia en la ciudad del Cusco, quienes conformaron la totalidad de la población investigada. A partir del análisis de sus respuestas se identificaron técnicas recurrentes como el phishing, el smishing y la suplantación de identidad digital; estas prácticas generan un impacto en la seguridad de los datos personales, aprovechando el desconocimiento tecnológico de las víctimas. Asimismo, se identificó que las principales vulneraciones se relacionan con el uso de contraseñas débiles, el acceso indebido a cuentas y la ausencia de protocolos de seguridad adecuados en las instituciones públicas como privadas. De esta manera se concluyó que el marco legal peruano vigente no se encuentra actualizado para enfrentar tales amenazas, lo que provoca espacios de impunidad y debilita la protección de la información personal; frente a ello resulta urgente impulsar una reforma legislativa acompañada de un fortalecimiento institucional en materia de seguridad digital.

Palabras clave: Ciberdelincuencia, datos personales, estafa, digital, suplantación de identidad.

Abstract

This study aimed to analyze the implications of new cybercrime techniques for the protection of personal data within the crime of fraud. A qualitative approach with a phenomenological design was used, utilizing interviews with seven criminal lawyers with experience in personal data and cybercrime in the city of Cusco, who comprised the entire research population. Based on the analysis of their responses, recurring techniques such as phishing, smishing, and digital identity theft were identified; these practices impact the security of personal data, taking advantage of victims' lack of technological knowledge. Furthermore, it was identified that the main breaches are related to the use of weak passwords, unauthorized access to accounts, and the lack of adequate security protocols in both public and private institutions. It was concluded that the current Peruvian legal framework is not up to date to address such threats, which creates spaces for impunity and weakens the protection of personal information. In light of this, it is urgent to promote legislative reform accompanied by institutional strengthening in the area of digital security.

Keywords: Cybercrime, personal data, fraud, digital, identity theft.

Índice

Índice de tablas

Índice de anexos

I. Introducción

El cuanto al primer capítulo se presentó el planteamiento del problema a partir de la identificación de nuevas técnicas de ciberdelincuencia que afectaron directamente la protección de datos personales en delitos de estafa para lo cual se describió el contexto real, se formularon la pregunta general así como las preguntas específicas que orientaron la investigación, se establecieron los objetivos generales - específicos, se argumentó la importancia del estudio desde la perspectiva jurídica, social, ética y científica.

En el segundo capítulo se desarrolló el marco teórico incorporando antecedentes nacionales e internacionales, se expusieron las principales bases conceptuales vinculadas a los delitos informáticos, la ciberdelincuencia y la protección de datos personales así como se definieron los términos esenciales que fueron empleados durante toda la investigación para asegurar una interpretación precisa.

El tercer capítulo estuvo dedicado a la metodología donde se indicó que la investigación tuvo un enfoque cualitativo, con diseño fenomenológico, que permitió comprender la experiencia desde la perspectiva de los abogados entrevistados también se describió el ámbito temporal - espacial de la investigación, así como la población; el instrumento de recolección de datos, el procedimiento que se siguió para el

desarrollo del trabajo de campo, la técnica de análisis de datos utilizada y las consideraciones éticas que fueron respetadas a lo largo de todo el proceso.

En el cuarto capítulo se presentaron los resultados obtenidos a partir de las entrevistas aplicadas a los abogados, organizados en función de los objetivos específicos planteados con ayuda de matrices de categorización, se redactaron los resultados en forma de interpretación narrativa culminando con la discusión de los hallazgos mediante un proceso de triangulación que integró lo dicho por los participantes, el análisis del investigador tanto la comparación con los antecedentes revisados.

En el quinto capítulo se expusieron las conclusiones alcanzadas también se formularon recomendaciones dirigidas a las instituciones correspondientes, tanto del sector público como privado, incluyendo también las referencias bibliográficas utilizadas, los anexos que contuvieron los instrumentos y documentos de soporte empleados durante la investigación.

II. Problema del problema

2.1. Descripción y formulación del problema

A nivel internacional, la protección de datos personales frente a la ciberdelincuencia ha emergido como un desafío multifacético, globalmente reconocido puesto que la digitalización acelerada de la sociedad ha ampliado las fronteras de la información, pero también ha generado nuevas vulnerabilidades en materia de privacidad y seguridad de datos; en este sentido, la Comisión Europea enfatiza que "la protección de datos es un derecho fundamental en la Unión Europea" (Consejo de la Union Europea, 2024), subrayando la necesidad de normativas completas para salvaguardar la privacidad de los ciudadanos.

A nivel nacional, la realidad problemática de la protección de datos personales frente a la ciberdelincuencia en Perú revela una serie de desafíos significativos que impactan la seguridad y privacidad de los ciudadanos. A pesar de contar con una ley de protección de datos personales desde 2011, la Ley N° 29733 (2011), la efectividad en su aplicación y cumplimiento continúa siendo cuestionada; tal es que esta situación se ve reflejada en informes y análisis realizados por entidades gubernamentales y organismos de control, como lo es, el Organismo Supervisor de la Inversión Privada en Telecomunicaciones (2022) en adelante conocido con las siglas OSIPTEL que ha identificado brechas en la adecuada protección de datos personales en el país, evidenciando deficiencias en la implementación de medidas de seguridad así como el

manejo adecuado de la información por parte de las empresas. Así mismo, Herrera (2020) destacada la necesidad de mejorar la protección de datos personales en el ámbito nacional e infiere que la mayoría de las empresas peruanas no cuentan con mecanismos adecuados para proteger la información personal de sus clientes, lo que pone en riesgo la privacidad y confidencialidad de los datos.

A nivel local, en la ciudad de Cusco, la realidad problemática se manifiesta de manera particular debido a factores socioeconómicos, tecnológicos y culturales específicos de la región. A pesar de que Cusco es una ciudad reconocida internacionalmente por su patrimonio histórico y cultural, su infraestructura digital y sus capacidades técnicas pueden ser limitadas en comparación con otras áreas urbanas más desarrollada es por ello que se ve reflejada en la falta de recursos y capacitación especializada en materia de seguridad cibernética en las instituciones de gobierno o las empresas locales, evidenciado con el último reporte en ciberdelincuencia realizado por el MINJUS (2022), entre los años 2019 y 2021 se registraron un total de 711 denuncias por delitos informáticos en Cusco, considerando que esta cifra es parte de un total nacional de 14,671 denuncias en el mismo período, la realidad problemática en Cusco respecto a la ciberdelincuencia se presenta como una preocupación significativa en el contexto peruano.

Es así que en los últimos años, el uso de tecnologías digitales y servicios en línea ha crecido rápidamente ello ha llevado a que muchas instituciones, tanto públicas como privadas, recopilen y almacenen grandes cantidades de datos personales, en cuanto a la información recopilada incluye nombres, direcciones, números de teléfono y detalles financieros, que son esenciales para la operación diaria de estas instituciones y para la comodidad de los ciudadanos, esta dependencia creciente de los datos

personales no ha sido acompañada por una implementación adecuada de medidas de seguridad para proteger esta información sensible.

Al principio, la falta de protección de los datos personales no era un problema ampliamente reconocido es por ello que las instituciones no priorizaban la seguridad de la información y los ciudadanos no eran completamente conscientes de los riesgos asociados pero con el tiempo, comenzaron a surgir incidentes aislados de violaciones de datos, donde la información personal fue accedida y utilizada sin autorización, aunque inicialmente esporádicos, pusieron en evidencia las vulnerabilidades en la protección de datos.

A medida que estas brechas de seguridad se hicieron más evidentes, los delincuentes encontraron una oportunidad para explotar la situación es así que los estafadores comenzaron a utilizar datos personales obtenidos de manera ilícita para cometer fraudes, desarrollando métodos cada vez más sofisticados para engañar a las víctimas. Los tipos de estafa variaron desde engaños telefónicos hasta fraudes en línea, cada uno adaptado para aprovechar las debilidades en la protección de datos, pues este aumento en la actividad delictiva generó una creciente preocupación entre los ciudadanos, quienes se sentían cada vez más inseguros sobre la protección de su información personal.

La problemática central radica en la capacidad limitada de las instituciones públicas y privadas para proteger adecuadamente los datos personales frente a estas nuevas amenazas digitales, a pesar de la existencia de normativas específicas diseñadas para regular el manejo y la protección de la información personal, como la Ley N°29733 en Perú, la implementación efectiva de estas normativas sigue siendo insuficiente.

Las estafas cibernéticas, que incluyen desde el phishing y el pharming hasta el uso de malware y ransomware, han evolucionado en complejidad y alcance; cuyas prácticas fraudulentas no solo generan pérdidas económicas significativas, sino que también socavan la confianza de los ciudadanos en las transacciones electrónicas y en las instituciones que gestionan sus datos.

El impacto social de esta problemática es considerable ya que las víctimas de estafa, a menudo, experimentan un perjuicio económico directo y una pérdida de confianza en el sistema financiero y en las tecnologías digitales, esta desconfianza puede llevar a una menor adopción de tecnologías digitales en la región, afectando negativamente el desarrollo económico local y limitando las oportunidades de crecimiento para las empresas a ello el fracaso en proteger adecuadamente los datos personales puede resultar en la erosión de la confianza en las instituciones, lo que a su vez dificulta la gobernabilidad y la implementación efectiva de políticas públicas.

Desde un punto de vista jurídico, la falta de una aplicación efectiva y uniforme de la Ley N°29733 destaca la necesidad urgente de fortalecer el marco regulador y los mecanismos de cumplimiento por lo que incluye no solo la mejora en la capacitación y sensibilización sobre la importancia de la protección de datos, sino también el desarrollo de infraestructuras tecnológicas más eficientes y actualizadas que puedan resistir los ataques cibernéticos.

2.1.1. Interrogante general

- ¿Cuáles son las implicancias de las nuevas técnicas de ciberdelincuencia en la protección de datos personales en el delito de estafa?

2.1.2. Interrogantes específicos

- ¿De qué manera las principales técnicas de ciberdelincuencia afectan la manipulación de datos personales de las víctimas en el delito de estafa?
- ¿Qué riesgos representan las vulneraciones directas de la protección de datos personales ante las tácticas empleadas en ciberdelincuencia en el delito de estafa?

2.2. Objetivos

2.2.1. Objetivo general

- Analizar las implicancias de las nuevas técnicas de ciberdelincuencia en la protección de datos personales en el delito de estafa.

2.2.2. Objetivo específicos

- Identificar las principales técnicas de ciberdelincuencia y su impacto en la seguridad de datos personales de las víctimas en el delito de estafa.
- Describir las vulneraciones directas de la protección de datos personales ante las tácticas empleadas en ciberdelincuencia en el delito de estafa.

2.3. Justificación e importancia

2.3.1. Justificación metodológica

La investigación se sustenta en un enfoque cualitativo, ya que busca analizar en profundidad los fenómenos relacionados con la protección de datos personales frente a las nuevas técnicas de ciberdelincuencia en delitos de estafa en Cusco, en merito a ello este enfoque permite comprender no solo los aspectos legales, sino también los impactos sociales y contextuales de este problema.

"Una justificación en una investigación, es la sección donde se explica por qué es relevante y necesaria la realización de un estudio" (Ñaupas, 2018, p. 63).

2.3.2. Justificación normativa

La protección de datos personales es un derecho fundamental que se encuentra consagrado en diversas normativas a nivel nacional e internacional puesto que en el contexto peruano, la Ley N°29733 (2011) regula la gestión de datos personales, estableciendo obligaciones claras para las entidades que manejan dicha información, este estudio se justifica jurídicamente en la necesidad de evaluar la eficacia de estas normativas y su aplicación práctica en Cusco, un área donde los delitos de estafa han mostrado un aumento significativo.

"La justificación normativa se refiere a la explicación sobre la necesidad de realizar un estudio en función de las disposiciones legales, reglamentos y políticas públicas existentes que regulan el tema objeto de investigación" (Gallardo, 2021, p. 59)

2.3.3. Justificación practica

En cuanto al punto de vista social, la sociedad cusqueña ha sido impactada de manera creciente por los delitos de estafa, los cuales no solo generan pérdidas económicas, sino también una profunda desconfianza en las instituciones y sistemas que gestionan los datos personales es así que la presente investigación tiene un valor social significativo, ya que busca abordar una problemática que afecta directamente la vida cotidiana de los ciudadanos y al identificar así como analizar los factores que influyen en la protección de datos personales, esta investigación puede contribuir a la formulación de políticas más efectivas y a la implementación de medidas de seguridad más eficaces, generando un entorno más seguro y confiable para la comunidad.

Hernandez et al. (2023) menciona que la justificación práctica responde a la necesidad de resolver problemas específicos o generar soluciones aplicables a la realidad concreta.

2.3.4. Justificación ética

Desde una perspectiva ética, la protección de datos personales está íntimamente ligada a la dignidad y privacidad de los individuos, la investigación se enmarca en una valoración axiológica que reconoce la importancia de proteger la información personal como un derecho inherente en cuanto al punto epistemológico, este estudio busca generar conocimientos que respeten y promuevan estos valores fundamentales y estará ligado a la responsabilidad ética de contribuir a una sociedad donde la privacidad y la seguridad de los datos sean garantizadas, previniendo así el abuso y la explotación de información personal.

Bernal (2016) indica que este tipo de justificación argumenta que la investigación es necesaria para garantizar derechos fundamentales, promover el bienestar colectivo o prevenir daños.

2.3.5. Justificación teórica

Desde un enfoque científico, este estudio permite una comprensión más profunda de las dinámicas y factores que influyen en la eficacia de las normativas vigentes y en las prácticas de las instituciones que gestionan datos personales ya que los hallazgos de esta investigación no solo enriquecerán el conocimiento existente, sino que también proporcionarán una base sólida para futuras investigaciones.

"Destaca cómo la investigación contribuye a ampliar, profundizar o revisar el marco conceptual existente" (Gallardo, 2021)

2.4. Categorías

2.4.1. Ciberdelincuencia

Sub categorías:

- Manipulación de datos
- Vulneraciones directas

2.4.2. Datos personales

Sub categorías:

- Implementación
- Mecanismos legales y sanciones

III. Marco teórico

3.1. Antecedentes

En el presente capitulo desarrollaremos a los antecedentes jurídicos relevantes para esta investigación por lo que iniciaremos con los antecedentes internacionales y se finalizaría con los antecedentes nacionales.

3.1.1. Antecedentes internacionales

Se tiene la investigación de Fuentes (2022) titulado “El derecho fundamental a la protección de datos personales en Argentina y en el mundo: Los conflictos extraterritoriales por los delitos informáticos” realizado para la obtención de título profesional de abogado, en la Universidad de San Andrés cuyo objetivo general fue examinar cómo Estados Unidos, la Unión Europea y Argentina han respondido a los conflictos de jurisdicción que surgen en el contexto de estos delitos. La metodología utilizada fue cualitativa que consistió en un análisis detallado de normativas internas, tratados internacionales, jurisprudencia y doctrina relevante. Como conclusión principal, se propuso una mayor integración y colaboración internacional como solución a los problemas jurisdiccionales, subrayando la importancia de proteger las garantías individuales a través de la jurisdicción territorial y la eliminación de trabas burocráticas para agilizar la cooperación internacional.

Este antecedente es relevante para la tesis, ya que ilustra la necesidad de una cooperación global más efectiva y de marcos regulatorios que se adapten a las realidades de la ciberdelincuencia.

Asimismo se tiene la tesis por Benavides (2022) titulada “Situación actual de la protección de datos personales” abordada para el grado de abogado en la Universidad Militar Nueva Granada Bogotá, cuyo objetivo general de esta investigación fue demostrar que, a pesar de los avances tecnológicos, el entorno de Internet sigue siendo inseguro para las actividades en línea. La metodología es cualitativa e incluyó un análisis de casos y la revisión de literatura que identifica las amenazas inherentes a la transferencia de datos en la web. La conclusión principal sostiene que, aunque Internet ofrece numerosos beneficios para la vida cotidiana, nuestras actividades en línea conllevan riesgos sustanciales y que ninguna página web o red social puede garantizar la seguridad completa de los datos personales, y que incluso las grandes empresas enfrentan dificultades para proteger y procesar adecuadamente la información.

Este antecedente es altamente relevante para la tesis, ya que refuerza la necesidad de una protección más gigantesca de los datos personales frente a las crecientes amenazas de ciberdelincuencia, destacando la vulnerabilidad intrínseca del entorno digital.

Por otro lado, se presenta la investigación realizada por Bujosa y Del Pozo (2022), titulado “Diligencias de investigación tecnológicas para la lucha contra la ciberdelincuencia” para obtención de grado de Doctor en la Universidad de Salamanca, el cual tuvo como objetivo general, analizar informes de entidades públicas y privadas sobre delincuencia grave, revisar noticias actuales, y consultar normativas nacionales

e internacionales relacionadas con los ciberdelitos. La metodología empleada fue cualitativa, examinando la bibliografía especializada y la jurisprudencia de altos tribunales, participando en eventos nacionales e internacionales para fortalecer el conocimiento en el ámbito procesal y de la ciberdelincuencia. La conclusión principal subrayó la necesidad urgente de regular exhaustivamente las diligencias de investigación tecnológicas, como el registro remoto, y de desarrollar herramientas de cooperación internacional para garantizar la ciberseguridad.

Este antecedente destaca la importancia de contar con un marco legal adaptado a las nuevas realidades tecnológicas, algo esencial para abordar la protección de datos personales frente a las técnicas de ciberdelincuencia.

Asimismo, se tiene la revista abordado por Castillo (2020) titulada "Ciberseguridad y vigilancia tecnológica: un reto para la protección de datos personales en los archivos" en la Universidad Autónoma de San Luis Potosí, cuyo objetivo general fue analizar el impacto de las políticas públicas internacionales, como la Agenda 2030 y las normas ISO, junto con la legislación nacional, como el Plan Nacional de Desarrollo y la Ley General de Protección de Datos Personales. La metodología empleada fue cualitativa y se basó en un análisis de fuentes documentales, con un enfoque en el papel cada vez más relevante de los archivistas en la preservación de la información y la cultura en un entorno digital en constante evolución. La investigación tuvo como conclusión principal que, los archivistas juegan un rol crucial en la sistematización, digitalización y preservación de la información, y que la protección de datos personales, aunque ha sido una prioridad en las agendas internacionales desde 1948, sigue siendo un área que requiere mayor regulación en el contexto de la ciberseguridad y la vigilancia tecnológica. Además, se identificó un

vacío legal significativo en materia de robo de identidad, destacando que México ocupa el octavo lugar mundial en denuncias por este delito.

Este antecedente es importante ya que destaca la necesidad de desarrollar marcos legales específicos en referencia a la protección de datos personales en un entorno digital.

Finalmente, como ultimo antecedente internacional se tiene el estudio de Aguilar et al. (2022) artículo titulado “La protección de datos personales en Ecuador” realizado en la Universidad Regional Autónoma de los Andes en Ecuador, tuvo como objetivo general analizar la protección de datos personales en el país, especialmente en el contexto de los delitos informáticos. La metodología utilizada fue cualitativa e incluyó un análisis exhaustivo de literatura que abarcó tanto fuentes primarias como secundarias, tales como artículos científicos y normativas legales nacionales e internacionales. La conclusión principal fue que, a pesar de la existencia de una ley específica, la protección de datos en Ecuador sigue siendo insuficiente, requiriéndose no solo mejoras jurídicas sino también un cambio cultural y una mayor inversión en infraestructura tecnológica.

Este antecedente es relevante para la tesis, ya que describe la necesidad de fortalecer tanto el marco legal como la conciencia social en la protección de datos, aspectos que son cruciales para abordar la ciberdelincuencia en Cusco.

3.1.2. Antecedentes nacionales

Ahora bien, como primer antecedente nacional se menciona a Villar (2024) tesis titulada “Tráfico ilegal de datos: necesidad de reforma del Código Penal peruano” para optar el título de Abogado en la Universidad Continental, cuyo objetivo general fue analizar cómo la adquisición, comercialización, intercambio o uso indebido de

datos personales constituye una grave infracción a la privacidad y la seguridad de los individuos. De metodología tipo cualitativa ya que a través de la revisión de la Ley N°27309-2000 y su posterior inclusión en la Ley N°30096 (2013), se identificó la necesidad de actualizar la legislación penal para hacer frente a las nuevas modalidades delictivas, como el phishing y el acceso no autorizado a sistemas informáticos. La conclusión principal destaca que, aunque la legislación existente reconoce el delito de tráfico ilegal de datos, persisten deficiencias en su tipificación y penalización, lo que pone en evidencia la urgencia de reformas legales que aborden de manera más amplia, los desafíos de la ciberdelincuencia en un entorno digital cada vez más interconectado.

Este trabajo proporciona un contexto valioso que permite comprender cómo las lagunas en la legislación actual pueden ser explotadas por los ciberdelincuentes, lo que refuerza la importancia de proponer mejoras en la normativa para garantizar una protección más eficaz de los datos personales en la región.

Ahora bien, se tiene el estudio de Álvarez y Llerena (2021) tesis titulada "Alcances jurídicos de la legislación nacional e internacional sobre protección de datos personales en la implementación de la tecnología 5G" para la obtención de grado de abogado en la Universidad Católica San Pablo que tuvo como objetivo general analizar los alcances jurídicos en la normativa relacionada con la protección de datos personales al implementar la Tecnología 5G en Perú en 2021. Se utilizó una metodología con enfoque cualitativo, con un diseño descriptivo fenomenológico de tipo hermenéutico, con un enfoque socio-jurídico. Cuya conclusión principal es que, las normas vigentes en Perú no brindan una protección suficiente para los datos personales de los usuarios de esta tecnología, lo que resalta la necesidad de revisar y fortalecer la legislación en este ámbito para garantizar una adecuada protección de la privacidad de los individuos en el contexto de la Tecnología 5G.

La experiencia de los usuarios y especialistas en el contexto de la Tecnología 5G en Arequipa proporciona un marco comparativo útil para analizar la situación en Cusco, permitiendo identificar posibles deficiencias en la protección de datos que podrían ser aprovechadas por delincuentes cibernéticos en delitos de estafa.

En esa misma línea resaltaremos a la autora Ventura (2020) tesis titulada "La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima" para obtener el título de Abogado de la Universidad Privada del Norte tuvo como objetivo general analizar la regulación legislativa frente a las modalidades como el phishing, smishing y vishing que son tipo de ciberdelincuencia en nuestro sistema penal peruano, lo que permitió que durante muchos años se cometieran fraudes cibernéticos sin una respuesta legal adecuada. La metodología de la investigación fue exploratoria y básica, con un enfoque cualitativo. Como conclusión principal que las modalidades del phishing, smishing y vishing aún no están reguladas en la legislación peruana, a pesar de ser formas comunes de fraude en la era digital. Además, se señaló la necesidad de mejorar la infraestructura y logística del sistema de administración de justicia para procesar los delitos informáticos de manera más efectiva.

Este antecedente es particularmente relevante para la tesis, ya que subraya las deficiencias en la regulación legal frente a las nuevas modalidades de ciberdelincuencia, lo que resalta la necesidad de reformas legislativas y de mejoras en la capacidad operativa del sistema judicial en Perú.

Finalmente el trabajo abordado por Aredo (2021) tesis titulada "El phishing y su vulneración a la protección de datos personales en los delitos informáticos" para la obtención de grado Abogado en la Universidad Cesar Vallejo, que tuvo como objetivo

general analizar si el phishing compromete la seguridad de la información en los crímenes informáticos, explorando específicamente los efectos del phishing en la obtención de datos personales, subrayando la importancia de proteger estos datos como una salvaguardia esencial del derecho a la privacidad. También se evaluaron los criterios de los delitos informáticos según el Código Penal de Perú. La metodología de este estudio fue cualitativa, centrándose en el análisis de documentos sin aplicaciones prácticas, lo que permitió un enfoque profundo en la revisión de la normativa y literatura existente. Cuya conclusión principal subrayaron la necesidad de ajustar la normativa vigente y llevar a cabo campañas de concienciación para prevenir la ingeniería social, dado que el phishing se aprovecha principalmente de la falta de educación informática entre los usuarios. Asimismo, se sugirió la implementación de mecanismos de autenticación más robustos para proteger los datos personales, y se señaló que las definiciones genéricas en la legislación sobre delitos informáticos dificultan una delimitación precisa del phishing.

Este antecedente es relevante para la tesis, ya que proporciona un análisis crítico de cómo las lagunas en la educación informática y la normativa legal actual permiten que el phishing continúe siendo una amenaza significativa para la seguridad de los datos personales.

3.2. Bases teóricas

3.2.1. Ciberdelincuencia

García y Pilco (2024) definen la ciberdelincuencia como el conjunto de prácticas ilegales que utilizan herramientas digitales para vulnerar la confianza y la seguridad de las personas, generando pérdidas económicas y afectaciones a la privacidad.

3.2.1.1.Antecedentes histórico conceptuales

La ciberdelincuencia como menciona la Naciones Unidas (2022) comenzó a tomar forma en los años 1960, cuando los primeros sistemas informáticos se implementaron de manera masiva en instituciones públicas y privadas, durante esta etapa inicial, los delitos consistían principalmente en accesos no autorizados a sistemas informáticos, comúnmente conocidos como hacking cuyos actos, inicialmente percibidos como intentos de exploración tecnológica, se transformaron en actividades con fines de lucro o daño intencionado, marcando el inicio de un fenómeno más complejo.

Con la llegada de internet en los años 90 y las redes globales facilitaron el acceso a grandes cantidades de datos y ampliaron las posibilidades para cometer fraudes electrónicos, extorsiones y suplantaciones de identidad.

A medida que las tecnologías avanzaron, también lo hicieron las técnicas utilizadas por los ciberdelincuentes, dando lugar a prácticas como el phishing, el ransomware y el smishing.

El desarrollo de estas técnicas no solo desafió las capacidades de las autoridades para responder, sino que también evidenció la necesidad de adaptar las leyes existentes, por ejemplo, el Convenio de Budapest (2001), se convirtió en el primer tratado internacional para combatir la ciberdelincuencia, proporcionando un marco legal y operativo para que los países colaboren en la lucha contra este fenómeno.

En la actualidad, la ciberdelincuencia representa una amenaza que afecta tanto a individuos como a organizaciones y gobiernos. La creciente dependencia de la tecnología ha incrementado la vulnerabilidad de los sistemas de información, lo que ha permitido a los delincuentes desarrollar técnicas más sofisticadas, los ataques

cibernéticos contra sistemas bancarios, datos de salud o infraestructuras de energía son ejemplos de cómo la ciberdelincuencia ha evolucionado para convertirse en un problema de seguridad nacional.

3.2.1.2.Naturaleza jurídica

La ciberdelincuencia tuvo una naturaleza jurídica principalmente penal ya que comprendió conductas ilícitas que lesionaron bienes jurídicos protegidos como la intimidad, la propiedad y la seguridad de la información valiéndose de medios tecnológicos; esta naturaleza penal se complementó con un enfoque constitucional puesto que muchas de estas conductas afectaron derechos fundamentales reconocidos en la Constitución Política como el derecho a la intimidad, la protección de datos personales, el secreto de comunicaciones y el derecho a la información segura lo cual evidenció la necesidad de adaptar el ordenamiento jurídico a los retos de la era digital por otro lado la ciberdelincuencia también tuvo una dimensión internacional ya que muchos de los delitos informáticos fueron cometidos desde otras jurisdicciones lo que exige cooperación entre países, armonización normativa y aplicación de tratados como el Convenio de Budapest.

3.2.1.3.Elementos constitutivos

La ciberdelincuencia se configuró a partir de varios elementos que permitieron entender su estructura como fenómeno delictivo en el entorno digital, en primer lugar estuvo presente la conducta dolosa, ya que el ciberdelincuente actuó con intención clara de causar daño o de obtener un beneficio indebido, utilizando medios informáticos como herramienta principal para ejecutar la acción, en segundo lugar se identificó el uso de tecnologías de la información y la comunicación, lo cual diferenció estos delitos de los tradicionales, ya que no requieren presencia física sino un entorno

digital donde el delincuente puede operar desde cualquier lugar, también se consideró el bien jurídico vulnerado, siendo generalmente la privacidad, el patrimonio, la identidad o la información personal de las víctimas, adicionalmente se tomó en cuenta la afectación a sistemas o infraestructuras digitales, ya que muchos de estos delitos no solo impactaron a las personas sino también a instituciones públicas o privadas mediante el ingreso no autorizado, manipulación de datos o sabotaje de plataformas, finalmente se incorporó como elemento la dificultad de persecución, porque estos delitos se caracterizaron por el anonimato, la velocidad de ejecución y la facilidad de ocultar rastros, lo que obstaculizó su investigación y sanción efectiva**.**

3.2.1.4.Características y modalidades

Indica Acurio (2016) que se refiere al conjunto de actividades ilícitas que utilizan tecnologías de la información y la comunicación como herramientas o medios para llevar a cabo actos delictivos.

a. Característica

Es de tipo transnacional ya que los delitos cibernéticos no reconocen fronteras físicas, lo que permite a los perpetradores actuar desde cualquier lugar del mundo, a menudo dificultando la localización y persecución penal y estas actividades suelen ser altamente técnicas, empleando métodos sofisticados como ataques de phishing, ransomware, intrusiones a sistemas de datos, y la manipulación de redes informáticas para acceder a información sensible o interrumpir servicios críticos.

b. Modalidades

La criminalidad informática incluye una amplia variedad de conductas ilícitas, entre las cuales destacan:

- Fraude informático: Uso indebido de herramientas digitales para obtener beneficios económicos, como la manipulación de sistemas financieros o la creación de sitios web falsos para capturar datos bancarios.
- Robo de identidad: Obtención y uso no autorizado de información personal para cometer actos fraudulentos.
- Delitos contra la confidencialidad de datos: Acceso indebido a sistemas de información, interceptación de comunicaciones electrónicas o alteración de datos almacenados.
- Ataques a infraestructuras críticas: Actividades dirigidas a desestabilizar sistemas fundamentales para la seguridad nacional, como redes de energía, salud o transporte.

3.2.1.5.Nuevas modalidades de ciberdelincuencia

Estas nuevas prácticas se caracterizan por su capacidad de adaptarse a las medidas de seguridad existentes, explotando vulnerabilidades tecnológicas, humanas y normativas algunas también resaltadas por García y Pilco (2024) son:

- Phishing y Smishing

  El phishing sigue consiste en engañar a las víctimas mediante correos electrónicos o sitios web falsos que aparentan ser de confianza, para obtener información sensible como contraseñas o datos bancarios,

  El smishing, por otro lado, utiliza mensajes de texto para lograr el mismo objetivo.

  En el contexto de la tesis, estas modalidades son relevantes porque exponen cómo los ciberdelincuentes manipulan la confianza de las víctimas para vulnerar su información personal, poniendo en riesgo el derecho a la protección de sus datos.

- Ransomware

  Considerada una modalidad altamente dañina, este tipo de ataque implica la instalación de software malicioso que encripta los datos de las víctimas, quienes solo pueden recuperar su información pagando un rescate, generalmente en criptomonedas para dificultar el rastreo.

  Aunque no se centra en la estafa directa, el ransomware puede ser utilizado como una herramienta secundaria en delitos de estafa, especialmente si los datos obtenidos a través de técnicas de engaño son posteriormente encriptados para extorsionar a las víctimas.

- Deepfakes

  Representan una modalidad emergente que combina inteligencia artificial y manipulación digital para crear imágenes, videos o audios falsos extremadamente realistas, técnica utilizada en fraudes, extorsiones e incluso en campañas de desinformación, el potencial para suplantar identidades o crear pruebas falsas plantea serios desafíos legales y éticos, ya que puede ser utilizada tanto para delitos económicos como para ataques a la privacidad.

- Ataques a infraestructuras críticas

  Los ciberdelincuentes también han comenzado a enfocarse en infraestructuras críticas, como redes de energía, sistemas de salud o redes de transporte los cuales buscan interrumpir servicios esenciales u obtener beneficios económicos mediante el chantaje puesto que en muchos casos, los atacantes aprovechan la falta de actualización de los sistemas o la inadecuada implementación de protocolos de ciberseguridad.

  Si bien este tipo de delito generalmente afecta a organizaciones, puede estar vinculado a estafas cuando los ciberdelincuentes acceden a bases de datos

personales para vender o manipular información como es en el caso de Cusco que podría reflejarse en el acceso indebido a sistemas municipales u otras entidades no protegidas.

- Sextorsión

  Otra modalidad en aumento, en la que los ciberdelincuentes amenazan a las víctimas con divulgar imágenes o videos íntimos obtenidos de manera ilegal, a menos que se les pague una suma de dinero.

  Si bien su relación con las estafas es menos evidente, la sextorsión puede involucrar la manipulación de datos personales obtenidos ilegalmente, lo que compromete la privacidad de las víctimas y puede derivar en casos de estafa emocional o económica.

3.2.1.6. Causas y consecuencias

En cuanto a sus causas, se identificó que surgió principalmente debido a la expansión acelerada del uso de internet sin que existiera una cultura digital sólida ni medidas de protección adecuadas, así como por la falta de legislación específica que se adaptara a las nuevas formas de delito que se desarrollaron en entornos virtuales, además se evidenció que muchos países, incluido el Perú, no contaron con una estructura institucional con capacidades técnicas y humanas suficientes para enfrentar este fenómeno, también influyó la facilidad de anonimato que ofrecieron las redes, lo que permitió a los delincuentes operar sin ser identificados ni sancionados de forma inmediata.

Respecto a su desarrollo, se observó que al inicio los ataques cibernéticos fueron esporádicos y limitados a sabotajes simples o envío de virus, sin embargo con el paso de los años y el avance de la tecnología, estos delitos se volvieron más complejos y organizados, pues los ciberdelincuentes comenzaron a utilizar técnicas

como el phishing, el smishing, el vishing, el malware personalizado y la suplantación de identidad a través de perfiles falsos en redes sociales o correos electrónicos engañosos, todo ello con el fin de obtener información confidencial de las víctimas y realizar estafas con un nivel de sofisticación cada vez mayor, incluso se detectó la existencia de redes criminales dedicadas exclusivamente a este tipo de actividad

En relación a sus consecuencias, estas fueron tanto sociales como jurídicas y económicas, ya que a nivel personal muchas víctimas perdieron ahorros, sufrieron afectaciones emocionales o vieron comprometida su privacidad, mientras que a nivel institucional se produjeron filtraciones masivas de datos, colapsos en sistemas informáticos y pérdida de credibilidad frente a los usuarios, además el estado tuvo que enfrentar retos importantes en términos de legislación, persecución penal y cooperación internacional, pues estos delitos no solo se cometieron desde dentro del país, sino que muchas veces provinieron de redes internacionales que operaron desde distintos continentes, lo que dificultó la identificación de los responsables y la aplicación de sanciones efectivas

3.2.1.7.Delito de estafa

En cuanto al delito de estafa se caracteriza por el uso de engaño, astucia, ardid u otra forma fraudulenta para obtener un beneficio ilícito en perjuicio de otra persona. Este delito afecta el patrimonio de la víctima, quien es inducida a error mediante maniobras engañosas del autor. En el Código Penal peruano, el artículo 196 establece que:

"El que procura para sí o para otro un provecho ilícito en perjuicio de tercero, induciendo o manteniendo en error al agraviado mediante engaño, astucia, ardid u

otra forma fraudulenta, será reprimido con pena privativa de libertad no menor de uno ni mayor de seis años" (Codigo Penal Peruano, 1991).

Las estafas pueden adoptar diversas formas, cada una con características y métodos específicos, algunas tipologías comunes incluyen: estafa simple, que implica un engaño directo a la víctima para obtener un beneficio económico; estafa agravada, que incluye situaciones como el abuso de confianza, uso de violencia, engaño a menores o personas vulnerables, y otras circunstancias que agravan la pena; fraude bancario, que implica el uso de técnicas fraudulentas para sustraer dinero de cuentas bancarias, como phishing, clonación de tarjetas y otros métodos; fraude inmobiliario, relacionado con la compra y venta de propiedades, donde el estafador se hace pasar por el propietario o vendedor legítimo; y estafa en venta de vehículos, donde se manipula información o documentos para vender vehículos con características diferentes a las anunciadas.

3.2.1.8.Modalidades del delito de estafa

Se manifiesta en diferentes modalidades, cada una con particularidades que permiten comprender su alcance jurídico.

La estafa simple constituye la forma más común, caracterizada por el engaño directo a la víctima con el fin de obtener un beneficio económico ilegítimo.

A esta modalidad se suma la estafa agravada, que contempla circunstancias de mayor gravedad, como el abuso de confianza, la participación de dos o más personas o la afectación a grupos vulnerables.

3.2.1.9. Artículo 196-A: Estafa agravada

El artículo 196-A del Código Penal regula la figura de la estafa agravada, estableciendo una pena privativa de libertad no menor de cuatro ni mayor de ocho años, además de multa (Codigo Penal Peruano, 1991).

La norma señala que la agravante se configura cuando el delito se comete en agravio de menores de edad, personas con discapacidad, mujeres en estado de gravidez o adultos mayores, debido a su condición de especial vulnerabilidad; también se considera agravada cuando participan dos o más personas en la comisión del hecho o cuando existe pluralidad de víctimas afectadas en un mismo acto delictivo.

También, se contempla la agravante en operaciones de compra y venta de vehículos motorizados o bienes inmuebles; en casos de acceso como sustracción de datos de tarjetas de crédito o de ahorro emitidas por entidades financieras; en situaciones en las que el autor se aprovecha de la vulnerabilidad particular de la víctima; finalmente, la norma incorpora el uso de tecnologías avanzadas, como la manipulación de voz, imagen o movimiento corporal a través de inteligencia artificial o herramientas análogas, siempre que generen perjuicio económico a la persona afectada.

3.2.1.10. Ciberestafa o fraude informático

Una tipología relevante en la actualidad es la estafa por Internet o ciberestafa, que ha aumentado significativamente con la proliferación del comercio electrónico y las transacciones en línea, la ciberestafa incluye métodos como el phishing, donde se engaña a la víctima para que revele información personal o financiera mediante correos electrónicos falsos que parecen ser de instituciones legítimas; el pharming, que redirige

a las víctimas a sitios web fraudulentos sin su conocimiento; y el hacking, donde los estafadores acceden ilegalmente a sistemas informáticos para robar información.

3.2.1.11. Penalidad

La pena por el delito de estafa varía dependiendo de las circunstancias y la gravedad del delito, en su forma básica, la estafa se castiga con una pena privativa de libertad no menor de uno ni mayor de seis años. Sin embargo, existen circunstancias agravantes que pueden incrementar la pena. Por ejemplo, si la estafa causa un perjuicio económico grave o se comete mediante el abuso de una relación de confianza, la pena puede ser de hasta ocho años de prisión.

3.2.1.12. Teoría relevante

a. Teoría del Triángulo del Fraude

La Teoría del Triángulo del Fraude, desarrollada por Donald R. Cressey, redactada y analizada por Saluja et al. (2021) teoría abordada en relación a la segunda categoría de la investigación, el cual es una herramienta fundamental para entender las causas del fraude y cómo prevenirlo, esta teoría identifica tres elementos esenciales que deben estar presentes para que se produzca un fraude: presión, oportunidad y racionalización.

La presión se refiere a las motivaciones o necesidades que llevan a una persona a cometer fraude, pueden ser de naturaleza financiera, como deudas o problemas económicos, o de carácter personal, como la necesidad de mantener un estilo de vida o satisfacer expectativas familiares creando el impulso inicial para considerar el fraude como una solución a estos problemas.

En cuanto a la oportunidad, se refiere a las circunstancias que permiten que el fraude ocurra, oportunidad que generalmente surge debido a debilidades en los

controles internos de una organización, como la falta de segregación de funciones, supervisión inadecuada o sistemas de auditoría deficientes ello proporciona el medio por el cual una persona puede cometer fraude sin ser detectada.

La racionalización es el proceso mediante el cual el individuo justifica sus acciones fraudulentas, las personas que cometen fraude a menudo encuentran maneras de justificar su comportamiento, convenciéndose de que sus acciones son aceptables o que no causarán daño.

Dicha teoría es altamente relevante para la categoría de delito de estafa en la investigación ya que ofrece un marco detallado para analizar las razones detrás de las estafas y proporciona una estructura para identificar los factores que contribuyen a la ocurrencia de fraudes, en el contexto de Cusco, aplicar esta teoría permite explorar cómo las distintas tipologías de estafa están influenciadas por la presión, la oportunidad y la racionalización.

Al identificar y analizar los elementos de presión, oportunidad y racionalización, se puede obtener una comprensión más profunda de las dinámicas que facilitan las estafas.

3.2.2. Protección de datos personales

3.2.2.1.Conceptos histórico conceptual

La protección de datos personales ha transitado un camino histórico significativo, desde su concepción inicial hasta su evolución en la era digital.

Este concepto comenzó a ganar relevancia en el siglo XX con el surgimiento de tecnologías capaces de recopilar y procesar grandes volúmenes de información ; en sus primeras etapas, la necesidad de proteger la información personal surgió como una respuesta a las intrusiones tecnológicas en la vida privada, siendo el artículo, The Right

to Privacy analizado por Nieves (2012), uno de los primeros en abordar esta problemática. Sin embargo, no fue hasta el desarrollo de las computadoras y la automatización de los procesos informáticos que los países empezaron a legislar sobre esta materia de manera concreta.

Como lo narran Sánchez y Rojas (2022); Alemania lideró este esfuerzo al promulgar, en 1970, la primera ley de protección de datos personales, marcando un hito en el ámbito internacional, este ejemplo fue seguido por países europeos como Suecia y Francia; posteriormente, la Unión Europea fortaleció estas directrices con la Directiva 95/46/CE y, más recientemente, con el Reglamento General de Protección de Datos que entró en vigor en 2018, convirtiéndose en el estándar internacional más avanzado en esta materia.

En América Latina, la regulación en este campo ha sido más tardía y fragmentada. Países como Argentina y México dieron los primeros pasos; en Perú, la Ley N°29733, promulgada en 2011, representó un avance importante al establecer un marco legal para la protección de datos personales, alineándose con los estándares internacionales.

3.2.2.2.Naturaleza jurídica

La protección de datos personales tuvo una naturaleza jurídica de carácter fundamental ya que se basó en el reconocimiento del derecho a la intimidad, a la autodeterminación informativa y al respeto por la privacidad, derechos consagrados en diversos tratados internacionales y en la propia Constitución Política del Perú; en ese marco jurídico este derecho fue considerado autónomo y progresivo por lo que mereció una regulación específica orientada a resguardar la información personal frente a su uso indebido, su tratamiento desproporcionado o su transferencia no

autorizada; de ese modo, la promulgación de la Ley N.° 29733 y su reglamento aprobado por Decreto Supremo N.° 003-2013-JUS representaron el reconocimiento expreso de la protección de datos personales como un derecho con garantías propias dentro del ordenamiento jurídico peruano además, esta ley dispuso la creación de la Autoridad Nacional de Protección de Datos Personales como ente supervisor del cumplimiento de las normas en esta materia, lo que confirmó su naturaleza jurídica vinculante y reguladora no solo para el sector público sino también para el ámbito privado.

3.2.2.3.Datos personales

Los datos personales son toda aquella información que identifica o permite identificar a una persona física de manera directa o indirecta.

Este concepto según la Comisión Europea (2024) incluye información básica como el nombre, apellido, número de documento de identidad o dirección, así como otros datos más sensibles relacionados con aspectos financieros, médicos, laborales o de comportamiento en entornos digitales.

En el ámbito legal, los datos personales se clasifican generalmente en dos categorías (Defensoria del Pueblo, 2019): los datos generales como nombre, edad o nacionalidad y los datos sensibles, que son aquellos que pueden afectar la privacidad o la dignidad de una persona, tales como información de salud, orientación sexual, creencias religiosas o ideología política.

El manejo adecuado de los datos personales es esencial en la era digital, ya que esta información es utilizada en múltiples ámbitos, desde transacciones comerciales hasta servicios públicos y redes sociales.

3.2.2.4.Definición conceptual general

La protección de datos personales según Serrano (2023) se refiere al conjunto de principios, medidas y procedimientos orientados a asegurar la confidencialidad y el manejo de los datos personales que puede identificar a un individuo, en ese entender la protección de datos personales implica un conjunto de normas, prácticas y tecnologías diseñadas para salvaguardar la confidencialidad y la protección de los datos que puede identificar a un individuo.

3.2.2.5.Datos robados en los delitos informáticos

El robo de datos se entiende según Acurio (2016) como una de las prácticas más recurrentes de la ciberdelincuencia ya que consistió en la apropiación indebida de información almacenada en sistemas digitales; los delincuentes ingresaron mediante enlaces maliciosos, malware o suplantación de identidad y accedieron a bases de datos con información sensible como identidades, direcciones o accesos a cuentas; jurídicamente esta conducta vulneró el derecho a la intimidad y a la autodeterminación informativa y aunque en el Perú existió normativa como la Ley 30096 los vacíos en la regulación dificultaron la sanción oportuna y abrieron espacios de impunidad.

3.2.2.6.Robo de información

Cotrina (2020) indico que el robo de información se diferenció de los datos robados porque abarcó también secretos empresariales, documentos internos y comunicaciones privadas; esta práctica afectó tanto a individuos como a organizaciones generando perjuicios económicos y en algunos casos comprometiendo la seguridad del Estado.

- **Datos personales**

  Es el núcleo de la protección jurídica porque es identificar a un individuo a través de nombres, direcciones, documentos o huellas digitales.

- **Datos comerciales**

  Comprenden contratos, estrategias de mercado, registros de clientes e información de proveedores; este tipo de información resulta valiosa en el mercado negro digital porque se utiliza para competencia desleal, chantajes o venta de bases de datos.

- **Datos financieros**

  Los datos financieros son los más buscados porque permiten realizar transferencias no autorizadas, compras ilegales o créditos fraudulentos; entre los más afectados se encuentran números de tarjetas, contraseñas bancarias e historiales financieros de personas y empresas.

3.2.2.7.Fraude en línea

Se reconoce como una de las expresiones más extendidas de la ciberdelincuencia porque aprovecha la confianza de los usuarios en los entornos digitales para obtener datos personales o financieros mediante engaños.

- Sitios falsos

  Los delincuentes crean páginas web que imitan a bancos, tiendas virtuales, servicios de correo electrónico o redes sociales; el objetivo es que las víctimas ingresen voluntariamente sus credenciales, contraseñas o números de tarjetas creyendo que están en un portal legítimo; esta técnica se consolida como una de las más efectivas porque reproduce con gran detalle el diseño de las páginas originales, lo que dificulta al usuario promedio detectar el fraude.

- Engaño a usuarios

El engaño no se limita a páginas falsas, también se manifiesta en correos electrónicos, mensajes de texto, llamadas telefónicas y notificaciones falsas que simulan ser comunicaciones oficiales; en estos mensajes se utilizan estrategias de ingeniería social para inducir a las personas a revelar datos sensibles o descargar archivos maliciosos.

3.2.2.8.Malware

Monje (2017) indica que este se entiende como un software malicioso diseñado para infiltrarse en sistemas informáticos y alterar su funcionamiento con fines ilícitos; su objetivo es vulnerar la seguridad de los datos, robar información confidencial o controlar dispositivos sin autorización.

- Virus: programas que se insertan en archivos legítimos y se propagan cuando los usuarios los ejecutan, dañando documentos, corrompiendo sistemas o eliminando información.
- Troyanos: aplicaciones que se presentan como inofensivas pero que permiten a los atacantes tener acceso remoto al sistema, robar datos o instalar otros programas maliciosos sin que el usuario lo note.

3.2.2.9.Ciberacoso

Según Haro (2021), el ciberacoso se entiende como una conducta hostil realizada a través de medios digitales que busca intimidar, amenazar o vulnerar la integridad psicológica de una persona; esta práctica afecta tanto a menores como a adultos y genera consecuencias graves que van desde el daño emocional hasta la afectación de la reputación y la seguridad personal.

- Acoso en redes sociales

Se manifiesta mediante publicaciones ofensivas, difamaciones, difusión de rumores o suplantación de identidad; estas acciones son visibles para amplios grupos de personas, lo que aumenta la exposición y la gravedad del daño; los agresores utilizan la inmediatez de las redes para hostigar de manera constante.

- Acoso por correo electrónico

  Se basa en el envío repetitivo de mensajes ofensivos, hostigadores o con contenido no deseado; en muchos casos se utilizan direcciones falsas para ocultar la identidad del remitente, lo que dificulta identificar al agresor.

- Mensajes amenazantes

  Constituyen una de las formas más directas del ciberacoso, ya que buscan generar miedo en la víctima a través de advertencias de daño físico, económico o social; estos mensajes pueden transmitirse por redes sociales, correos, llamadas o aplicaciones de mensajería instantánea.

3.2.2.10. Protección

La protección es el conjunto de medidas, acciones y principios destinados a garantizar la seguridad, integridad y bienestar de algo o alguien frente a posibles riesgos, amenazas o daños, en términos generales, implica establecer barreras, controles o políticas que minimicen la vulnerabilidad y aseguren que los derechos, intereses o propiedades se mantengan resguardados.

Desde una perspectiva legal, la protección abarca la creación y aplicación de normativas que salvaguardan derechos fundamentales, como el derecho a la privacidad, el acceso a la justicia o la igualdad ante la ley, por otro lado, en el ámbito tecnológico, la protección como infiere e n la revista Transformación digital en el Perú (2023) se relaciona con el uso de herramientas y protocolos para garantizar la

seguridad de la información, preservando la confidencialidad, la integridad y la disponibilidad de los datos.

3.2.2.11. Protección constitucional

El artículo 2 inciso 6 de la Constitución reconoce el derecho fundamental de toda persona a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal tanto familiar.

En desarrollo de este mandato constitucional, el Estado promulgó la Ley N.° 29733, Ley de Protección de Datos Personales, con el propósito de establecer principios y reglas que orientan el tratamiento de la información personal.

En noviembre de 2024 se aprobó el Decreto Supremo N.° 016-2024-JUS que actualiza el Reglamento de la Ley N.° 29733; este reglamento introduce lineamientos más detallados sobre el consentimiento, el tratamiento de datos sensibles y el flujo transfronterizo de información, además obliga a las instituciones a implementar medidas de seguridad preventivas y protocolos de reporte inmediato en casos de incidentes que comprometan la información personal (Decreto Supremo N.° 016-2024-JUS, 2024).

3.2.2.12. Normatividad vigente

En Perú, la Ley N°29733 (2011) Ley de Protección de Datos Personales, establece un marco normativo cuyo propósito es garantizar el respeto por los derechos fundamentales, como la vida privada y la autodeterminación informativa. Según esta normativa, el tratamiento de datos personales debe respetar principios clave, como el consentimiento previo, la proporcionalidad en la recolección y el uso de datos, y la finalidad legítima para la que son recopilados, así mismo , el reglamento de esta ley

introduce lineamientos más detallados sobre las medidas de seguridad que deben implementar las entidades públicas y privadas para evitar el acceso no autorizado a la información.

En el ámbito internacional, el Reglamento General de Protección de Datos (2022) en la Unión Europea, ha marcado un estándar internacional en esta materia ya que se basa en principios como la legalidad, que exige que los datos solo se procesen con una base jurídica válida; la transparencia, que garantiza que las personas estén informadas sobre cómo se utiliza su información; la limitación del propósito, que prohíbe el uso de datos para fines distintos a los especificados inicialmente; y la minimización de datos, que busca que solo se recopile la información estrictamente necesaria para cumplir con los objetivos establecidos e introdujo derechos innovadores, como el derecho al olvido, que permite a los usuarios solicitar la eliminación de sus datos en ciertos casos, y el derecho a la portabilidad de los datos.

Una de las diferencias significativas entre el marco europeo y el peruano radica en el alcance y la implementación de estas normativas. Mientras que el GDPR establece sanciones económicas estrictas y aplica a cualquier entidad que procese datos de ciudadanos europeos, independientemente de su ubicación, la Ley N°29733 enfrenta desafíos relacionados con la supervisión y cumplimiento efectivo en el contexto local, donde las infraestructuras tecnológicas y los recursos para garantizar el cumplimiento son limitados.

3.2.2.13. Objeto de legalidad

Tiene como función primordial establecer un orden jurídico que permita prevenir el abuso de poder y proteger los derechos de las personas. Esto implica que todas las actuaciones de los ciudadanos, empresas e incluso del estado deben

enmarcarse en las disposiciones legales vigentes, respetando los principios de justicia, igualdad y transparencia.

En la citada norma Ley N° 29733 (2011) en título IV refiere a las obligaciones específicas que se debe de cumplir a fin de asegurar la protección y la confidencialidad de los datos, se deduce que el propietario de los datos, es decir, la persona a la que pertenecen los datos personales, está obligado a suministrar información precisa y actualizada siendo esencial para que la gestión de los datos se efectúe de forma precisa y eficaz, así mismo, el titular debe actuar con diligencia al dar su autorización para la gestión de su información personal, asegurándose de comprender plenamente las finalidades para las cuales se utilizarán sus datos y las implicaciones de dicho tratamiento. También es responsabilidad del titular ejercer sus facultades de acceso, corrección, eliminación y rechazo de forma oportuna, lo cual implica estar informado acerca de sus derechos y los métodos para hacerlos valer.

3.2.2.14. Principios

El encargado del tratamiento de datos personales ya sean empresas privadas o públicas, que puede tratarse de un individuo o entidad, ya sea pública o privada, que determina el tratamiento de los datos personales, tiene un conjunto de obligaciones para asegurar la protección de estos datos, de accesos indebidos, pérdidas, alteraciones o usos incompatibles con los fines para los cuales fueron recolectados.

Entre estas medidas, se incluyen técnicas de cifrado, sistemas de control de acceso y protocolos de seguridad informática, asimismo, es imprescindible que el tratamiento de los datos esté respaldado por la autorización explícita e informada del titular, siendo esta una de las principales obligaciones del encargado.

a. Transparencia

Es un principio esencial que obliga al encargado a informar de manera clara y accesible a los titulares de los datos sobre las finalidades del tratamiento, los procesos involucrados y los derechos que les asisten.

b. Reserva de la información

Además, el encargado del tratamiento tiene la obligación de asegurar la privacidad de la información personal implicando que cada individuo que participen en el tratamiento de los datos deben estar comprometidas a mantener la reserva de la información, salvo en los casos en que la ley permita o exija su divulgación y tiene también la obligación responder a las solicitudes de los titulares de los datos en relación con sus derechos de acceso, rectificación, cancelación y oposición, proporcionando respuestas claras y en el marco de los tiempos estipulados por la legislación.

c. Finalidad

Los datos personales solo deben ser recopilados y utilizados para propósitos específicos, explícitos y legítimos, evitando su uso para fines distintos sin el consentimiento del titular.

d. Proporcionalidad

Se refiere a la necesidad de limitar la recolección de datos al mínimo necesario para cumplir con la finalidad declarada, evitando el tratamiento excesivo o irrelevante de información.

e. Seguridad

Busca garantizar la protección de los datos personales mediante la implementación de medidas técnicas y organizativas adecuadas para prevenir su acceso no autorizado, pérdida o alteración.

3.2.2.15. Autoridad nacional de protección de datos persónales

La falta de cumplimiento de estas obligaciones antes mencionadas puede llevar a sanciones administrativas y legales, lo que subraya la importancia de que tanto el titular como el encargado del tratamiento cumplan con sus responsabilidades. En este sentido, y en concordancia con la Contraloría General de la República (2022) la Autoridad Nacional de Protección de Datos Personales llamada en adelante [ANDPD] juega una función fundamental en la vigilancia y aseguramiento de cumplimiento de las normativas, pudiendo realizar auditorías, investigaciones y aplicar sanciones cuando sea necesario.

En el Perú, la ANPDP es la entidad responsable de supervisar y garantizar el cumplimiento de la normativa de protección de datos personales, entidad, adscrita al Ministerio de Justicia y Derechos Humanos, tiene un rol fundamental en la promoción y defensa del derecho a la privacidad y la protección de los datos personales de los ciudadanos peruanos.

Entre sus funciones principales, la ANPDP supervisa que las organizaciones tanto públicas como privadas que manejan datos personales cumplan con las disposiciones legales y reglamentarias vigentes incluyendo verificar que el tratamiento de los datos se realice con el consentimiento adecuado, que los datos se mantengan exactos y actualizados, y que se implementen las medidas de seguridad necesarias a fin de resguardar la información frente a accesos indebidos y otros riesgos.

3.2.2.16. Teoría relevante de protección de datos personales

a. Teoría de la Gestión de la Privacidad en la Comunicación (Communication Privacy Management Theory)

La Teoría de la Gestión de la Privacidad en la Comunicación, desarrollada por Petronio (2019), se enfoca en cómo las personas deciden compartir o proteger su información privada mediante la creación de límites, estos límites son dinámicos y varían según el contexto y las relaciones interpersonales. Las reglas de privacidad se desarrollan a través de interacciones sociales y determinan cuándo, cómo y con quién se comparte la información.

Esta teoría es relevante ya que proporciona un marco para entender cómo los individuos gestionan su privacidad, lo cual es esencial para evaluar la efectividad de las medidas de protección de datos.

Al aplicar dicha teoría en esta investigación, se puede explorar cómo los ciudadanos de Cusco manejan su información personal en su vida diaria permitiendo analizar las decisiones sobre la divulgación de datos puede ayudar a identificar la efectividad de las políticas y prácticas actuales de protección de datos para con ello comprender no solo el cumplimiento de las normativas, sino también las percepciones y comportamientos de las personas respecto a su privacidad.

La relación de esta teoría con la protección de datos personales es directa y significativa ya que la teoría explica las dinámicas detrás de la gestión de la información privada, proporcionando una base sólida para analizar los desafíos y oportunidades en la implementación de políticas de protección de datos. Además, permite identificar áreas donde las normas pueden necesitar ajustes para ser más efectivas y alineadas con las prácticas y expectativas de los ciudadanos.

3.3. Definición de términos

- Ciberdelincuencia

  Se refiere a las actividades ilícitas realizadas a través de medios electrónicos o digitales, donde el uso de la tecnología es esencial para llevar a cabo delitos como estafas, robo de identidad y acceso no autorizado a información.

- Datos Personales

  Información que permite identificar o hace identificable a una persona física, incluyendo nombres, direcciones, números de identificación, datos financieros o cualquier otro dato relacionado con su privacidad.

- Phishing

  Técnica de ingeniería social utilizada para engañar a las personas, con el objetivo de obtener información confidencial como contraseñas, datos bancarios o números de tarjetas de crédito, mediante correos electrónicos o sitios web falsos.

- Deepfakes

  Contenido audiovisual manipulado mediante inteligencia artificial para crear imágenes, videos o audios falsos, que pueden ser utilizados para suplantar identidades o engañar a personas con fines delictivos.

- Protección de Datos Personales

  Conjunto de medidas legales, técnicas y organizativas destinadas a garantizar la privacidad y seguridad de los datos personales frente a su uso indebido o no autorizado.

- Estafa Digital

  Modalidad de fraude que se lleva a cabo a través de plataformas tecnológicas o sistemas digitales, donde los perpetradores engañan a las víctimas para obtener beneficios económicos o acceder a información sensible.

- Suplantación de Identidad

  Acto de hacerse pasar por otra persona en entornos digitales, utilizando su información personal para cometer fraudes o acceder a recursos que no le corresponden.

- Regulación Jurídica

  Normativas, leyes y directrices establecidas para regular el uso, manejo y protección de datos personales, así como las sanciones aplicables a quienes vulneren estos principios.

- Riesgos Informáticos

  Amenazas potenciales que comprometen la seguridad de los sistemas digitales, ya sea por ataques malintencionados, fallos técnicos o vulnerabilidades explotadas por ciberdelincuentes.

- Consentimiento Informado

  Permiso otorgado por el titular de los datos personales para su recopilación y uso, con pleno conocimiento de las finalidades y condiciones bajo las cuales serán tratados.

IV. Metodología

4.1. Tipo y nivel de investigación

El enfoque cualitativo fue definido por Hernandez y Mendoza (2023) se caracteriza por su énfasis en comprender fenómenos sociales, humanos o culturales desde la perspectiva de los participantes, permitiendo explorar en profundidad las percepciones, experiencias y prácticas que subyacen en estos fenómenos.

En el contexto específico de este estudio, el enfoque cualitativo permitió explorar las complejidades y las dinámicas sociales que influyen en la problemática abordada. A través de entrevistas en profundidad y análisis interpretativo, se pudieron identificar patrones, temas y relaciones significativas que informen sobre las prácticas y percepciones de los actores involucrados en este ámbito.

En cuanto al diseño de esta investigación fue fenomenológico que según Gallardo (2021) enfatiza que se caracteriza por su enfoque en la comprensión detallada y contextualizada de un fenómeno particular, desde la especial perspectiva de los participantes del estudio.

4.2. Ámbito temporal y espacial

La investigación se desarrolló en la provincia de Cusco; durante los años 2024-2025, centrándose en el análisis de la protección de datos personales frente a las nuevas técnicas de ciberdelincuencia en delitos de estafa.

4.3. Población y muestra

La población de esta investigación estuvo compuesta por abogados especializados en protección de datos personales y ciberdelincuencia, así mismos magistrados del Ministerio Publico y Poder Judicial del distrito de Cusco seleccionados debido a su conocimiento y experiencia en el tema, lo cual es fundamental para el análisis y comprensión del problema de investigación.

En cuanto a la muestra, se trabajó con siete abogados especializados en protección de datos personales y ciberdelincuencia en Cusco. La selección se realizó bajo un muestreo por elección propia, dado que se eligió de manera intencional a los profesionales que cumplían con los siguientes criterios.

Criterios de inclusión:

- Especialización: Los participantes deben ser abogados con especialización en derecho penal o ciberseguridad, con experiencia comprobada en casos relacionados con delitos informáticos o protección de datos personales.
- Experiencia profesional: Se incluirán profesionales que cuenten con al menos cinco años de experiencia en el campo del derecho penal o la ciberseguridad, lo que garantiza un nivel adecuado de conocimiento y comprensión de los temas en cuestión.
- Relevancia del rol: Los participantes deben estar involucrados activamente en la práctica del derecho, ya sea como litigantes, consultores o académicos, lo que asegura que sus perspectivas estén actualizadas y sean aplicables al contexto actual de Cusco.

Criterio de exclusión

- Se excluirán de la muestra aquellos participantes que, a pesar de cumplir con los requisitos básicos de especialización y experiencia, no estén actualmente involucrados en la práctica activa del derecho penal o la ciberseguridad.

4.4. Instrumentos

Las técnicas cualitativas estuvieron diseñadas para obtener información detallada y contextualizada que permita una comprensión de los fenómenos estudiados por ende se detallara el instrumento utilizado:

- Entrevistas: Las entrevistas permitieron explorar las experiencias, percepciones y conocimientos de los participantes sobre el tema de estudio ya que se contó con abogados especializados en derecho penal y delitos informáticos, se realizarán de manera individual y permitirán una interacción directa.

4.5. Procedimiento

Para someter la investigación a una recolección de datos el instrumento fue revisados por un panel de expertos los cuales son el Mag. Percy Miranda Chipa quien cuenta con amplia experiencia en el derecho penal con más de 18 años en función actualmente labora como defensor público, seguidamente se tuvo a Mag. Richard Max Quispe Calderón quien cuenta con una amplia experiencia con más de 7 años en función doctrinario de diversas universidades y finalmente como ultimo validador a Dr. Mario Hugo Silva Astete quien destaca como funcionario en la Corte Superior de Justicia de Cusco con más de 30 años de experiencia, este panel evaluó la pertinencia, claridad y coherencia de las preguntas incluidas en las entrevistas lo cual permitió realizar una recolección de datos adecuada cumpliendo el código de ética de la investigación.

4.6. Análisis de datos

La presentación y el análisis de los datos recopilados se realizaron utilizando métodos y técnicas adecuados para interpretar de manera efectiva los resultados de la investigación.

Para los datos obtenidos de entrevistas y respuestas abiertas en entrevistas, se emplearon técnicas de análisis cualitativo como la codificación temática y el análisis de contenido identificando patrones, categorías, ofreciendo una comprensión profunda de las percepciones y experiencias de los participantes.

Para aumentar la validez y confiabilidad de los resultados, se empleó la triangulación de datos, que consiste en utilizar múltiples métodos y fuentes de información para corroborar los hallazgos.

Por último, se derivarán las conclusiones de la investigación basadas en los datos obtenidos, integrando todos los hallazgos para proporcionar una respuesta comprensiva a las preguntas de investigación y cumplir con los objetivos planteados.

4.7. Consideraciones éticas

Durante el desarrollo de la investigación se respetaron en todo momento los principios éticos que rigen el trabajo académico, pues se garantizó que la participación de los abogados entrevistados fuera completamente voluntaria, además se les explicó previamente el propósito del estudio y se solicitó el consentimiento informado para hacer uso de su información personal, asimismo se utilizó la información recolectada únicamente con fines académicos sin realizar ningún tipo de manipulación ni alteración de sus respuestas, del mismo modo se aseguró la confidencialidad de sus identidades, ya que sus aportes fueron codificados para evitar cualquier vínculo directo con sus nombres o datos personales, por otro lado se garantizó también la originalidad

de esta investigación debido a que el análisis, los instrumentos, las categorías y los resultados fueron elaborados exclusivamente para el presente estudio sin copiar ni replicar trabajos previos, lo que reafirmó su carácter inédito y su aporte propio al conocimiento jurídico en el contexto local.

V. Resultados y discusión

5.2. Resultados

A continuación, se detallaron los resultados obtenidos en base a las entrevistas realizadas a siete abogados este criterio se expone cada resultado según el orden estructurado en el instrumento y conforme al sentido real de las respuestas brindadas.

Tabla 1

Técnicas de manipulación de datos más utilizadas según los abogados entrevistados

¿Cuáles consideran que son las técnicas más utilizadas de manipulación de datos en delitos de estafa en Cusco?	
Abog. Sanchez Valencia	Suplantación de identidad, llamadas telefónicas, mensajes de texto
Juez Holgado Noa	Suplantación de identidad, redes sociales, captación de menores
Abog. Quispe Ramos	Anticresis de inmuebles, escaneo de nombre de propietarios
Juez Román Gil	Phishing, smishing, vishing, malware, spyware, spoofing, suplantación de identidad
Abog. Loaiza Morales	Phishing, llamadas telefónicas, páginas falsas, clonación, suplantación de identidad
Abog. Chávez Soto	Redes sociales, correos electrónicos, WhatsApp, suplantación de identidad
Fiscal Chirinos Meneses	Suplantación de identidad, redes sociales, Facebook, WhatsApp, creación de perfiles falsos

La mayoría de los abogados entrevistados señaló que la suplantación de identidad fue la técnica más común usada en los casos de estafa digital, ya que algunos explicaron que los delincuentes utilizaban llamadas o mensajes de texto para engañar a las víctimas mientras que otros mencionaron que estas suplantaciones se daban a través de redes sociales como Facebook y WhatsApp donde los perpetradores creaban perfiles falsos y con ellos lograban ganarse la confianza de las personas además se

indicaron casos en los que los estafadores usaban correos electrónicos o páginas falsas para robar información personal lo cual se relaciona con prácticas como el phishing el smishing o el vishing también se reportó una situación distinta donde se usaban documentos escaneados para modificar el nombre de los propietarios en trámites de anticresis lo que muestra que las estafas no solo se daban por internet sino también en estos casos legales pero finalmente todos coincidieron en que muchas personas caían en estos engaños por falta de conocimiento digital y porque confiaban en lo que recibían sin verificar si era real o falso

Tabla 2

Afectación de las técnicas de manipulación en los datos personales según entrevistados

	Desde su experiencia ¿cómo afecta estas técnicas a la protección de los datos personales de las víctimas?
Abog. Sanchez Valencia	Pérdida económica, daño emocional, daño psicológico
Juez Holgado Noa	Pérdida patrimonial, vulneración a la intimidad
Abog. Quispe Ramos	Daño económico, daño personal, daño familiar, daño social, falta de respuesta del estado.
Juez Román Gil	Robo de identidad, acceso a cuentas, créditos falsos, extorsión, daño emocional y económico
Abog. Loaiza Morales	Riesgo de información, pérdidas económicas, daño emocional, estrés, ansiedad
Abog. Chávez Soto	Falta de consentimiento, incomodidad al compartir datos, uso indebido por bancos
Fiscal Chirinos Meneses	Afectación al patrimonio

Los abogados entrevistados coincidieron en que las técnicas de manipulación de datos afectan directamente la protección de los datos personales de las víctimas ya que varios señalaron que estas prácticas generan pérdidas económicas que muchas

veces no pueden recuperarse además de provocar consecuencias emocionales que van desde incomodidad y ansiedad hasta afectaciones psicológicas más graves también se mencionó que muchas víctimas no comprenden los riesgos reales de entregar sus datos lo cual hace que los delincuentes accedan a cuentas bancarias soliciten créditos e incluso extorsionen a las personas con la información robada algunos de los entrevistados también resaltaron que la afectación no es solo individual sino también familiar y social ya que estas situaciones impactan en la conducta de la víctima y en cómo se relaciona con su entorno asimismo se mencionó que hay una sensación de abandono por parte de las autoridades al no responder con eficacia ante este tipo de delitos finalmente se señaló que en algunos casos los datos son usados sin consentimiento lo cual vulnera la privacidad de las personas y debería ser sancionado con mayor firmeza.

Tabla 3

Vulnerabilidades más frecuentes en la protección de datos personales según entrevistados

¿Cuáles consideran que son las vulnerabilidades más frecuentes en la protección de datos personales?	
Abog. Sanchez Valencia	Falta de respaldo, debilidad en resguardo, empresas privadas
Juez Holgado Noa	Falta de seguridad en bases de datos, deficiencia en protección estatal y privada
Abog. Quispe Ramos	Suplantación de identidad, uso de tarjetas electrónicas
Juez Román Gil	Contraseñas débiles, wifi público, desconocimiento digital, empresas sin protocolos de protección
Abog. Loaiza Morales	Falta de educación digital, contraseñas simples, no reconocimiento de técnicas de manipulación
Abog. Chávez Soto	Falta de monitoreo, sistemas inseguros, pruebas no confiables, controles desactualizados
Fiscal Chirinos Meneses	Contraseñas repetidas, acceso no autorizado, vulnerabilidad generalizada

En cuanto a esta tercera tabla los abogados entrevistados identificaron varias debilidades comunes que afectan la protección de los datos personales muchos de ellos coincidieron en que existe una falta generalizada de educación en temas de seguridad digital además varios mencionaron que muchas personas usan la misma contraseña para todas sus cuentas lo cual facilita el acceso no autorizado cuando una de ellas es vulnerada, también se señaló que las redes wifi públicas representan un riesgo constante ya que al conectarse sin medidas de seguridad se expone información personal a terceros por otro lado algunos participantes comentaron que las empresas tanto privadas como públicas no han implementado controles técnicos adecuados para proteger las bases de datos lo que deja espacios abiertos que los ciberdelincuentes aprovechan con facilidad además se resaltó que no se monitorean los sistemas de forma

continua ni se actualizan los protocolos de seguridad lo que aumenta el nivel de exposición.

Tabla 4

Opinión sobre la suficiencia de la normativa peruana frente a la ciberdelincuencia

En tu opinión ¿La normativa actual sobre protección de datos en Perú es suficiente para abordar las amenazas de ciberdelincuencia en delitos de estafa?	
Abog. Sanchez Valencia	Normativa no adaptada, legislación desactualizada
Juez Holgado Noa	Falta de combate, normativa ineficaz
Abog. Quispe Ramos	Código penal desactualizado, implementación deficiente, avance de la ciberdelincuencia
Juez Román Gil	Insuficiencia normativa, falta de actualización, débil fiscalización, cooperación internacional limitada
Abog. Loaiza Morales	Casos impunes, falta de dinamismo, necesidad de sistemas adecuados, adaptación tecnológica
Abog. Chávez Soto	Impunidad, vacíos legales, normativa rígida, falta de adaptación del ordenamiento jurídico
Fiscal Chirinos Meneses	No

En este apartado las respuestas fueron drásticas ya que todos los abogados entrevistados coincidieron en que la normativa peruana actual no resulta suficiente para enfrentar las amenazas de la ciberdelincuencia ya que varios indicaron que las leyes no se encuentran adaptadas al contexto digital actual y que tampoco se actualizan con la rapidez necesaria para responder ante nuevas técnicas delictivas además se mencionó que el código penal no ha sido modificado de forma adecuada lo que impide sancionar correctamente estas conductas y deja muchos casos en la impunidad también se destacó que existe una falta de fiscalización por parte de las autoridades así como una cooperación internacional limitada lo cual debilita el enfrentamiento que se tenga

con estos delitos informáticos por otro lado se subrayó que el ordenamiento jurídico en su estado actual no contempla medidas concretas ni herramientas tecnológicas que permitan identificar a los autores ni evitar que repitan sus acciones.

Tabla 5

Evaluación de los mecanismos legales y sancionadores frente a la ciberdelincuencia

¿Cómo evalúa la efectividad de los mecanismos legales y sancionadores en la lucha contra la ciberseguridad en Cusco?	
Abog. Sanchez Valencia	Delito tangible, necesidad de recurso, personal especializado, actualizar normativa
Juez Holgado Noa	Precariedad tecnológica, falta de personal capacitado
Abog. Quispe Ramos	Normas desactualizadas, mejorar Código Penal, avance tecnológico
Juez Román Gil	Recursos insuficientes, policía y justicia con limitaciones, lentitud del sistema
Abog. Loaiza Morales	Falta de efectividad, carencia de sistemas, escasa cooperación interinstitucional, delitos más complejos
Abog. Chávez Soto	Inadecuada respuesta legal, dificultad para identificar autores, uso del anonimato
Fiscal Chirinos Meneses	Deficiencia en la investigación, no en la norma

Como precede en la tabla cinco los entrevistados indicaron que los mecanismos legales y sancionadores aún no son efectivos para enfrentar la ciberdelincuencia en Cusco ya que mencionaron que existe una falta de personal capacitado tanto en el sistema fiscal como en la policía lo cual limita la capacidad de reacción frente a estos delitos también se dijo que las leyes actuales necesitan ser actualizadas y adaptadas al ritmo con el que evolucionan las nuevas tecnologías además se reportó que los procesos judiciales son lentos y que muchas víctimas ni siquiera denuncian por desconfianza en la capacidad del sistema por otro lado algunos abogados señalaron

que el problema no está en la norma sino en la forma en la que se investiga ya que no existen herramientas eficientes que permitan rastrear con rapidez los dispositivos o usuarios responsables de los ataques digitales además se afirmó que la recolección de pruebas electrónicas es complicada y que la falta de coordinación entre instituciones nacionales e internacionales debilita aún más la respuesta ante este tipo de delitos.

Tabla 6

Medidas para mejorar la protección de los datos personales según entrevistados

Desde su experiencia, ¿Qué medidas adicionales podrían implementarse para mejorar la protección de los datos personales en el contexto de la ciberdelincuencia?	
Abog. Sanchez Valencia	Actualizar legislación, avances digitales, falta de entes reguladores
Juez Holgado Noa	Fortalecer gobierno digital, coordinación interinstitucional, política nacional
Abog. Quispe Ramos	Implementación tecnológica, detección de alteraciones, actualización del Código Penal
Juez Román Gil	Educación digital, campañas, inversión en tecnología, colaboración público-privada
Abog. Loaiza Morales	Invertir en sistemas de detección, programas de prevención, conciencia ciudadana
Abog. Chávez Soto	Contraseñas seguras, doble autenticación, software de seguridad, ordenamiento jurídico desfasado
Fiscal Chirinos Meneses	Equipos especializados, oficina técnica, personal capacitado, evitar eliminación de pruebas

En cuanto al aporte de la última preguntas propusieron diversas medidas para mejorar la protección de los datos personales varios coincidieron en que el estado debería actualizar con urgencia la legislación vigente para adaptarla al ritmo de los avances digitales además se planteó que la creación de una oficina especializada

ayudaría a prevenir la eliminación de pruebas y permitiría una respuesta inmediata ante estos delitos también se señaló que se necesita personal capacitado tanto en el manejo de sistemas como en el uso de herramientas tecnológicas adecuadas por otro lado se sugirió implementar campañas de educación digital dirigidas a la población para generar conciencia sobre los riesgos que existen al compartir información en línea algunos abogados insistieron en que deben fortalecerse las acciones de coordinación entre instituciones públicas y privadas para facilitar el intercambio de información y hacer más eficiente la persecución del delito finalmente se recomendó el uso de programas de seguridad como contraseñas dobles con autenticación en dos pasos y antivirus actualizados que deberían ser promovidos desde el propio estado como parte de una política pública de prevención.

5.2. Discusión

En cuando al objetivo general abordado en este trabajo se presenta los resultados obtenidos a partir de las entrevistas realizadas a los abogados quienes evidenciaron que las nuevas técnicas de ciberdelincuencia han generado un impacto directo sobre la protección de los datos personales sobre todo en delitos de estafa ya que los entrevistados coincidieron en que las modalidades delictivas más recurrentes han sido el phishing el smishing la suplantación de identidad y el uso de perfiles falsos en redes sociales plataformas que se han convertido en terreno fácil para captar víctimas que desconocen los riesgos a los que se exponen al interactuar digitalmente con desconocidos, en esa línea también señalaron que estas prácticas se han visto facilitadas por la falta de conocimiento tecnológico de la población así como por la inexistencia de una respuesta oportuna por parte de las instituciones encargadas de prevenir y sancionar estos hechos lo que permite que los ciberdelincuentes operen con impunidad no solo generando pérdidas económicas sino vulnerando gravemente el

derecho a la privacidad, también comentaron que se observó que la mayoría de víctimas entrega voluntariamente sus datos al no saber identificar señales de alerta.

Ante las respuestas obtenidas se encuentra respaldo en diversos antecedentes internacionales y nacionales que abordan esta misma problemática desde distintas realidades por ejemplo el estudio de Benavides (2022) concluyó que a pesar de los avances digitales actuales el entorno virtual sigue siendo inseguro para las actividades cotidianas en línea pues ninguna página web ni red social garantiza plenamente la protección de datos personales incluso para grandes corporaciones lo que se alinea con lo observado en Cusco donde las estafas digitales han afectado tanto a ciudadanos comunes como a usuarios con experiencia básica en internet; de igual manera el trabajo de Aredo (2021) quien señaló que la legislación penal peruana aún mantiene definiciones genéricas que no permiten una delimitación precisa del phishing lo que también fue mencionado por los abogados al referirse a las dificultades para encajar estos actos dentro de tipos penales claros y sancionables y por otra parte el estudio de Aguilar et al. (2022) en Ecuador indicó que a pesar de existir normas específicas la protección efectiva de datos no es posible si no se combina con una inversión sostenida en tecnología y un cambio cultural en la forma de manejar la información personal lo que coincide directamente con las declaraciones de los entrevistados que señalaron que en Cusco aún no existe conciencia plena del riesgo digital ni desde el ciudadano ni desde las instituciones.

A partir de lo expuesto la investigadora puede afirmar que las implicancias de las nuevas técnicas de ciberdelincuencia en la protección de los datos personales no solo se relaciona con el aumento de las prácticas ilícitas digitales sino también con la falta de una estructura que articule prevención, intervención e investigación especializada ya que el problema no está únicamente en la existencia de las técnicas

como tales sino en la vulnerabilidad del sistema social jurídico y cultural , se destaca también que la legislación no ha evolucionado al ritmo de la tecnología y que los operadores jurídicos carecen de herramientas eficaces para detectar prevenir y sancionar estos delitos.

Ahora bien respecto al primer objetivo específico los entrevistaron señalaron que las técnicas de ciberdelincuencia más comunes son el phishing el smishing y la suplantación de identidad digital todos coincidieron en que estas técnicas están dirigidas a engañar a las víctimas mediante correos electrónicos mensajes de texto llamadas telefónicas o redes sociales donde los delincuentes simulan ser una persona de confianza o una entidad oficial con el fin de obtener datos personales y bancarios de las víctimas, también se advirtió que el acceso a estos datos muchas veces no requiere de hackeos sino simplemente de inducir al error aprovechando la falta de conocimientos digitales que tiene la mayoría de personas y sobre todo no perciben el riesgo en tiempo real ya que muchas veces entregan información privada como contraseñas números de tarjeta direcciones o códigos de verificación sin verificar la autenticidad del remitente o del enlace recibido aumentando así casos de estafa virtual ya que no requiere contacto físico ni interacción directa sino que se ejecuta por medio de manipulaciones digitales.

Esta realidad tiene concordancia con varios antecedentes que fueron insertados en la investigación por ejemplo el estudio de Aredo (2021) que indico que el phishing compromete directamente la seguridad de los datos personales debido a la falta de educación y que esta técnica se mantiene vigente precisamente porque la normativa es vaga y los usuarios no tienen herramientas para detectar el engaño de manera oportuna lo que también fue mencionado por los abogados entrevistados que muchas víctimas ni siquiera saben que han sido estafadas hasta que su cuenta ha sido vaciada o su

identidad ha sido usada para solicitar créditos; así mismo Ventura (2020) coincidió en que el smishing y el vishing aún no están regulados en el sistema penal y que esta falta de precisión normativa permite que estos actos no siempre sean sancionados lo cual confirma lo dicho por los participantes al mencionar que muchas veces la denuncia no procede; otro antecedente que guarda relación es el de Benavides (2022) quien afirmó que internet sigue siendo un entorno de alto riesgo para los datos personales ya que ni siquiera las grandes plataformas digitales ofrecen seguridad completa.

Es por ello que desde un punto de vista de la investigadora se puede interpretar que el problema no se reduce a la existencia de técnicas como el phishing o el smishing sino que va más allá e implica una desprotección en la que las normas legales no están actualizadas los órganos jurídicos no cuentan con medios tecnológicos suficientes y los ciudadanos no han sido preparados para enfrentar las amenazas del entorno digital.

Finalmente en cuanto al segundo objetivo específico los resultados describieron varias formas en que la protección de los datos personales ha sido vulnerada directamente una de las más frecuentes fue el acceso no autorizado a cuentas personales bancarias o redes sociales por medio de enlaces maliciosos que solicitaban información bajo pretextos falsos también indicaron que existe una exposición excesiva de información personal en redes abiertas sin medidas de seguridad lo que facilita que los delincuentes recopilen datos para suplantar identidades y acceder a otros espacios privados se mencionó que muchos de estos ataques aprovechan la debilidad en el manejo de contraseñas que suelen ser repetidas, predecibles o compartidas sin algún tipo de precaución, lo que claramente permite vulnerar la privacidad de forma rápida sobre todo se advirtió que las instituciones tanto públicas como privadas no han implementado protocolos efectivos para asegurar sus bases de datos.

Esta situación fue anticipada en los antecedentes revisados como el caso de Aguilar et al. (2022) que mostró cómo en Ecuador la existencia de una ley no garantiza una protección real si no se implementan medidas institucionales eficaces ni se promueve un cambio cultural respecto al uso responsable de los datos personales lo que coincide con lo indicado que muchas personas ni siquiera son conscientes de que su información ha sido vulnerada hasta que se ven afectadas; por otro lado el estudio de Castillo (2020) también concuerda con esta afirmación al destacar que la vigilancia tecnológica y la falta de regulación sobre el robo de identidad han generado un vacío que impide actuar con rapidez y eficacia frente a estas situaciones de vulneración digital y como lo detallan Álvarez y Llerena (2021) que en el contexto de la tecnología 5G se ha identificado la falta de una normativa para proteger los datos lo que resulta útil para entender que esta debilidad no es exclusiva de un sector sino que se repite en distintos ámbitos del entorno digital.

Desde mi posición como investigadora, esta realidad evidenció que no puede explicarse solo desde la existencia de leyes, sino desde la falta de voluntad y acción por parte de las instituciones que deberían garantizar su cumplimiento, un punto que me resultó preocupante que muchas víctimas no tengan siquiera conciencia de que han sido vulneradas, es por ello que entendí que no basta con reformar leyes ni con crear oficinas técnicas si no se trabaja de forma paralela en crear una cultura de protección desde la ciudadanía, donde cada persona comprenda el valor de su información.

VI. Conclusiones

PRIMERO: Se concluye que las nuevas técnicas de ciberdelincuencia implican una seria amenaza para la protección de datos personales en los delitos de estafa en Cusco, pues operan en un marco legal que no responde con eficacia a las innovaciones delictivas, que además presenta vacíos normativos que favorecen la impunidad de los infractores; de igual forma, la falta de educación digital en la ciudadanía y la limitada capacitación de funcionarios encargados de la seguridad de la información refuerzan la vulnerabilidad de las víctimas.

SEGUNDO: Del análisis se identificó que las técnicas más recurrentes de ciberdelincuencia en el contexto de los delitos de estafa fueron el phishing, el smishing y la suplantación de identidad digital, modalidades que se materializan en correos electrónicos falsos, mensajes engañosos, perfiles clonados así como llamadas fraudulentas; dichas técnicas afectan directamente la seguridad de los datos personales ya que gran parte de la población no reconoce estos riesgos ni adopta medidas de protección, lo que facilita a los ciberdelincuentes el acceso a información privada de gran valor.

TERCERO: Respecto a las vulneraciones directas, se evidenció que estas se producen principalmente por el uso de contraseñas débiles o repetidas, la exposición pública de información personal en entornos digitales inseguros así como la carencia de protocolos de seguridad en instituciones que manejan bases de datos sensibles; permiten a los delincuentes ingresar sin dificultad a cuentas personales, bancarias o redes sociales, consolidando su actividad ilícita sin que existan mecanismos institucionales efectivos de detección o de respuesta temprana.

VII. Recomendaciones

PRIMERA: Se recomienda al Congreso de la República aprobar una reforma integral del Código Penal que tipifique de manera específica las nuevas técnicas de ciberdelincuencia y que además incorpore mecanismos de actualización normativa continua, de modo que el sistema legal pueda adaptarse con rapidez a la evolución tecnológica.

SEGUNDA: Se recomienda a la Secretaría de Gobierno y Transformación Digital y a los Gobiernos Regionales del país promover campañas masivas de educación digital en escuelas, universidades y medios de comunicación que instruyan a la población en la identificación de señales de fraude como correos sospechosos, enlaces maliciosos o perfiles clonados, ya que únicamente con ello la ciudadanía podrá reconocer y rechazar de inmediato estas técnicas.

TERCERA: Se recomienda a las instituciones públicas y privadas que gestionan información personal implementar obligatoriamente sistemas de seguridad digital avanzados que integren de manera simultánea mecanismos de verificación en dos pasos, reconocimiento facial biométrico, preguntas de seguridad y detección automática de accesos inusuales; dichos sistemas deberán estar conectados a una base de datos centralizada capaz de emitir alertas en tiempo real a la Policía Nacional del Perú y a las entidades competentes para que activen protocolos inmediatos de intervención.

VIII. Referencias

Acurio, S. (2016). *Delitos informaticos.* https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Aguilar, M., Gordillo, D., León, G., & Paredes, J. (2022). *La protección de datos personales en Ecuador*. Repositorio Institucional de la Universidad Regional Autonoma de los Andes Ecuador: https://revistas.uh.cu/revflacso/article/view/3594

Alvarez, C., & Llerena, K. (2021). *Alcances jurídicos de la legislación nacional e internacional sobre protección de datos personales en la implementación de la tecnología 5G.* Repositorio Institucional de la Universidad Catolica San Pablo: https://repositorio.ucsp.edu.pe/backend/api/core/bitstreams/b1878ce9-1112-4e09-a8bc-40ee337e311a/content

Aredo, L. (2021). *El phishing y su vulneración a la protección de datos personales en los delitos informáticos.* Repositorio Institucional de la Universidad Cesar Vallejo: https://repositorio.ucv.edu.pe/handle/20.500.12692/80920

Benavides, D. (2022). *Situación actual de la protección de datos personales.* Repositorio Institcional de la Universidad Militar Nueva Granada Bogota: http://hdl.handle.net/10654/44003

Bernal, C. (2016). *Metodología de la investigación (4.a ed.).* Pearson.

Bujosa, L., & Del Pozo, M. (2022). *Diliigencias de investigacion tecnologicas para la lucha contra la ciberdelincuencia.* Repositorio Institucional de la Universidad de Salamanca: http://hdl.handle.net/10366/149611

Campus Internacional de la Ciberseguridad. (2024). *Phishing: Cómo los Hackers roban tu información personal.* https://www.campusciberseguridad.com/blog/item/177-phishing-como-hackers-roban-tu-informacion-personal

Castillo, J. (2020). *Ciberseguridad y vigilancia tecnológica: un reto para la protección de datos personales en los archivos.* Repositorio Institucional de la Universidad Autonoma de San Luis Potosi: https://dialnet.unirioja.es/servlet/articulo?codigo=7295555

Codigo Penal Peruano. (1991).

Comision Europea. (2022). *Reglamento general de protección de datos*. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

Comision Europea. (2024). *¿Qué son los datos personales?* https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_es

Congreso de la Republica. (2011). *Ley 29733.* Ley de proteccion de datos personales: https://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

Congreso de la Republica del Perú. (2011). *Ley N° 29733.* Ley de proteccion de datos personales: https://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf

Congreso de la Republica del Perú. (2013). *Ley N° 30096.* Ley de Delitos Informaticos y sus modificatorias: https://www.gob.pe/institucion/mpfn/informes-publicaciones/1678028-ley-n-30096

Consejo de la Union Europea. (2024). *Protección de datos en la UE.* https://www.consilium.europa.eu/es/policies/data-protection/#:~:text=El%20art%C3%ADculo%208%20de%20la,conciernan%20y%20a%20obtener%20su%20rectificaci%C3%B3n.

Contraloria General de la Republica. (2022). *Auditoria de cumplimiento.* Compendio Informativo: https://cdn.www.gob.pe/uploads/document/file/3902383/Compendio%20Normativo%20-%20Auditor%C3%ADa%20de%20Cumplimiento.pdf.pdf?v=1670013304

Cotrina, R. (2020). *El espionaje corporativo y su incidencia.* https://repositorio.upn.edu.pe/bitstream/handle/11537/26127/Cotrina%20Roldan%2C%20Roy%20Eduardo.pdf?sequence=11&isAllowed=y

Defensoria del Pueblo. (2019). *Manual de proteccion de datos personales.* https://www.defensoria.gob.pe/wp-content/uploads/2019/11/Manual-de-Protecci%C3%B3n-de-Datos-Personales.pdf

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

Derechos Humanos Naciones Unidas. (1948). *Pacto Internacional de Derechos Económicos, Sociales y Culturales.* https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights

Fuentes, E. (2022). *El derecho fundamental a la protección de datos personales en Argentina y en el mundo: Los conflictos extraterritoriales por los delitos*

informáticos. Repositorio Institucional de la Universidad de San Andres Argentina: https://repositorio.udesa.edu.ar/jspui/bitstream/10908/22383/1/%5bP%5d%5bW%5d%20T.%20Ab.%20Fuentes%20Ben%c3%adtez%2c%20Estanislao.pdf

Gallardo, E. (2021). *Metodología de investigación.* Universidad Continental: https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_U

Garcia, J., & Pilco, G. (2024). *El derecho a la propiedad privada y nuevas modalidades de delitos cibernéticos.* http://dspace.unach.edu.ec/bitstream/51000/13485/1/Garc%C3%ADa%20Andrade%2C%20J%20y%20Pilco%20Guam%C3%A1n%2C%20%20G%20%282024%29%20El%20derecho%20a%20la%20propiedad%20privada%20y%20nuevas%20modalidades%20de%20delitos%20cibern%C3%A9ticos%20en%20la%20legisl

Gobierno de Perú. (2023). *Transformacion digital en el Perú.* https://cdn.www.gob.pe/uploads/document/file/5430989/4852446-tema-4-seguridad-y-confianza-digitallogro-de-aprendizaje-cuaderno-de-estudio.pdf?v=1700150364

Haro, F. (2021). *Acoso y ciberacoso como fen´omeno delictivo.* https://iescelia.org/ojs

Hernandez Sampieri, R., & Mendoza, C. (2023). *Metodologia de la Investigacion- Las rutas cuantitativa, cualitativa y mixta* (Vol. segunda edición). Mexico: Mc graw Hill.

Herrera, P. (2020). *Las empresas deben proteger los datos de los trabajadores.* Diario Oficial el Peruano: https://elperuano.pe/noticia/105549-las-empresas-deben-proteger-los-datos-de-los-trabajadores

Ley De Protección De Datos Personales. (2024). *Decreto Supremo N.° 016-2024-JUS.* https://www.gob.pe/institucion/smv/normas-legales/6426760-016-2024-jus

Ministeri de Justicia y Derechos Humanos. (2022). *Ciberdelincuencia.* Reporte de informacion estadistica y recomendaciones para la prevenció: https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf?v=1661790352

Monje, R. (2017). *Seguridad informatica y el malware.* https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2641/00004128.pdf

Nieves, M. (2012). *The right to privacy: la génesis de la protección de la privacidad en el sistema constitucional norteamericano, el centenario legado de Warren y Brandeis.* https://doi.org/10.5944/rdp.85.2012.10723

Ñaupas, H. V. (2018). *Metodología de la investigación Cuantitativa – Cualitativa y Redacción de la tesis.* Mexico: 5ta edicion de la U Bogota.

Oficina de las Naciones Unidas contra a Droga y el Delito. (2023). *Ciberdelincuencia.* https://www.unodc.org/e4j/es/tertiary/cybercrime.html

Oficina de las Naciones Unidas contra la droga y el delito. (2022). *Tipos generales. Marco jurídico y derechos humanos.* https://cdn.www.gob.pe/uploads/document/file/2941907/CYBERDELITO%20VOL%201%2017x24_compressed.pdf.pdf

Ollmann, G. (2007). *The vishing guide.* https://nsi.org/ReferenceLibrary/599.pdf

Organismo Supervisor de la Inversión Privada en Telecomunicaciones . (2022). *Informe de evaluacion de resultados del PEI 2020-2023.*

https://www.osiptel.gob.pe/media/xkua1d2j/informe-eval-resultados-pei-2020.pdf

Petronio, S., & Hernandez , R. (2019). *Teoría de la gestión de la privacidad de las comunicaciones*. Oxford University Press: https://oxfordre.com/communication/communication/view/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-373

Rahman, L., Timko, D., Wali, H., & Neupane, A. (2023). *Los usuarios realmente responden al smishing.* https://dl.acm.org/doi/abs/10.1145/3577923.3583640

Saluja, S., Agarwal, A., & Mittal, A. (2021). *Entendiendo las teorías del fraude y avanzando con el modelo de integridad*. https://www.emerald.com/insight/content/doi/10.1108/JFC-07-2021-0163/full/html

Sanchez, G., & Rojas, I. (2022). *Leyes de proteccion de datos personales en el mundo.* https://revista.seguridad.unam.mx/print/2124

Serie de Tratados Europeos. (2001). *Covenio sobre la Ciberdelincuencia.* Budapest: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Serrano, M. (2023). *La protección de los datos personales en defensa de la dignidad individual ante los riesgos de pérdida de privacidad.* Derechos digitales en Iberoamérica: https://protecciondata.es/wp-content/uploads/2023/02/aqui-2.pdf#page=9

Tobar, J. (2022). *Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse.* http://dspace.utb.edu.ec/handle/49000/13062

Urdanegui, A. (2023). *Los delitos informaticos y la vulneracion del derecho fundamental de proteccion de datos personales en Lima Metropolitana.* Repositorio Institucional de la Universidad Autónoma del Perú: https://repositorio.autonoma.edu.pe/bitstream/handle/20.500.13067/2999/Urdanegui%20Rangel%2c%20Anabeliza.pdf?sequence=1&isAllowed=y

Ventura, M. (2020). *La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima.* Repositorio Institucional de la Universidad Privada del Norte: https://repositorio.upn.edu.pe/handle/11537/28942

Villar, J. (2024). *Tráfico ilegal de datos: necesidad de reforma del Código Penal peruano.* Repositorio Institucional de la Universidad Continental : https://hdl.handle.net/20.500.12394/14477

Los anexos, panel fotográfico y otros documentos están resguardados en la oficina del repositorio digital institucional en la Biblioteca Central de la Universidad Tecnológica de los Andes