Universidad Católica de Santa María

Facultad de Ciencias Jurídicas y Políticas

Escuela Profesional de Derecho

Desafíos jurídicos de la ciberseguridad en el sistema financiero peruano y su impacto en el derecho a la privacidad del consumidor 2025

Tesis presentada por:

Vargas Benavente, Marcelo Renato

ORCID: 0009-0007-0320-6775

Carpio Martinez, Enrique Marcelo

ORCID: 0009-0005-2962-3265

para optar el Título Profesional de Abogado

Asesor:

Mg. Veliz Vizcardo, Giancarlo Christian

ORCID: 0009-0005-8910-0394

Arequipa - Perú

2026

UCSM-ERP

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

DERECHO

TITULACIÓN CON TESIS

DICTAMEN APROBACIÓN DE BORRADOR

Arequipa, 27 de Mayo del 2026

Dictamen: 014430-C-EPDD-2026

Visto el borrador del expediente 014430, presentado por:

2018600981 - VARGAS BENAVENTE MARCELO RENATO
2018201211 - CARPIO MARTINEZ ENRIQUE MARCELO

Titulado:

DESAFÍOS JURÍDICOS DE LA CIBERSEGURIDAD EN EL SISTEMA FINANCIERO PERUANO Y SU IMPACTO EN EL DERECHO A LA PRIVACIDAD DEL CONSUMIDOR 2025

Nuestro dictamen es:

APROBADO

Titulo Profesional/Titulo de Segunda Especialidad/Grado Académico a optar:

ABOGADO

29539317 - RODRIGUEZ MARTINEZ CARLOS ALBERTO ALFONSO
DICTAMINADOR

29426306 - NEYRA AMAT CARLOS ALBERTO
DICTAMINADOR

73079095 - NAJAR BECERRA CESAR ALEJANDRO
DICTAMINADOR

Desafíos jurídicos de la ciberseguridad en el sistema financiero peruano y su impacto en el dere privacidad del consumidor 2025

INFORME DE ORIGINALIDAD

8%	10%	6%	2%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUD

FUENTES PRIMARIAS

1	www.informatica-juridica.com	Fuente de Internet
2	hdl.handle.net	Fuente de Internet
3	vlex.com.pe	Fuente de Internet
4	www.indecopi.gob.pe	Fuente de Internet
5	hraei.gob.mx	Fuente de Internet
6	docslib.org	Fuente de Internet

Excluir citas	Apagado	Excluir coincidencias	< 1%
Excluir bibliografía	Apagado		

DEDICATORIA

Dedico esta tesis a mi padre, quien desde un principio me indicó el norte, a mi madre quien me enseñó que las cosas se hacen y terminan bien, y finalmente quiero dedicarla a mí mismo, por haber completado esta preciosa carrera profesional.

Marcelo Carpio.

A mi padre, quien fue siempre mi inspiración y la meta a superar en el camino profesional, por enseñarme con su ejemplo el valor del esfuerzo y la perseverancia. A la vida, por brindarme las oportunidades que hicieron posible este logro, y que me impulsan a seguir creciendo con gratitud y esperanza

Marcelo Vargas.

AGRADECIMIENTOS

Agradezco a la Universidad Católica de Santa María por otorgarme la formación académica y el espacio para desarrollarme a nivel profesional. A mi asesor, Dr. César Alejandro Nájar Becerra, por su orientación precisa. Y, especialmente, a mi familia, por su paciencia y apoyo constante durante este proceso.

Marcelo Carpio.

A Dios, por darme la fortaleza y la guía en este camino. A mi familia, por su apoyo incondicional en todas mis decisiones y el aliento constante. A mi compañero de primer año, por su amistad y respaldo en los inicios de esta etapa. Y a los docentes de la Universidad Católica de Santa María, por su enseñanza y dedicación que contribuyeron a mi formación profesional. A todos, mi sincera gratitud por acompañarme en la elaboración de este importante documento, que marca el inicio de nuestra vida profesional.

Marcelo Vargas.

RESUMEN

La presente investigación aborda el problema jurídico relacionado con la deficiencia del marco normativo de ciberseguridad en el sistema financiero peruano y su incidencia en la tutela del derecho a la privacidad del consumidor, en un contexto de creciente digitalización de los servicios financieros. En ese sentido, el objetivo general fue evaluar los desafíos jurídicos de la ciberseguridad en el sistema financiero peruano y determinar su impacto en la protección del derecho a la privacidad del consumidor al año 2025. La investigación adoptó un enfoque mixto, con predominio del método jurídico-dogmático, complementado con técnicas de análisis documental y recolección de percepciones a través de encuestas.

Entre los principales hallazgos, se identificó que, si bien la Ley N.º 29733 y su normativa conexa establecen un marco general de protección de datos personales, presentan limitaciones en su aplicación frente a los riesgos derivados de entornos digitales complejos, lo que evidencia brechas en la tutela efectiva del derecho a la privacidad. Asimismo, se determinó que existe una significativa asimetría en el conocimiento y prácticas de los consumidores respecto a la protección de su información personal, lo que incrementa su vulnerabilidad en el uso de servicios financieros digitales. En conclusión, la investigación evidencia que las deficiencias del marco normativo vigente, junto con factores asociados al comportamiento y conocimiento del consumidor, inciden de manera directa en la protección insuficiente del derecho a la privacidad en el sistema financiero peruano.

Palabras clave: Ciberseguridad, Sistema Financiero Peruano, derecho a la privacidad

ABSTRACT

This research addresses the legal problem related to the deficiencies in the cybersecurity regulatory framework of the Peruvian financial system and its impact on the protection of consumers' right to privacy, within a context of increasing digitalization of financial services. In this regard, the overall objective was to evaluate the legal challenges of cybersecurity in the Peruvian financial system and determine their impact on the protection of consumers' right to privacy by 2025. The research adopted a mixed-methods approach, primarily using the legal-dogmatic method, complemented by documentary analysis techniques and the collection of perceptions through surveys.

Among the main findings, it was identified that, while Law No. 29733 and its related regulations establish a general framework for the protection of personal data, they present limitations in their application to the risks arising from complex digital environments, thus revealing gaps in the effective protection of the right to privacy. Furthermore, it was determined that there is a significant asymmetry in consumers' knowledge and practices regarding the protection of their personal information, which increases their vulnerability when using digital financial services. In conclusion, the research demonstrates that deficiencies in the current regulatory framework, along with factors related to consumer behavior and knowledge, directly impact the insufficient protection of the right to privacy within the Peruvian financial system.

Keywords: Cybersecurity, Peruvian Financial System, right to privacy

ÍNDICE

DEDICATORIA
AGRADECIMIENTOS
RESUMEN
ABSTRACT
INTRODUCCIÓN 1
CAPÍTULO I 3
PLANTEAMIENTO DEL PROBLEMA 4
1.1. Descripción del problema 4
1.2. Objetivos 7
1.2.1. Objetivo general 7
1.2.2. Objetivos específicos 7
CAPÍTULO II 8
MARCO TEÓRICO 9
2.1. Estado del arte 9
2.1.1. Antecedentes locales 9
2.1.2. Antecedentes nacionales 9
2.1.3. Antecedentes internacionales 11
2.2. La Ciberseguridad 12
2.2.1. Concepto de ciberseguridad 12
2.2.2. Alcances sobre las normativas vigentes. 15
2.2.3. Auditorías Algorítmicas Independientes 19
2.3. Datos personales 22
2.3.1. Concepto y como los datos personales son importantes 22
2.3.2. ¿Por qué la vulneración de datos es un tema importante a tratar? 23
2.3.3. Manejo de datos por parte del sistema financiero 23
2.3.4. Inteligencia artificial y su impacto en el derecho 24
2.4. Los derechos del Consumidor en el sistema financiero peruano 25
2.4.1. Cómo es que se protegen los derechos de los consumidores. 29
2.4.2. Falta de conocimiento de los consumidores sobre sus derechos. 29
2.4.3. El papel del consumidor en la protección de su propia información. 30
2.4.4. Derecho al olvido 32

2.4.5. Medidas que promuevan la responsabilidad e información. 33
2.4.6. Requisitos y procedimiento para cautelar el derecho del consumidor. 35
2.5. Sistema Financiero Peruano 36
2.5.1. Alcances de la normativa vigente. 36
2.5.2. Cómo es que el sistema financiero digital se va actualizando 37
2.5.3. Medidas para solucionar los vacíos o problemas encontrados. 38
2.6. Derecho comparado 39
2.6.1. Estados unidos 39
2.6.2. Unión europea 40
2.6.3. Latinoamérica 41
2.7. Marco Legal 42
CAPÍTULO III 46
MARCO METODOLÓGICO 47
3.1. Enfoque 47
3.2. Nivel 47
3.3. Método 48
3.4. Unidades de estudio 48
3.5. Técnicas 49
3.6. Instrumentos 49
CAPÍTULO IV 51
RESULTADOS 52
4.1. Evidencia comparativa, normativa y empírica 52
4.1.1. Jurisprudencia 52
4.1.2. Doctrina 56
4.1.3. Resultado de consumidores 60
4.1.4. Resultado de profesionales 67
4.2. Efectividad de la Ley N.º 29733 y normativas vigentes 82
4.2.1. Evaluación normativa y alcance de la Ley N.º 29733 y su Reglamento 82
4.2.2. Análisis de las normas complementarias y su coherencia 86
4.3. Responsabilidad del consumidor en la protección de su información 90
4.3.1. Nivel de conocimiento y prácticas del consumidor 92
4.3.2. Estrategias de fortalecimiento del rol del consumidor y cultura digital 94
4.4. Debilidades estructurales y amenazas cibernéticas en el sistema 97
4.4.1. Principales vulnerabilidades del sistema financiero digital peruano 97

4.4.2. Consecuencias jurídicas de las vulneraciones a la privacidad 99
4.5 Comparación del marco regulatorio peruano con legislaciones extranjeras 101
4.5.1 Modelos comparados: Unión Europea (RGPD), Estados Unidos 101
4.5.2 Evaluación de la aplicabilidad del derecho comparado al contexto 103
4.6. Propuesta de Ente Supervisor 110
4.6.1. Fundamentación jurídica de la propuesta 110
4.6.2. Configuración del régimen de responsabilidad reforzada 113
CONCLUSIONES 122
RECOMENDACIONES 124
REFERENCIAS BIBLIOGRÁFICAS 127

ÍNDICE DE FIGURAS

Figura 1 ¿Crees que los bancos y financieras deberían proteger tus datos personales?……60

Figura 2 ¿Alguna vez has leído los términos y condiciones al usar una aplicación bancaria?.....61

Figura 3 ¿Sientes que tu información está segura cuando haces operaciones por internet en el banco?.....62

Figura 4 ¿Sabías que existe una ley en Perú que protege tus datos personales?.....63

Figura 5 ¿Qué harías si una empresa bancaria usa mal tu información personal?.....64

Figura 6 ¿Sabes qué es la ciberseguridad?.....65

Figura 7 ¿Sabes que puedes pedir al banco que te diga qué datos tiene sobre ti?.....66

Figura 8 ¿Cuántos años de experiencia tiene en su sector?.....69

Figura 9 ¿Cuál considera que es el principal riesgo cibernético en el sistema financiero peruano?.....70

Figura 10 ¿Cree que las entidades financieras peruanas cuentan con protocolos de ciberseguridad suficientes para proteger los datos de sus clientes?.....71

Figura 11 ¿Qué tan preparado considera al sistema financiero peruano para responder ante un ciberataque masivo?.....72

Figura 12 ¿La legislación peruana actual es suficiente para enfrentar los desafíos de ciberseguridad en el sistema financiero?.....73

Figura 13 ¿Qué tan efectiva considera la supervisión de la SBS en la protección de la privacidad del consumidor ante incidentes de ciberseguridad?.....75

Figura 14 ¿Las medidas de ciberseguridad implementadas por las entidades financieras respetan plenamente la privacidad del consumidor?.....76

Figura 15 ¿Los consumidores son informados de manera clara cuando ocurre una vulneración de sus datos personales?.....77

Figura 16 ¿Qué tan vulnerable considera el derecho a la privacidad del consumidor frente a amenazas cibernéticas en el Perú?.....78

Figura 17 ¿Qué medidas son más urgentes para fortalecer la ciberseguridad en el sistema financiero peruano?.....79

Figura 18 ¿Debería existir una obligación legal de notificación inmediata a los usuarios tras incidentes de ciberseguridad que afectan sus datos?.....80

Figura 19 ¿Qué tan prioritario considera que es para el Estado fortalecer la ciberseguridad para proteger la privacidad del consumidor?.....81

Figura 20 ¿Cuál considera que es el principal desafío jurídico en la protección de datos personales en el sistema financiero peruano?.....82

Figura 21 ¿Cuál considera que es el principal desafío jurídico en la protección de datos personales en el sistema financiero peruano?.....84

ÍNDICE DE TABLAS

Tabla 1 ¿Sabes que es un dato personal?.....59

Tabla 2 ¿Crees que los bancos y financieras deberían proteger tus datos personales?.....59

Tabla 3 ¿Alguna vez has leído los términos y condiciones al usar una aplicación bancaria?.60

Tabla 4 ¿Sientes que tu información está segura cuando haces operaciones por internet en el banco?.....61

Tabla 5 ¿Sabías que existe una ley en Perú que protege tus datos personales?.....62

Tabla 6 ¿Qué harías si una empresa bancaria usa mal tu información personal?.....63

Tabla 7 ¿Sabes qué es la ciberseguridad?.....64

Tabla 8 ¿Sabes que puedes pedir al banco que te diga qué datos tiene sobre ti?.....65

Tabla 9 ¿Ha tenido alguna vez un problema con un banco por mal uso de su información?..67

Tabla 10 ¿Te gustaría recibir más información por parte del Estado o empresas del sistema financiero sobre cómo proteger tus datos?.....68

Tabla 11 ¿Cuántos años de experiencia tiene en su sector?.....68

Tabla 12 ¿Cuál considera que es el principal riesgo cibernético en el sistema financiero peruano?.....70

Tabla 13 ¿Cree que las entidades financieras peruanas cuentan con protocolos de ciberseguridad suficientes para proteger los datos de sus clientes?.....71

Tabla 14 ¿Qué tan preparado considera al sistema financiero peruano para responder ante un ciberataque masivo?.....72

Tabla 15 ¿La legislación peruana actual es suficiente para enfrentar los desafíos de ciberseguridad en el sistema financiero?.....73

Tabla 16 ¿Qué normativa considera más relevante en la protección de los datos frente a ciberataques?.....74

Tabla 17 ¿Qué tan efectiva considera la supervisión de la SBS en la protección de la privacidad del consumidor ante incidentes de ciberseguridad?.....75

Tabla 18 ¿Las medidas de ciberseguridad implementadas por las entidades financieras respetan plenamente la privacidad del consumidor?.....76

Tabla 19 ¿Los consumidores son informados de manera clara cuando ocurre una vulneración de sus datos personales?.....77

Tabla 20 ¿Qué tan vulnerable considera el derecho a la privacidad del consumidor frente a amenazas cibernéticas en el Perú?.....78

Tabla 21 ¿Qué medidas son más urgentes para fortalecer la ciberseguridad en el sistema financiero peruano?.....79

Tabla 22 ¿Debería existir una obligación legal de notificación inmediata a los usuarios tras incidentes de ciberseguridad que afectan sus datos?.....80

Tabla 23 ¿Qué tan prioritario considera que es para el Estado fortalecer la ciberseguridad para proteger la privacidad del consumidor?.....81

Tabla 24 ¿Cuál considera que es el principal desafío jurídico en la protección de datos personales en el sistema financiero peruano?.....82

Tabla 25 ¿Qué normativa considera más relevante en la protección de los datos frente a ciberataques?.....83

INTRODUCCIÓN

La presente investigación se desarrolló en el contexto del sistema financiero peruano, el mismo que atravesó dentro de los últimos años un proceso de digitalización, específicamente en la masificación de servicios por internet y la adopción de nuevas tecnologías, todo ello generando beneficios múltiples como la rapidez, accesibilidad y amplia competitividad, así mismo se presentaron los diversos riesgos que cada vez más complejos vinculados con los temas principales de la presente investigación, la ciberseguridad y la vulneración de datos personales de los consumidores, afectando el derecho fundamental a la privacidad.

Por lo que, dentro de este contexto, resultó indispensable evaluar el nivel de utilidad del marco normativo vigente y analizar cómo esta problemática afectó o limitó la capacidad de las instituciones financieras privadas y públicas en garantizar una protección adecuada frente a las amenazas digitales que cada vez se van evolucionando y poniendo en tela de juicio si es que realmente estaba preparada la norma para las futuras eventualidades. Esta investigación se propuso, realizar un análisis jurídico, doctrinal y empírico de los desafíos que surgen dentro de la relación de la ciberseguridad, la protección de datos personales y los derechos del consumidor, con el propósito de aportar soluciones y/o recomendaciones prácticas que contribuyeran a fortalecer la seguridad jurídica y la confianza en el sistema financiero.

En el Capítulo I se expuso el planteamiento del problema, los objetivos de la investigación y la justificación que sustenta la relevancia académica, social y profesional. En el Capítulo II se desarrolló el marco teórico, donde se abordó los conceptos fundamentales y normativos sobre la ciberseguridad, la protección de datos personales, la inteligencia artificial y los derechos del consumidor, todo ello con un análisis de derecho comparado internacional. En el Capítulo III se explicó la metodología, la misma que fue de carácter mixto con un diseño que integró los enfoques cualitativos y cuantitativos para así obtener una visión integral del presente problema. En el Capítulo IV se abordaron los resultados derivados del análisis doctrinal, casos y estadística, lo que permitió acreditar la falta de cumplimiento de la normativa vigente y la necesidad urgente de modernizar los mecanismos de tutela. Pasando a la última sección, donde se formularon las conclusiones que recopilaron los hallazgos relevantes encontrados durante la investigación sobre aplicación de la Ley de Protección de Datos Personales y las disposiciones anexadas en el

sistema financiero peruano y se desarrollaron y propusieron las recomendaciones orientadas con el fin de modernizar el marco jurídico vigente, a reforzar las políticas públicas y promover una cultura de responsabilidad entre el consumidor y las instituciones financieras, para así garantizar un entorno digital competente, seguro y respetuoso de los derechos fundamentales.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1.Descripción del problema

En el Perú, según lo comentado por la Presidencia del Consejo de Ministros (2024) hace más de 20 años, a través de la transformación digital, aparecieron nuevas tecnologías disruptivas que obligaron al Estado a replantear muchas ideas en cuanto a que es necesario un cambio organizado y cultural para poder maximizar todas las oportunidades del mundo digital.

La ciberseguridad cumple un rol determinante en la política internacional del siglo XXI, con impactos significativos en torno a la seguridad nacional, por su influencia en la sociedad, desde su masificación hasta su normalidad en la cotidianeidad, como menciona Aguilar (2021) su importancia recae en que un sector considerable tiene acceso a internet, sin embargo, muchos usuarios de estos servicios no poseen un conocimiento pleno de cómo funciona la ciberseguridad y la relevancia de la misma.

Considerando lo mencionado por Infobae (2025) el Perú espera un aumento significativo de ciberataques en diferentes sectores, los cuales deberán de reforzar su seguridad informática ante amenazas que podrían comprometer datos sensibles y generar millonarias pérdidas económicas ante el incremento de sofisticación de ataques y el mal uso de la Inteligencia Artificial. Asimismo sobre la falta de cumplimiento de las empresas del sistema financiero en cuanto a la protección de datos personales, según un estudio de la Superintendencia de Banca, Seguros y AFP (2020) y el estudio de privacidad global (2020) de la fundación de datos protegidos, dan a conocer que no se implementa la Ley N° 29733 de manera efectiva, ley que regula la protección de datos personales, y teniendo en cuenta que según Alvarado (2016) la seguridad de la información es un principio fundamental establecido en la Ley de Protección de Datos Personales (LPDP), y como tal, constituye una responsabilidad tanto para los titulares como para los encargados de los bancos de datos personales. Esto implica que todas las partes involucradas en el tratamiento de datos personales tienen la obligación de garantizar su protección y asegurar su manejo adecuado.

Para Chavez (2022) entre 2018 y septiembre de 2022, algunas de las entidades financieras con mayor cantidad de sanciones incluyen el Banco de Crédito del Perú, Interbank, Scotiabank, BBVA y el Banco Falabella, registrando de esta manera por la Superintendencia de Banca, Seguros y AFP un total de 22,214 denuncias sobre

vulneración de datos personales. Uno de aquellos casos de vulneración de dichas normas, tal como lo expone Paucar (2024) es sobre la filtración del Banco Interbank que involucró la exposición de información personal como nombres completos, números de tarjetas, teléfonos, fechas de nacimiento, números de identificación y detalles sobre transacciones financieras, asimismo según la Autoridad Nacional de Protección de Datos Personales (2020) mediante Resolución Directoral 2196-2020 sancionó al banco BBVA Perú al incumplir las disposiciones de la Ley de protección de datos personales, y considerando lo mencionado por CapitalOne (2022) sufrieron una filtración masiva de datos personales que expuso información personal y financiera de más de 100 millones de personas de EE. UU. y Canadá.

Con lo anterior expuesto se evidencia no solo de manera nacional, sino de manera internacional, que los temas de cumplimiento de las leyes de protección de datos personales y ciberseguridad son de suma importancia y en el caso peruano se necesita una urgente actualización, fortalecimiento de la normativa en cuanto a proteger los datos personales y una adecuada ciberseguridad para que de esta manera se den estrategias para su correcto cumplimiento no solo por parte de la entidad financiera, sino también por parte del consumidor y que este último actúe de manera diligente.

Teniendo en cuenta que como lo menciona Equipo Grou (2019) cada vez son más las entidades financieras que deciden hacer fuertes inversiones en sus productos para digitalizarlos, y con esta medida lograr servicios más integrales y dar una experiencia competitiva en el mercado. Dichos avances digitales, si bien han mejorado el acceso a sus productos y servicios permitiendo que los consumidores realicen transacciones rápidas, seguras y de fácil entendimiento, estos conllevan desafíos jurídicos en cuanto a evitar que los delitos informáticos se den a través de fallas de ciberseguridad.

Por lo que considerando lo mencionado por Eguiguren (2015) el reconocimiento de la protección de los datos personales como un derecho fundamental es un fenómeno relativamente reciente tanto a nivel nacional como comparado; la regulación y protección de estos datos resulta esencial para asegurar que las personas puedan ejercer un mayor control y autonomía sobre su información personal, la cual a menudo es registrada, organizada y transmitida sin su consentimiento.

Queda en evidencia qué quienes se ven principalmente afectados son los consumidores, puesto que como resalta Riega Viru et al., (2021) el cambio genera problemas, las

constantes amenazas al sistema financiero hacen que este tenga que estar en un estado de constante actualización y promoción de las mismas para la seguridad de los consumidores, quienes, no siempre pueden seguirle el paso a las nuevas tecnologías, no todos los consumidores cuentan con el mismo acceso a internet o a los mismos servicios de estas entidades financieras; si bien el Estado Peruano a través de la ley N° 30618, aprobada mediante el Congreso de la República (2017) da una definición sobre seguridad digital y se tiene un marco normativo donde se encuentran los delitos cibernéticos, no existe una estrategia nacional de ciberseguridad que esté lo suficientemente preparada para combatir estos delitos, mucho menos en la posibilidad de tutelarlos de manera efectiva, lo cual evidencia la relevancia de esta investigación y por qué debe ser una prioridad.

Es atribuible a la figura del legislador del Código de Protección y Defensa del Consumidor, dos supuestos, como resalta Flores (2021) el primero siendo que el legislador no consideró mayor especificidad permitiendo que se apliquen las normas generales o bien, el segundo supuesto, que el auge tecnológico no fue previsible a corto y mediano plazo; en ambos supuestos lo que persiste es la urgencia de tener una normativa más vigente para lograr una vasta protección al consumidor. La confianza que se crea entre el consumidor y una entidad del sistema financiero es sumamente importante, es entregar como consumidor parte de los bienes más apreciados como lo son el dinero y el tiempo, confiando en que estas entidades brindarán seguridad a largo plazo, sin embargo, cuando esta confianza se rompe, y no hay una legislación contundente para actuar, tanto consumidor como la entidad quedan completamente desprotegidos y vulnerables.

En el contexto peruano, surge la necesidad de determinar si el marco normativo vigente en materia de protección de datos personales y ciberseguridad resulta idóneo para garantizar de manera efectiva el derecho fundamental a la privacidad del consumidor en el sistema financiero digital. Si bien la Ley N.º 29733 y las regulaciones emitidas por la Superintendencia de Banca, Seguros y AFP establecen obligaciones relativas al tratamiento de datos personales, medidas de seguridad y responsabilidades de las entidades financieras, se advierte una posible tensión entre el alcance de dichas disposiciones y los riesgos emergentes derivados del uso intensivo de tecnologías digitales en el sector financiero. En particular, se identifican vacíos y limitaciones en aspectos como la gestión de incidentes de ciberseguridad, los deberes de información frente a vulneraciones de datos, la supervisión de proveedores tecnológicos y la respuesta jurídica frente a nuevas

modalidades de fraude digital, lo que podría generar una protección insuficiente del derecho a la privacidad del consumidor. En ese sentido, el problema jurídico se concreta en determinar en qué medida las limitaciones del marco normativo vigente en ciberseguridad inciden en la tutela efectiva del derecho a la privacidad del consumidor en el sistema financiero peruano al año 2025.

1.2. Objetivos

1.2.1. Objetivo general

Evaluar los desafíos jurídicos de la ciberseguridad en el Sistema Financiero Peruano y su impacto en el derecho a la privacidad del consumidor en Perú al 2025.

1.2.2. Objetivos específicos

- Evaluar la efectividad de la Ley N° 29733 y otras normativas vigentes en el Perú respecto a la protección de datos personales y la ciberseguridad en el ámbito financiero.
- Analizar el papel del consumidor en la protección de su propia información personal, y proponer medidas que promuevan su responsabilidad y formación en el uso seguro de servicios financieros digitales.
- Examinar las principales debilidades en seguridad y las amenazas cibernéticas que afectan al sistema financiero peruano, evaluando su impacto en la privacidad de los usuarios.
- Comparar el marco regulatorio peruano con las legislaciones de otros países que han demostrado mejores resultados en cuanto a la protección de datos y la ciberseguridad en el sector financiero.
- Evaluar la creación de un ente rector especializado en ciberseguridad y protección de datos del sistema financiero que centralice competencias, ejerza potestad sancionadora efectiva y garantice al consumidor un referente institucional claro ante vulneraciones a su privacidad en el entorno financiero digital.

CAPÍTULO II

MARCO TEÓRICO

2.1. Estado del arte

2.1.1. Antecedentes locales

En el artículo de investigación propuesto por García y Perea (2020) se expresa el problema de la tensión entre el derecho al olvido y la libertad de expresión, la metodología empleada es de investigación a través de la argumentación jurídica cuyo objetivo principal es escudriñar el contenido tanto del derecho a la libertad de expresión como al de la privacidad, así como proyectar los desafíos para la adecuación y evitar una posible afectación a la libertad de expresión al tutelar el derecho a la privacidad, y como parte de los resultados obtenidos se destaca que el tratamiento de información está comenzado a regularse en nuestra localidad, concluyendo finalmente que existe una incipiente flaqueza en la vida privada de los ciudadanos, el valor de esta investigación reside en el reconocimiento de un problema medianamente reciente y la necesidad de ser debidamente tutelado y reforzado por un marco normativo consistente y coherente.

2.1.2. Antecedentes nacionales

La tesis de investigación proporcionada por Vesga (2024) menciona el problema del uso indebido de las tecnologías de la información y su impacto en la violación de los derechos fundamentales, especialmente el derecho a la privacidad y la seguridad personal, se tiene como objetivo principal analizar cómo los delitos informáticos que involucran datos personales han afectado el derecho a la privacidad en dicha provincia durante el año 2023, y utilizó la metodología cuantitativa aplicada para examinar las fuentes consultadas y se llevó a cabo una encuesta, se emplearon cuestionarios y entrevistas para recolectar los datos, el resultado de la investigación y conclusión principal se basa en la urgencia de reforzar las medidas de seguridad y los protocolos para proteger tanto los datos personales como la información financiera de los usuarios. Además, sugiere la creación de plataformas digitales que validen en tiempo real para evitar la suplantación de identidad, así como la capacitación constante de los usuarios para prevenir actividades ilícitas. Sobre el aporte al presente trabajo de investigación, es importante porque dicho trabajo profundiza directamente sobre los delitos informáticos que cometen aquellos terceros contra el consumidor y propone soluciones para mejorar dicha protección de datos personales, fundamentos que complementan el tema de nuestro trabajo de investigación.

La tesis de investigación proporcionada por Bermudez (2024) destaca que el problema principal de la investigación es el uso indebido de datos personales en el sistema financiero y bancario, lo que ha incrementado los riesgos de violaciones a la privacidad y fraudes digitales, se tiene como objetivo principal analizar la vulneración del derecho a la intimidad en el sistema financiero y bancario de Lima, Perú en 2023, y utilizó una metodología de recopilación de datos validadas por especialistas, el resultado de la investigación fue, que se necesita fortalecer y actualizar la normativa peruana para proteger el derecho a la intimidad en el sistema financiero del Perú y la conclusión principal fue que la normativa de protección de datos personales en el sistema financiero de Perú, específicamente la Ley Nº 29733, es ineficaz en su implementación y presenta múltiples deficiencias que vulneran el derecho a la privacidad de los usuarios. Sobre el aporte al presente trabajo de investigación, es importante como antecedente porque ayudará a analizar la vulneración del derecho a la intimidad, derecho que es uno de los muchos que son vulnerados y que se expondrán en el presente trabajo de investigación, refiriéndose a la necesidad de fortalecer la normativa adoptando mejores prácticas para garantizar los derechos sobre los datos personales.

Olivos (2019) en el artículo de investigación menciona que una gran cantidad de países adoptan en su derecho interno reglamentaciones puntuales para estar protegidos frente a actos invasivos y arbitrarios a aspectos de la vida que solo deberían ser pertenecientes a la persona, de igual manera actúan organismos internacionales quienes exponen el requerimiento de tomar decisiones para actuar frente a los riesgos que estás nuevas tecnologías presentan, específicamente en cuanto a la informática, el problema que menciona está relacionado a la masificación del tratamiento de datos personales, su tráfico, y cómo estos conforman una amenaza al ordenamiento jurídico a través de un enfoque descriptivo y crítico, el objetivo alcanzado fue demostrar la privacidad como objeto de protección en Perú incorporada en la Constitución Política de 1993 en el art. 2.6 reconociendo su tutela; siendo el resultado principal demostrar que este tipo de información sensible y privada, es ahora el equivalente a una moneda de cambio, finalmente se concluye que el peso normativo de la ley en Perú es posiblemente uno de los retos más relevantes a los cuales se les debe prestar atención.

La importancia de este artículo para con la presente tesis deviene no solo en su precaución al alertar a la ciudadanía sobre la situación que se vive actualmente, sino en

cómo la legislación actual carece de una estructura sólida e inmutable para estar listos frente a las adversidades que puedan ocurrir.

2.1.3. Antecedentes internacionales

La tesis de Cueto (2019) refiere que el problema principal de la investigación es la adaptación del sistema financiero y las entidades bancarias a la revolución digital impulsada por el uso de Big Data, se tiene como objetivo principal entender como el análisis del Big Data ha transformado el valor de la información y las propuestas de negocio en el sistema financiero, y se utilizó una metodología basada en el estudio y la investigación exploratoria de técnicas cualitativas, el resultado y conclusión principal de dicha investigación es que cuando se habla de Big Data, se hace referencia a técnicas que empresas utilizan para analizar y procesar grandes volúmenes de datos que se producen día a día y su aplicación dentro de la entidad financiera. Sobre el aporte al presente trabajo de investigación, es importante como antecedente porque el término Big Data resulta relevante en el mundo financiero y bancario al ser grandes participantes de la revolución tecnológica y que al recibir estas grandes cantidades de datos personales, se tendrá que aplicar de manera adecuada para la protección de aquellos y por consiguiente otorga un mejor entendimiento el enfoque empresarial de estas instituciones al momento de manejar grandes cantidades de datos personales de los consumidores.

En la tesis presentada por Quezada (2019) destaca la creciente notabilidad para con la protección de datos personales en las años 2000 y 2019; en contraposición al Derecho quien no puede seguirle el paso a la tecnología, menciona que el problema radica en la exponencialidad de la tecnología, así como la volatilidad del mercado, lo que genera incertidumbre y complica la creación de mecanismos eficientes, el enfoque con el que se trabajó fue netamente crítico y analítico, su objetivo principal fue exponer el tratamiento de datos por estas instituciones del sistema financiero y extenderla a terceros relacionados con operaciones económicas; el resultado principal indica una insuficiencia tanto por parte de la legislatura chilena como por su doctrina, no obstante destaca el desarrollo de un proyecto de ley que logra ser un avance significativo, finalmente concluye que el sistema de información actual no es suficiente y posee una escasa regulación y falta de conocimiento por los usuarios frente a su existencia y *modus operandi.* La magnitud de esta investigación evidencia que este problema no solo acontece a nivel nacional, sino internacional; y el desafío que presenta tener una legislatura fuerte y lo suficientemente

flexible para que no quede obsoleta con el irrefrenable avance tecnológico, además de como reforzar dicha legislatura para que sea acatada no solo por los usuarios o consumidores, sino también por las empresas que ya llevan operando tanto en Chile como en Perú por largo de tiempo.

2.2. La Ciberseguridad

2.2.1. Concepto de ciberseguridad

Mediante el Congreso de la República (2011) en el Decreto de Urgencia Nº 007-2020 nombrada "Decreto de Urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento" en su artículo 3 acápite h. El referido autor define la ciberseguridad como la capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital y que comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país.

En un intento por ampliar la definición de ciberseguridad dentro del marco normativo del Estado Peruano el Proyecto de Ley Nº 01776/2021-CR, Congreso de la República (2024) se precisa que la denominada ley garantiza la ejecución de operaciones de ciberseguridad y seguridad digital a través de un centro nacional de ciberseguridad, intentó definirla como la capacidad tecnológica que resguarda la recolección de herramientas, políticas, directrices, enfoques de gestión de riesgos, acciones, capacitaciones, mejores prácticas, garantía y tecnologías que se pueden usar para proteger la disponibilidad, integridad y confidencialidad de los activos en las cimentaciones que son propiedad del estado, organizaciones privadas y de los ciudadanos, ante amenazas y vulnerabilidades en el ambiente digital.

La Recomendación UIT-T X.1205 de la Unión Internacional de Telecomunicaciones, (2008) en su inciso 3 en el capítulo de definiciones; en la cual se puede rescatar la distinción de propiedades de la ciberseguridad, y la define como la agrupación de herramientas, políticas, conceptos y salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, garantías y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno. Los activos de la organización y los usuarios son los dispositivos informáticos

conectados, los usuarios, los servicios o aplicaciones, los sistemas de comunicaciones, las comunicaciones a través de lo multimedia, y la totalidad de la información transmitida y/o almacenada en el ciber entorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciber entorno. Las propiedades de seguridad incluyen una o más de las siguientes: 1) disponibilidad; 2) integridad, que puede incluir la autenticidad y el no repudio; y 3) confidencialidad.

A raíz de estos avances es posible colegir que la ciberseguridad surge como resultado de una necesidad a fin de garantizar la seguridad, no solo de las personas en el ciberespacio, sino, de igual manera a sistemas informáticos a fin de reducir cualquier tipo de ciberataques; es así como se añade en el Proyecto de Ley Nº 08842/2024-CR promulgada por el Congreso de la República (2024), ley que declara de interés nacional y necesidad pública la creación del Comité de Alto Nivel de Ciberseguridad del Estado Peruano.

En otro intento del Congreso de la República (2025) se ofreció la definición de ciberseguridad, explicada como la práctica de salvaguardar la información digital, dispositivos y activos frente a vulneraciones cibernéticas, se eleva como una necesidad estratégica. Su propósito primordial es proteger los sistemas informáticos, aplicaciones, dispositivos, datos financieros y personales frente a diversas amenazas, como el ransomware, las estafas de phishing y el robo de datos.

La Superintendencia de Banca y Seguros, en su Resolución N.º 504-2021 dentro de su Reglamento para la gestión de la seguridad de la información y la ciberseguridad SBS (2021), en su artículo 2 del capítulo de definiciones tiene a la ciberseguridad como la protección de los activos de información a través de la prevención, detección, respuesta y recuperación frente a incidentes que afecten su disponibilidad, confidencialidad o integridad en el ciberespacio; el que a su vez es dependiente dentro de un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos.

Conforme al Tribunal Constitucional Pleno (2018) del Reino de España en su Sentencia Nº 142/2018 interpuesta por el presidente del Gobierno contra la Ley 15/2017, de 25 de julio, de la Agencia de Ciberseguridad de Cataluña logra definir a la ciberseguridad como poseedora de un notable carácter instrumental que le permite proyectarse sobre diversos

aspectos materiales y alcanzar también múltiples funcionalidades. Es identificable con la defensa o la seguridad nacionales en los posibles casos de mayor gravedad y con la seguridad pública cuando se trata de la salvaguarda ordinaria de las redes y las infraestructuras de telecomunicaciones. No obstante, puede proyectarse sobre otros planos, como por ejemplo es el caso de la administración electrónica, que engloba la organización de medios y previsión de medidas de protección de la administración, así como la protección de los derechos de los ciudadanos cuando se relacionan con la Administración por medios electrónicos.

Contrario a lo que pueda parecer, España, a diferencia de otros países del entorno global, no ha definido todavía una legislación específica y completa en materia de ciberseguridad. Sí existe legislación distribuida en distintos ámbitos ministeriales, pero que no ha sido desarrollada a partir de una política común que refleje el ámbito nacional y estratégico de la ciberseguridad (Fojón & Sanz, 2016).

No obstante, también dentro de la doctrina española, se tiene que la ciberseguridad se ocupa de la protección de los activos digitales, incluyendo redes, hardware y software, así como la información que es procesada, almacenada, en sistemas o transportada a través de entornos de información interconectados, y se hace referencia al conjunto de técnicas, sistemas de gestión y otras medidas que pretenden proteger la información digital y los medios que la tratan de incidentes deliberados o accidentales, es así como Ortega (2021) da mayores alcances al respecto, enriqueciendo el término y a su vez aumentando la parte de hardware, es decir todo lo exterior, físico y perceptible por los sentidos, siendo así que esté englobado en el ámbito de ciberseguridad

Por otro lado, en la legislación chilena es posible encontrar mediante el Congreso Nacional de Chile (2024) la Ley Nº 21663 nombrada como Ley Marco de Ciberseguridad en la cual en su artículo 2 en el capítulo de Definiciones ofrece el significado de la ciberseguridad como la preservación de la confidencialidad e integridad de la información, de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.

Para Astorga y Schmidt (2019) la ciberseguridad es también una allegada como seguridad cibernética, enfoca varias áreas, como: supervisar y gobernar, investigación, operación y mantenimiento, proteger y defender, entre otros. “Proteger y defender” es el

campo que se aboca a la protección a la vida, protección de la propiedad y seguridad de la información. [...] La formación en ciberseguridad con el foco puesto en el uso correcto de redes sociales en la niñez y la adolescencia recae en diferentes entes participantes en la acción didáctica: personal docente, estudiantes, padres y madres de familia, comunidad educativa e integrantes del contexto; es decir que dentro de la región Centroamericana no solo se exponen las áreas a las cuales está enfocada la ciberseguridad, sino que ya considera primordial su formación para los miembros más nuevos de su sociedad como vienen siendo los niños y adolescentes.

Para Borbúa (2017) asimismo, en Ecuador se establece el término ciberseguridad con dos acepciones diferentes. La primera, desde un ámbito más estratégico, y la cual sirve como soporte conceptual dentro de esta tesis, en la que se identifica la condición de un ciberespacio libre de amenazas, peligros y daños, así como el nivel de riesgo al que están expuestos sus organizaciones y ciudadanos; y la segunda, más operativa y funcional, trata de preservar la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, entre otros atributos.

Finalmente es clave entender que la ciberseguridad es uno de los desafíos más importantes a la seguridad, siendo un asunto estratégico del mismo nivel que las Armas de Destrucción Masiva y la Yihad Global, de acuerdo con lo mencionado por Gunn (2008) la situación no solo es crítica para el Estado Peruano, sino también para ciudadanos de los Estados Unidos de América, pues es considerado a la altura de problemas de envergadura internacional. En general, la ciberseguridad se caracteriza como una colección de tecnologías y procesos diseñados para proteger computadoras, redes, programas y datos contra actividades maliciosas, ataques, daños o acceso no autorizados (Aftergood, 2017).

2.2.2. Alcances sobre las normativas vigentes.

El Decreto Supremo que aprueba la "Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030" en su Artículo 2 respecto del Ámbito de aplicación menciona que esta misma es de aplicación obligatoria por los componentes del Sistema de Defensa Nacional en los tres niveles de gobierno, en el marco de sus funciones y competencias. Promulgado por el ex-presidente del Perú, Francisco (Sagasti, 2021).

Otro alcance que se tiene dentro de la legislación peruana es la ley que modifica el Decreto Legislativo Nº 1141, decreto legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia -

DINI, a fin de regular la seguridad digital, en su artículo 10.- Plan de Inteligencia Nacional - PIN menciona que [...] 10.1 Para efectos del desarrollo de actividades de inteligencia, contrainteligencia y seguridad digital, en el ámbito de su competencia, el Sistema de Inteligencia Nacional (SINA) cuenta con el Plan de Inteligencia Nacional (PIN), que contiene los objetivos, políticas, estrategias, gestión de riesgos y responsabilidades de sus componentes, relacionados con las amenazas a la seguridad nacional y la identificación de oportunidades favorables a ella, siendo su cumplimiento de carácter obligatorio. Es aprobado por el Consejo de Seguridad y Defensa Nacional en abril del año anterior a su ejecución, a propuesta del ente rector del SINA, previa conformidad del Consejo de Inteligencia Nacional (COIN); es así como se encuentra conforme al Congreso de la República.

De manera complementaria a través del Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, en su artículo 2 respecto a sus alcances menciona que las normas y procedimientos que rigen la materia de Confianza Digital son aplicables a las entidades establecidas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 004-2019-JUS, y, a las organizaciones de la sociedad civil, ciudadanos, empresas y academia; de esta manera el Congreso de la República (2017) intentó en múltiples ocasiones brindar la mayor cantidad posible de alcances dentro de la incipiente necesidad actual.

Asimismo el Congreso de la República (2018) en su Decreto Legislativo 1353 - Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses en su artículo 2 respecto del campo de aplicación menciona que las normas contenidas en el presente Decreto Legislativo son aplicables a todas las entidades señaladas en el Artículo I del Título Preliminar de la Ley Nº 27444, Ley del Procedimiento Administrativo General; así como a las empresas del Estado, personas naturales y jurídicas de derecho privado, en lo que corresponda; y a las personas comprendidas en la Ley Nº 29733, Ley de Protección de Datos Personales.

La ley de Delitos Informáticos promulgada por el Congreso de la República (2025) en su artículo 473 sobre el ámbito del proceso y competencia, en su inciso 1. menciona que

los delitos que pueden ser objeto de acuerdo, sin perjuicio de los que establezca la Ley, son los siguientes: a) Asociación ilícita, terrorismo, lavado de activos, delitos informáticos, contra la humanidad; es aquí donde se encuentra englobado dentro de delitos informáticos para mayor especificidad, asimismo el Decreto Supremo Nº 029-2021-PCM.

El Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, por ejemplo, en su artículo 2 destaca al ente rector y en su acápite 2.2. dice la materia de Gobierno Digital comprende los ámbitos de tecnologías digitales, identidad digital, interoperabilidad, servicios digitales, datos, seguridad digital y arquitectura digital, los cuales se relacionan entre sí con la finalidad de mejorar la prestación de servicios centrados en los ciudadanos, la gestión interna de las entidades de la Administración Pública y la relación entre éstas en la prestación interadministrativa de servicios públicos de manera segura para fortalecer la confianza y satisfacer las necesidades de los ciudadanos y personas en general en el entorno digital, orientado a la transformación digital del Estado. Es así como dentro de la misma legislación en el capítulo I llamado el Marco de Identidad Digital del Estado Peruano en su punto 9.3 menciona que comprende la gestión de la identidad digital en los siguientes ámbitos, a) ámbito de la interacción de los peruanos con servicios digitales provistos por las entidades de la Administración Pública y b) ámbito de la interacción de los extranjeros con servicios digitales provistos por las entidades de la Administración Pública. De igual manera en el inciso siguiente 9.4 La PCM, a través de la Secretaría de Gobierno Digital, amplía los ámbitos establecidos en función de la necesidad pública, cambio tecnológico, importancia estratégica o normativa expresa que lo demande; la misma que se hace efectiva mediante Decreto Supremo refrendado por la PCM.

En el artículo 94 sobre el Marco de Seguridad Digital del Estado Peruano en su inciso 2 se menciona que integra aquellas normas que conforman los ámbitos de defensa, inteligencia, justicia e institucional, establecidos en el artículo 32 de la Ley y se articula y sustenta en las normas, procesos, roles, responsabilidades y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información. La seguridad digital es un ámbito del Marco de Confianza Digital establecido en el Decreto de Urgencia

Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

Asimismo el capítulo II sobre la Gestión del Marco de Seguridad Digital del Estado Peruano en su artículo 98 sobre el ámbito de defensa, inciso 1, menciona que la ciberdefensa es gestionada por el Ministerio de Defensa, quien articula con sus órganos ejecutores el planeamiento y conducción de operaciones militares en y mediante el ciberespacio conforme los objetivos y lineamientos de la Política de Seguridad y Defensa Nacional aprobados por el Consejo de Seguridad y Defensa Nacional (COSEDENA) y de manera articulada con los objetivos de seguridad digital.

De igual manera el inciso 2 menciona que el Comando Conjunto de las Fuerzas Armadas está a cargo de la ciberdefensa de los activos críticos nacionales y recursos claves, cuando la capacidad de protección de sus operadores y/o sector responsable de cada uno de ellos o de la DINI o quien haga sus veces, sean sobrepasadas, y se vea afectada la seguridad nacional; y de manera consiguiente en el artículo 99 de la misma ley, respecto a su ámbito de inteligencia menciona que esta inteligencia y contrainteligencia en este ámbito es gestionada, en el marco de sus competencias, por la DINI , quien articula con la Secretaría de Gobierno Digital, la PCM y los órganos competentes, el planeamiento y conducción de operaciones de inteligencia para asegurar los activos críticos nacionales y de manera complementaria el artículo 100 habla sobre el ámbito de Justicia, es decir donde es aplicable la mencionada normativa, en su inciso 1 menciona que las acciones para garantizar la lucha eficaz contra la ciberdelincuencia es dirigida por el Ministerio del Interior (MININTER) y la Policía Nacional del Perú (PNP) , quienes articulan con el Ministerio de Justicia y Derechos Humanos (MINJUSDH) , el Instituto Nacional Penitenciario (INPE) , el Ministerio Público - Fiscalía de la Nación, el Tribunal Constitucional, Academia de la Magistratura, la Secretaría de Gobierno Digital de la PCM y el Poder Judicial (PJ) , conforme a lo dispuesto en la Ley Nº 30096, Ley de Delitos Informáticos, y los convenios aprobados y ratificados por el Estado Peruano en esta materia.

Finalmente en el artículo 101 hace referencia al ámbito institucional, el cual es dirigido, evaluado y supervisado por la PCM, a través de la Secretaría de Gobierno Digital, quien articula con las entidades de la Administración Pública la implementación de las normas, directivas y estándares de seguridad digital, ciberseguridad y seguridad de la información,

y supervisa su cumplimiento, así como el artículo 102 habla sobre la correcta articulación de ámbitos en donde la Secretaría de Gobierno Digital dirige y articula acciones para la gestión de incidentes y riesgos de seguridad digital que afecten a la sociedad con los responsables de los ámbitos de defensa, inteligencia y justicia, conforme lo establece el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento y su Reglamento (Congreso de la República, 2013).

2.2.3. Auditorías Algorítmicas Independientes

Según Metaxa (2022), las auditorías algorítmicas consisten en procedimientos sistemáticos en los que se "pregunta" repetidamente a un algoritmo mediante distintos insumos y se observan sus salidas, con el objetivo de inferir cómo opera internamente, incluso cuando el sistema es opaco o de caja negra. Este autor explica que dicho enfoque se apoya en técnicas de auditoría históricas adaptadas al ámbito de la inteligencia artificial, e incluye no solo el análisis técnico de código o datos, sino también consideraciones éticas, institucionales y de transparencia. Las auditorías permiten modelar la lógica del algoritmo, evaluar si cumple con estándares de justicia, sesgo o exactitud, y proponer mecanismos de corrección. En este sentido, Metaxa enfatiza que dichas auditorías deben considerarse como herramientas de gobernanza más allá del mero control técnico, e implican costos humanos, computacionales y ambientales que deben ser contemplados.

Mökander (2023) aborda la auditoría de IA como una evaluación independiente de los sistemas algorítmicos que extiende el concepto tradicional de auditoría hacia los entornos automatizados. El autor señala que estas auditorías no solo examinan el "qué" hace el algoritmo, sino también el "cómo" y el "por qué", integrando aspectos legales (por ejemplo, cumplimiento normativo), éticos (por ejemplo, equidad, transparencia) y técnicos (por ejemplo, robustez, explicabilidad). Asimismo, Mökander destaca que la independencia del auditor —es decir, su separación de quienes desarrollan o operan el sistema — es clave para garantizar credibilidad, y que los resultados deben traducirse en recomendaciones operativas. Finalmente, advierte que sin un marco regulatorio claro y sin estándares aplicados, la auditoría puede quedarse en un ejercicio simbólico y no lograr verdadero impacto.

Brand (2025) sostiene que para que las auditorías algorítmicas sean efectivas, deben implementarse a lo largo de todo el ciclo de vida del algoritmo: desde su fase de diseño, pasando por la validación, hasta su operación en producción y eventual retirada o reformulación. El autor argumenta que limitar la auditoría solo a una fase posterior al despliegue reduce su alcance y capacidad de mitigación de riesgos. Por tanto, Brand propone un enfoque integrado que combine herramientas específicas (por ejemplo, test de sesgo, trazabilidad de datos, verificación de modelos) con metodologías de auditoría robustas y una gobernanza institucional que supervise su implementación. Además, hace hincapié en que la auditoría debe contemplar tanto los efectos deseados como los no

deseados del sistema, analizando el impacto real en los usuarios y en la sociedad, no solo el cumplimiento técnico.

Laine (2024), mediante una revisión sistemática de literatura, concluye que las auditorías algorítmicas constituyen una práctica clave para la gobernanza ética de los sistemas de IA, pues permiten supervisar impactos, sesgos y decisiones automatizadas que afectan a grupos vulnerables. El estudio identifica que el enfoque ético requiere que los auditorios consideren no sólo la performance cuantitativa del algoritmo (por ejemplo, precisión) sino también su alineamiento con valores como la justicia, la transparencia y la dignidad humana. Laine subraya que muchas auditorías hasta ahora han sido técnicas o fragmentadas, y que la integración de la ética demanda marcos holísticos y normativos que las sustenten. Finalmente, destaca la necesidad de que las auditorías produzcan informes comprensibles para públicos no técnicos, reforzando su utilidad social y su legitimación.

Groves et al. (2024) investigan el régimen regulatorio de auditorías algorítmicas independientes implementado en la ciudad de Nueva York bajo la Local Law 144, que exige auditorías externas anuales de sesgos en herramientas automatizadas de empleo. El estudio muestra que, aunque esta normativa representa un paso adelante para la rendición de cuentas algorítmica, afronta retos importantes: la definición de quién es auditor, el grado de transparencia del informe y el alcance real de la supervisión. Los autores hallan que muchas organizaciones auditan por cumplimiento, pero sin transformar sus sistemas de modo sustantivo. En consecuencia, advierten que la mera obligatoriedad de auditoría no garantiza eliminación de sesgos o daños algorítmicos si no se acompañan de credibilidad institucional, estándares técnicos públicos y participación de los afectados.

La guía de la Eticas Foundation (2023) sostiene que las auditorías algorítmicas adversariales —realizadas por terceros externos al desarrollador del sistema— constituyen un instrumento esencial para revelar sesgos ocultos y ejercer transparencia en sistemas opacos de IA. Distingue estas de las auditorías internas o de segundo partido, enfatizando que las primeras ofrecen mayor independencia y credibilidad al poder acceder a resultados reales, aunque denuncian que por diseño pueden tener acceso limitado a datos o componentes internos. La guía indica que su función no es ofrecer un veredicto exhaustivo, sino más bien identificar anomalías, inspirar correcciones y alertar a reguladores y público. Además, destaca que sin normativas que obliguen a estas auditorías y sin estándares para evaluarlas, su impacto seguirá siendo limitado.

Según el artículo publicado por la consultora peruana Consultec (2024), en el contexto peruano las auditorías algorítmicas independientes se presentan como una herramienta valiosa para evaluar la equidad y exactitud de algoritmos usados en servicios digitales, sin comprometer secretos comerciales. El texto afirma que su adopción creciente exige que el marco legal peruano se adapte, pues todavía no existen regulaciones claras que obliguen a su implementación. Asimismo, enfatiza que la transparencia algorítmica —incluida la auditoría— debe vincularse con derechos del consumidor, protección de datos y responsabilidad de los operadores, de modo que las plataformas respondan por la lógica y efectos de sus sistemas automatizados.

Tillca (2024) analiza cómo la inteligencia artificial se emplea cada vez más en auditoría interna en el sector público peruano, y sugiere que ese desarrollo fortalece la función de las auditorías algorítmicas como parte de la gobernanza de sistemas automáticos. El autor expone que, al equipar a órganos de control con IA y métodos de análisis de datos, se amplía la posibilidad de detectar patrones atípicos, fraude o sesgos ocultos en los algoritmos. Sin embargo, también advierte que la incorporación de IA en auditoría requiere marcos normativos claros, recursos humanos calificados, y capacidad para interpretar resultados técnicos en un entorno jurídico y ético. En este sentido, surgen preguntas sobre la calidad de las auditorías, la independencia de los auditores y la rendición de cuentas frente a resultados hallados.

Napurí (2025) sostiene que las auditorías externas de algoritmos —es decir, realizadas por entidades independientes del desarrollador del sistema— son esenciales para detectar sesgos en algoritmos usados en procesos de selección, evaluación o prestación de servicios, lo cual tiene implicancias profundas para la justicia algorítmica. El autor argumenta que, sin auditorías independientes, los operadores pueden continuar aplicando sistemas opacos que discriminan o vulneran derechos, puesto que no están sujetos a supervisión efectiva. Además, plantea que para que tales auditorías sean funcionales se requieren criterios de acreditación del auditor, reporte público de hallazgos y participación de las organizaciones representativas de los afectados, de modo que la justicia algorítmica no se convierta en mera formalidad.

Según Costanza-Chock et al. (2023), aunque las auditorías algorítmicas se están convirtiendo en un mecanismo popular para la rendición de cuentas de sistemas automatizados, este campo aún carece de definición clara y estándares compartidos. Los

autores advierten que sin marcos normativos robustos, acreditación de auditores y transparencia en los resultados, la etiqueta "auditado" puede convertirse en un eslogan vacío y no garantizar responsabilidad real. Por ello, proponen que se exija a los operadores de sistemas automatizados: (1) auditorías independientes basadas en estándares definidos; (2) notificarse a los individuos afectados por decisiones algorítmicas; (3) divulgación pública de hallazgos; (4) la participación de las comunidades expuestas al riesgo; y (5) acreditación formal de auditores. En suma, plantean que la efectividad de las auditorías depende tanto de su técnica como de su institucionalización.

2.3. Datos personales

2.3.1. Concepto y como los datos personales son importantes

Acorde con el Reglamento Europeo y del Consejo (2016) los datos personales según su definición son:

"Se entiende por datos personales cualquier tipo de información que permita identificar o hacer identificable a una persona natural (también denominada "el titular"). Esta identificación puede lograrse de forma directa o indirecta, por ejemplo, a través de datos como el nombre, un número de identificación, ubicación geográfica, identificadores digitales, o mediante características particulares asociadas a su identidad física, fisiológica, genética, mental, económica, cultural o social."

Así mismo, en el Perú, a través de la Ley N° 29733, Ley de Protección de Datos Personales, se define datos personales como: "Se considera dato personal a cualquier información vinculada a una persona natural que permita reconocerla o hacerla identificable mediante medios razonablemente accesibles. Esta información puede presentarse en forma numérica, textual, visual, sonora, relacionada con costumbres o hábitos, o en cualquier otro formato que permita identificar directa o indirectamente a dicho individuo" (Congreso de la República, 2011).

Por último, para llegar a profundizar dicho concepto según lo mencionado por Hernandez (2018) el término "dato" proviene del latín *datum*, que se traduce como "aquello que se da", haciendo referencia a cualquier tipo de información proporcionada, ya sea en forma alfabética, numérica o simbólica, que represente hechos, elementos o circunstancias; en cambio, cuando se hace referencia a un dato personal, se está hablando

de información que permite identificar o individualizar a una persona específica, esto incluye, por ejemplo, el nombre, número de documento, edad, número telefónico, estado de salud, correo electrónico, domicilio, situación financiera, así como sus creencias políticas, religiosas o su orientación sexual.

2.3.2. ¿Por qué la vulneración de datos es un tema importante a tratar?

Se está viviendo una etapa, desde hace ya un tiempo, donde la protección de los datos personales se ha vuelto esencial ante el incremento de incidentes que afectan la seguridad en el sector financiero, ejemplos recientes ocurridos en países como Italia, Sudáfrica y el propio Perú evidencian una creciente frecuencia de delitos informáticos y una pérdida de confianza por parte de los usuarios hacia las entidades bancarias; esta situación pone de manifiesto una vulnerabilidad persistente, a lo largo del tiempo, la privacidad ha sido reconocida como un derecho fundamental, lo que subraya la urgencia de fortalecer su resguardo frente al denominado Poder Informático; en este contexto, resulta imprescindible asegurar el cumplimiento efectivo de las normas y la protección del derecho a la privacidad, especialmente en un entorno financiero cada vez más digitalizado e interconectado (Davalos & Mujica, 2022).

Parte de la vulneración de datos recae en el consentimiento otorgado por los consumidores al principio de otorgar sus datos a terceros, por ello se evidencia la relevancia de que el Estado garantice los derechos mediante la implementación de procedimientos administrativos sancionadores; en el caso peruano, existen actualmente dos mecanismos de esta naturaleza orientados a la protección de datos personales, sin embargo, aunque ambos buscan salvaguardar el principio de consentimiento, la inexistencia de un procedimiento único y consolidado, junto con la frecuente omisión del consentimiento informado por parte de los usuarios, debilita de forma significativa la protección efectiva de este derecho fundamental en la práctica (Escobar, 2022).

2.3.3. Manejo de datos por parte del sistema financiero

Acorde con la Ley N° 29733, Ley de Protección de Datos Personales, se menciona sobre la confidencialidad de los datos personales lo siguiente:

“Las personas que manejan, organizan o intervienen en el tratamiento de un banco de datos personales tienen el deber de conservar la reserva de la información y de su historial, aun cuando ya no exista vínculo alguno con el titular del banco” (Congreso de la República, 2011).

Por estos motivos, cabe destacar que, en la actualidad, muchas empresas incluso consideran que los datos personales representan uno de sus activos más valiosos, incluso por encima del valor económico directo, esto se debe a que, mediante el análisis de dicha información, pueden obtener un conocimiento preciso sobre las preferencias y necesidades de las personas, lo que les permite diseñar y ofrecer productos o servicios adaptados a esos requerimientos específicos (Pacheco, 2019).

Todas estas inconmensurables cantidades de información que guardan las instituciones financieras en secreto, se conocen como Big Data y para obtener utilidad de toda esta información, los bancos recurren al procesamiento de datos con mecanismos que cada vez exigen mayor eficiencia, exactitud y celeridad, lo que en cierta manera resulta perjudicial para el usuario, quien es el único propietario y titular de la información contenida en dichos sistemas, los cuales deben contar con las garantías adecuadas que le permitan ejercer sus derechos de control sobre tales datos que deben ser verosímiles, exactos, completos y vigentes, además, en caso contrario, contar con las vías legales para ejercer oportunamente sus pretensiones, a fin de que la información errónea sea rectificada e incluso eliminada a la mayor brevedad posible (Gonzales et al., 2024).

2.3.4. Inteligencia artificial y su impacto en el derecho

En principio, acorde con Mendoza (2022) puede afirmarse que el concepto de Inteligencia Artificial se utiliza, en términos generales, para describir la capacidad de las máquinas de replicar funciones cognitivas propias del ser humano; estos sistemas adquieren conocimiento mediante el análisis de ejemplos, pruebas, datos y patrones de comportamiento de los usuarios, además, emplean modelos como las redes neuronales para mejorar su desempeño: dado su carácter dinámico, el alcance de la Inteligencia Artificial está en constante transformación, en paralelo con los avances tecnológicos que surgen en este campo.

No obstante, la protección de los datos personales enfrenta importantes retos ante el acelerado avance y expansión de la Inteligencia Artificial, su implementación conlleva inevitablemente el tratamiento de grandes volúmenes de datos, dentro de los cuales se encuentran diversas categorías de información personal; tal como lo indica la Agencia de Protección de Datos Personales de Noruega, la mayoría de las aplicaciones basadas en Inteligencia Artificial requieren cantidades significativas de datos para poder aprender y tomar decisiones de manera eficaz; en este contexto, los datos no solo resultan

fundamentales para que estos sistemas alcancen su máximo rendimiento, sino también para minimizar posibles errores o sesgos durante su procesamiento (Morales, 2019).

Es un hecho que la Inteligencia artificial está en un auge increíble, desde sus primeras aplicaciones hasta la actualidad, la Inteligencia Artificial ha debido enfrentar múltiples desafíos; uno de los más relevantes radica en que los sistemas computacionales carecen de comprensión de significados, no poseen conciencia de sí mismos, emociones ni capacidad de interacción social., por esta razón, una máquina únicamente puede ejecutar las tareas para las que ha sido diseñada, ya que no tiene la capacidad de pensar de manera genuina como lo haría un ser humano (Florencia, 2020).

Por otro lado, para enfrentar el creciente fraude financiero en un entorno digitalizado, el propósito de ahora es aplicar inteligencia artificial avanzada para detectar y prevenir fraudes con mayor precisión y eficiencia que los métodos tradicionales, subrayando la necesidad urgente de proteger los datos y recursos financieros, adaptándose a las demandas de seguridad y eficiencia en un mundo digital en constante evolución, beneficiando a la sociedad en su conjunto (Fernández & Darwin, 2025).

2.4. Los derechos del Consumidor en el sistema financiero peruano

Los derechos del consumidor se encuentra en el Código de Protección y Defensa del Consumidor mediante el Congreso de la República (2025) a través del cual en el artículo IV se encuentran dentro de las definiciones, lo que se entiende para los efectos del presente Código, como a los consumidores o usuarios 1.1 Las personas naturales o jurídicas que adquieren, utilizan o disfrutan como destinatarios finales productos o servicios materiales e inmateriales, en beneficio propio o de su grupo familiar o social, actuando así en un ámbito ajeno a una actividad empresarial o profesional. No se considera consumidor para efectos de este Código a quien adquiere, utiliza o disfruta de un producto o servicio normalmente destinado para los fines de su actividad como proveedor. 1.2 Los microempresarios que evidencien una situación de asimetría informativa con el proveedor respecto de aquellos productos o servicios que no formen parte del giro propio del negocio. 1.3 En caso de duda sobre el destino final de determinado producto o servicio, se califica como consumidor a quien lo adquiere, usa o disfruta. 1.) Proveedores.- Las personas naturales o jurídicas, de derecho público o privado, que de manera habitual fabrican, elaboran, manipulan,

acondicionan, mezclan, envasan, almacenan, preparan, expenden, suministran productos o prestan servicios de cualquier naturaleza a los consumidores. En forma enunciativa y no limitativa se considera proveedores a:

1. Distribuidores o comerciantes. - Las personas naturales o jurídicas que venden o proveen de otra forma al por mayor, al por menor, productos o servicios destinados finalmente a los consumidores, aun cuando ello no se desarrolle en establecimientos abiertos al público.
2. Productores o fabricantes. - Las personas naturales o jurídicas que producen, extraen, industrializan o transforman bienes intermedios o finales para su provisión a los consumidores.
3. Importadores. - Las personas naturales o jurídicas que importan productos para su venta o provisión en otra forma en el territorio nacional.
4. Prestadores. - Las personas naturales o jurídicas que prestan servicios a los consumidores.
5. Producto. - Es cualquier bien mueble o inmueble, material o inmaterial, de origen nacional o no.
6. Servicio. - Es cualquier actividad de prestación de servicios que se ofrece en el mercado, inclusive las de naturaleza bancaria, financiera, de crédito, de seguros, previsionales y los servicios técnicos y profesionales. No están incluidos los servicios que prestan las personas bajo relación de dependencia.
7. Relación de consumo. - Es la relación por la cual un consumidor adquiere un producto o contrata un servicio con un proveedor a cambio de una contraprestación económica. Esto sin perjuicio de los supuestos contemplados en el artículo III.
8. Asociaciones de consumidores. - Son organizaciones que se constituyen de conformidad con las normas establecidas para tal efecto en el Código Civil. Su finalidad es proteger, defender, informar y representar a los consumidores y usuarios, pudiendo interponer ante las autoridades competentes reclamos y denuncias a nombre de sus asociados y de las personas que hayan otorgado poder

a su favor, así como en defensa de intereses difusos o colectivos de los consumidores, con sujeción a lo previsto en el presente Código.

9. Asimetría informativa. - Característica de la transacción comercial por la cual uno de los agentes, el proveedor, suele tener mayor y mejor información sobre los productos y servicios que ofrece en el mercado a los consumidores.
10. Habitualidad. - Se considera habitual aquella actividad que se realiza de manera común y reiterada de tal forma que pueda presumirse que se desarrolla para continuar en el mercado. Este concepto no está ligado a un número predeterminado de transacciones que deban realizarse. Las actividades de venta de productos o contratación de servicios que se realicen en locales abiertos son consideradas habituales por ese simple hecho.

Dentro del mismo código el capítulo I menciona los derechos de los consumidores en su artículo 1 homónimo:

1.1 En los términos establecidos por el presente Código, los consumidores tienen los siguientes derechos:

1. Derecho a una protección eficaz respecto de los productos y servicios que, en condiciones normales o previsibles, representen riesgo o peligro para la vida, salud e integridad física.
2. Derecho a acceder a información oportuna, suficiente, veraz y fácilmente accesible, relevante para tomar una decisión o realizar una elección de consumo que se ajuste a sus intereses, así como para efectuar un uso o consumo adecuado de los productos o servicios.
3. Derecho a la protección de sus intereses económicos y en particular contra las cláusulas abusivas, métodos comerciales coercitivos, especulación o acaparamiento en situación de emergencia debidamente declaradas o cualquier otro delito análogo e información interesadamente equívoca sobre los productos o servicios.
4. Derecho a un trato justo y equitativo en toda transacción comercial y a no ser discriminados por motivo de origen, raza, sexo, idioma, religión, opinión, condición económica o de cualquier otra índole.

5. Derecho a la reparación o reposición del producto, a una nueva ejecución del servicio, o en los casos previstos en el presente Código, a la devolución de la cantidad pagada, según las circunstancias.
6. Derecho a elegir libremente entre productos y servicios idóneos y de calidad, conforme a la normativa pertinente, que se ofrezcan en el mercado y a ser informados por el proveedor sobre los que cuenta.
7. A la protección de sus derechos mediante procedimientos eficaces, céleres o ágiles, con formalidades mínimas, gratuitos o no costosos, según sea el caso, para la atención de sus reclamos o denuncias ante las autoridades competentes.
8. Derecho a ser escuchados de manera individual o colectiva a fin de defender sus intereses por intermedio de entidades públicas o privadas de defensa del consumidor, empleando los medios que el ordenamiento jurídico permita.
9. Derecho a la reparación y a la indemnización por daños y perjuicios conforme a las disposiciones del presente Código y a la normativa civil sobre la materia.
10. Derecho a asociarse con el fin de proteger sus derechos e intereses de manera colectiva en el marco de las relaciones de consumo.
11. Derecho al pago anticipado o prepago de los saldos en toda operación de crédito, en forma total o parcial, con la consiguiente reducción de los intereses compensatorios generados al día de pago y liquidación de comisiones y gastos derivados de las cláusulas contractuales pactadas entre las partes, sin que les sean aplicables penalidades de algún tipo o cobros de naturaleza o efecto similar.
12. Derecho a contar con opción o alternativa de atención personal cuando el proveedor ofrezca al público cualquier sistema de atención automatizada asistido por inteligencia artificial o asistente digital.

1.2. La enumeración de los derechos establecidos no excluye los demás que este Código garantiza ni los reconocidos en leyes especiales.

1.3 Es nula la renuncia a los derechos reconocidos por la presente norma, siendo nulo todo pacto en contrario.

2.4.1. Cómo es que se protegen los derechos de los consumidores.

El derecho de protección al consumidor es un derecho constitucional, ubicado en la Constitución Política del Perú (1993) en su artículo 65 llamado como protección al consumidor, el cual establece que el Estado defiende el interés de los consumidores y usuarios. Para tal efecto garantiza el derecho a la información sobre los bienes y servicios que se encuentran a su disposición en el mercado. Asimismo, vela, en particular, por la salud y la seguridad de la población.

Mediante el Código de Protección y Defensa del Consumidor el Congreso de la República (2012) en su artículo II menciona la finalidad es decir que los consumidores accedan a productos y servicios idóneos y que gocen de los derechos y los mecanismos efectivos para su protección, reduciendo la asimetría informativa, corrigiendo, previniendo o eliminando las conductas y prácticas que afecten sus legítimos intereses. En el régimen de economía social de mercado establecido por la Constitución, la protección se interpreta en el sentido más favorable al consumidor, de acuerdo con lo establecido en el presente Código.

2.4.2. Falta de conocimiento de los consumidores sobre sus derechos y casos relevantes.

La Constitución prescribe en su artículo 65 la defensa de los intereses de los consumidores y usuarios, a través de un derrotero jurídico binario; vale decir, establece un principio rector para la del Estado y, simultáneamente, consagra un derecho subjetivo. En lo primero, el artículo tiene la dimensión de una pauta básica o postulado destinado a orientar y fundamentar la actuación del Estado respecto a cualquier actividad económica. Así, el juicio estimativo y el juicio lógico derivado de la conducta del Estado sobre la materia tienen como horizonte tuitivo la defensa de los intereses de los consumidores y los usuarios. En lo segundo, la Constitución reconoce la facultad de acción defensiva de los consumidores y usuarios en los casos de transgresión o desconocimiento de sus legítimos intereses; es decir, apareja el atributo de exigir al Estado una actuación determinada cuando se produzca alguna forma de amenaza o afectación efectiva de los derechos de consumidor o usuario, incluyendo la capacidad de acción contra el propio proveedor; es así como en la Sentencia del Tribunal Constitucional del Perú (Poder Judicial, 2006).

2.4.3. El papel del consumidor en la protección de su propia información personal.

Según Ley de protección de datos personales (LPDP) Congreso de la República (2017) se define al titular de datos personales como la personal natural quien es responsable de los datos personales y en su inciso siguiente al titular del banco de datos personales añade a la persona jurídica de derecho privado o entidad pública que denote el objetivo final y el contenido del banco de datos personales, su tratamiento y las medidas de seguridad. En el mismo orden de ideas en el artículo 13 inciso 5 menciona que estos datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto, y que dicho consentimiento debe ser previo, informado, expreso e inequívoco de lo cual se desprenden estas cuatro características que son fundamentales (Congreso de la República, 2017). En lo posterior dentro del mismo artículo en su inciso 7 se habla sobre la revocación de este consentimiento en cualquier momento, siempre atendiendo al efecto de sus requisitos con ocasión de su otorgamiento (Congreso de la República, 2017).

El Principio de consentimiento se encuentra expreso en la LPDP del Congreso de la República (2017) donde menciona que para el tratamiento de datos personales debe mediar el consentimiento del titular. Es decir que parte del papel del consumidor ya recae en su responsabilidad al aceptar o denegar este tratamiento de datos personales.

En el artículo 9, principio de seguridad, de la LPDP del Congreso de la República (2017) se menciona que el titular del banco de datos personales y el encargado de su tratamiento, deben afianzar los objetivos técnicos, organizativos y legales requeridas para salvaguardar la seguridad de los datos personales, estas medidas de seguridad deben ser apropiadas y conformes al tratamiento que se vaya a llevar a cabo en concordancia con el segmento de datos personales donde se trate; de lo cual se desprende una nueva responsabilidad, no solo del titular sino del encargado de su tratamiento.

En el artículo 10, principio de disposición de recurso, de la LPDP del Congreso de la República (2017) se desprende que todo titular de datos personales debe tener acceso a las vías administrativas o jurisdiccionales idóneas para presentar su reclamo y defender sus derechos, en caso estos se vean afectados por el tratamiento de sus datos personales; de ello se colige que parte de su rol es de hacer respetar sus derechos en caso estos se vean afectados.

El único inciso que hace mención a la indemnización por los daños generados a los titulares de los datos personales es el número 25, Congreso de la República (2017) indicando que quien sea afectado a consecuencia del incumplimiento de esta Ley, por el titular o encargado o por terceros, tiene derecho a obtener la indemnización que corresponda según ley; esto también entra en el rol que tiene el consumidor pues le da más facultades para actuar ejerciendo sus derechos.

En adición a ello el autor Hernandez (2022) reconoce que estos titulares no sólo están facultados a iniciar procedimientos administrativos sancionadores contra entidades y/o personas naturales que traten de una manera indebida sus datos personales, sino que inclusive tienen la facultad sobre la posibilidad de recurrir a la tutela resarcitoria, es decir responsabilidad civil, con el fin de restaurar estos daños que se coligen de mencionado tratamiento legal.

En la misma línea conforme a la Sentencia del Tribunal Español 292/2000, Tribunal Constitucional Español (2000) menciona que este derecho a la protección de datos atribuye a su titular una serie de capacidades en múltiples poderes jurídicos cuya ejecución imputa a terceros ciertas responsabilidades jurídicas; de lo cual se interpreta que parte del rol del consumidor no es exclusivo a sus facultades o responsabilidades sino que es oponible a terceros.

Uno de los diversos aspectos que destaca el Reglamento es que a fin de demostrar la obtención del consentimiento de la LPDP la carga de la prueba recae en la totalidad de supuestos en el titular del banco de datos personales o quien sea responsable del tratamiento y hay coincidencias frente a la doctrina norteamericana reconociendo esto como un eje central; descrito así por la autora Olivos (2020) para rescatar lo que a priori parece una nueva responsabilidad que recae en el rol de consumidor.

Para Laisha (como se cita en Mubarak, 2017) el consentimiento es una concepción fundamental en la protección de datos personales en el cual se crea una unidad que le ofrece al usuario la completa discrecionalidad de decidir si usar sus datos personales por terceras partes o no, precisando que esta aprobación es obligatoria cuando respecto de datos personales no sea posible su entrada en el anonimato o su desasociación.

Para el autor Alejandro (como se cita en Morales, 2021) hay dos aristas de la IA que son puntualmente importantes para la privacidad, siendo el primero es que la IA pueda

tomar decisiones automatizadas y el segundo mencionando que el sistema se desenvuelve aprendiendo de la práctica e información proporcionada; no obstante cabe destacar que toda la información con la que la IA trabaja es una gran recopilación de datos personales respecto de la cual una persona que dio consentimiento al tratamiento de estos no pudo preveer como es que estos serían utilizados o con que finalidad, inclusive quizás no siendo debidamente informado al respecto del uso de estos para fines de entrenamiento de IA para una toma de decisiones automatizada a largo plazo.

2.4.4. Derecho al olvido

En principio para entender este concepto conforme lo explica la Agencia española de protección de datos (2023) el derecho al olvido permite limitar la difusión de datos personales en buscadores cuando la información, aunque es legítima, se ha vuelto irrelevante u obsoleta siendo esta una manifestación del derecho de supresión frente al impacto prolongado de internet sobre la privacidad. Según Gilvonio (2025) nos menciona que la legislación peruana ha mejorado en la protección de datos personales, sin embargo, aun este no alcanza el nivel de regulaciones europeas avanzadas como lo tendría el GDPR y asimismo nos subraya la necesidad de reforzar la protección de datos confidenciales y establecer un marco legal específico para implementar el derecho al olvido en el Perú.

Por otro lado, el Tribunal Constitucional reconoció por primera vez al derecho al olvido como parte del derecho constitucional a la autodeterminación informativa, asimismo se definió que el derecho al olvido como una garantía de eliminar o suprimir datos personales de internet en su momento de haber sido veraces, han dejado de serlos por motivos como cambios fácticos o jurídicos y que podría afectar el honor, la reputación o la intimidad del afectado (Kong, 2022). Esta sentencia evidencio que, si bien se reconoce jurisprudencialmente al derecho al olvido, este aún no existe en una ley específica, por lo que su alcance está delimitado por una interpretación constitucional y la aplicación de la Ley 29733

Del mismo modo según López (2024) nos indica que si bien no hay una norma expresa que reconozca el derecho al olvido, este se vino construyendo via jurisprudencia tanto a nivel administrativo como constitucional. Los desarrollos jurisprudenciales han delineado poco a poco los fundamentos y límites de este derecho. No obstante, dicho autor advierte que la evolución del derecho involucraría necesariamente la adopción del derecho al olvido para brindar una mayor seguridad jurídica.

2.4.5. Medidas que promuevan la responsabilidad e información en el uso seguro de servicios financieros digitales.

Un buen punto de referencia sería la Ley 28587 del Congreso de la República (2025) ley complementaria a la ley de protección al consumidor en materia de servicios financieros, la cual menciona en su artículo 2 sobre la transparencia en la información, que las empresas sujetas al alcances de dicha Ley, están obligadas a ofrecer a los usuarios toda la información que estos demanden de manera previa a la celebración de cualquier contrato propio de los productos o servicios que brindan sin perjuicio de los dispuesto en las normas legales de carácter especial; esta es una de las medidas que promueven la responsabilidad de las empresas frente a los usuarios.

Más adelante en su artículo 8 de la misma Ley del Congreso de la República (2025) menciona la difusión en las tasas de interés, comisiones y gastos, destacando que están obligadas a difundir constantemente lo antes mencionado respecto a lo que sea recaudado desde los usuarios en las operaciones financieras que hayan sido ofrecidas al mercado, buscando garantizar el acceso a los usuarios a dicha información mediante múltiples tipos de comunicación directa, e indirecta como televisión, radio, periódicos, de manera local y a través de páginas web, siendo esto supervisado por la SBS respecto a las condiciones en las que estas se lleven a cabo.

Finalmente en sus artículos 9 y 10 de la presente Ley, Congreso de la República (2025) se menciona que la SBS y en adición el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual están capacitados para dar la mayor difusión posible de toda la información que consideren pertinente con el objetivo de incrementar la transparencia del mercado de servicios financieros; mientras tanto el subsiguiente artículo menciona que cualquier omisión que se llevase a cabo referente a las disposiciones contenidas en esta Ley, será sancionada por estas dos instituciones conforme a dónde recaiga su responsabilidad; de todo esto se puede colegir que el Estado Peruano busca proteger al consumidor al hacer recaer la responsabilidad de la debida comunicación sobre la información utilizada dentro del sistema financiero como medida para el uso seguro de servicios digitales.

Ahora en el Código de Defensa y Protección del Consumidor, Congreso de la República (2010) en su artículo 50 refiere a las cláusulas abusivas de ineficacia absoluta,

en su inciso a. menciona que las que excluyan o limiten la responsabilidad del proveedor o de quienes dependan de él por dolo o culpa, o aquellas que fuesen trasladadas al consumidor por hechos u omisiones del proveedor; por consiguiente si bien no es una medida que busque promover la responsabilidad por sí misma, sí consigue delimitarla al colocarle una barrera que no puede ni debe ser atravesada, y de ser el caso que contiene una respuesta inmediata.

Más adelante en el Código, Congreso de la República (2010) en su artículo 100 se habla de la responsabilidad civil mediante la cual se hace mención al proveedor que ocasione daños y perjuicios al consumidor se encuentra en la obligación de indemnizar conforme a las disposiciones del Código Civil, sin perjuicio de la responsabilidad penal, sanciones administrativas y vías correctivas reparadoras y complementarias que sean presentables acorde a la aplicación del Código; en consecuencia es una medida tomada para presentar la obligación de indemnización frente al consumidor si es que se le ha ocasionado algún daño o perjuicio como podría ser una filtración de datos, suplantación de identidad, robo de credenciales, etc.

Una de las medidas que se contempla dentro del ordenamiento jurídico se encuentra en la LPDP, Congreso de la República (2011) en su artículo 33 donde hace mención a las funciones de la Autoridad Nacional de Protección de Datos Personales (ANPDP) en cuyo inciso 7 habla sobre coordinar la inclusión de información sobre la importancia de la vida privada y de la protección de datos personales en la totalidad de los planes de estudios dentro de múltiples niveles educativos y hacer énfasis en la capacitación de los docentes en los mencionados temas, por lo tanto esta medida no solo busca resaltar la relevancia de la protección de los datos personales sino que fomenta su debida comunicación y aprendizaje al corazón de una sociedad como viene siendo la mayor parte de los grados académicos.

Dentro de la Ley General del Sistema Financiero (LGSF), Congreso de la República (1996) en su artículo 141 llamado falta grave de quienes violen el secreto bancario, menciona que sin perjuicio de la responsabilidad penal señalada en el Código Penal, se le considera una falta grave a para efectos laborales y si no fuese el caso entonces sancionado con multa, la pertinencia de este artículo recae en la sanción que hay en el caso de una filtración de datos en la cual se haya visto involucrado alguien otorgando los permisos oportunos de manera interina para que esto se llevase a cabo. En el mismo orden

de ideas en el artículo 361, sanciones, de la misma ley, Congreso de la República (1996), se destaca un listado de sanciones conforme a la gravedad de la infracción cometida, y al finalizar la lista se alega que la aplicación de estas sanciones no eximen de responsabilidad civil o penal en caso sea pertinente, por consiguiente la medida sancionadora no solo existe dentro de esta Ley, sino que se extiende a otros ámbitos como el civil o penal.

En concordancia con lo anteriormente expuesto en el artículo 135 de la LGSF, Congreso de la República (1996) se expone la obligación que las empresas del sistema financiero tienen que mantener debidamente informada a su clientela respecto de su situación económica y financiera, mediante publicaciones de los estados financieros en el Diario Oficial y en uno que sea de extensa circulación nacional por lo menos 4 veces al año; y en el artículo 137 de la misma Ley la Superintendencia deberá difundir la información de los primordiales indicadores de la situación de las empresas del sistema financiero, y dentro de muchas facultades también se añaden las que considere necesaria para el público, de todo esto se colige que no es solo una medida para promover la responsabilidad de las empresas del sector financiero, sino también del consumidor de estas empresas en revisar los estados financieros donde tenga activos que considere relevantes para él mismo.

Finalmente dentro del artículo 143-A. de la LGSF, Congreso de la República (1996) se hace mención a cómo las empresas del sistema financiero deben suministrar información a la SUNAT, dentro de inciso 5, acápite 1 se menciona que esta información es debidamente tratada bajo las reglas de confidencialidad y seguridad informática que es exigida mediante estándares y recomendaciones internacionales respecto del intercambio automático de información financiera emitidos por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), por lo expuesto se entiende que esta medida cumple debidamente con la correcta manera del uso de datos personales y financieros mediante una entidad estatal que cumple con los lineamientos de la OCDE.

2.4.6. Requisitos y procedimiento para cautelar el derecho del consumidor.

En el Código de Protección y Defensa del Consumidor del Congreso de la República (2010) en su artículo 109 habla sobre las medidas cautelares, en cualquier etapa del procedimiento, de oficio o a pedido de parte, el Indecopi puede, dentro del ámbito de su correspondiente competencia, dictar una o varias de las siguientes medidas cautelares destinadas a asegurar el cumplimiento de la decisión definitiva:

1. La cesación de los actos materia de denuncia.
2. El comiso, el depósito o la inmovilización de los productos, etiquetas, envases y de cualquier otro bien que sea materia de denuncia.
3. La adopción de las medidas necesarias para que las autoridades aduaneras impidan el ingreso al país de los productos materia de denuncia.
4. El cierre temporal del establecimiento del denunciado.
5. Cualquier otra medida que tenga por objeto evitar que se produzca algún perjuicio derivado del acto denunciado o que tenga como finalidad la cesación de éste.

El Indecopi puede, de considerarlo pertinente, ordenar una medida cautelar distinta a la solicitada por la parte interesada. En caso de existir peligro actual o inminente si es que no se adoptan las medidas cautelares correspondientes, el secretario técnico puede imponerlas, con cargo a dar cuenta inmediatamente a la comisión. La comisión ratifica o levanta la medida cautelar impuesta. El Órgano Resolutivo de Procedimientos Sumarísimos en materia de protección al consumidor goza también de la facultad de ordenar medidas cautelares (Congreso de la República, 2012).

2.5. Sistema Financiero Peruano

La Ley Nº 26702, General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros define al sistema financiero como el conjunto de empresas, que debidamente autorizadas operan en la intermediación financiera (Congreso de la República, 2019). Incluye las subsidiarias que requieran de autorización de la Superintendencia para constituirse.

La literatura indica que existe una relación positiva entre el crecimiento económico de un país y el desarrollo de su sistema financiero, es así como Čihák lo menciona.

2.5.1. Alcances de la normativa vigente.

La Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros promulgada por el Congreso de la República, menciona en su artículo 1 como los alcances de la ley general, indicando que la presente ley establece el marco de regulación y supervisión a que se someten las empresas que

operen en el sistema financiero y de seguros, así como aquéllas que realizan actividades vinculadas o complementarias al objeto social de dichas personas.

Salvo mención expresa en contrario, la presente ley no alcanza al Banco Central.

2.5.2. Cómo es que el sistema financiero digital se va actualizando y protegiendo las posibles amenazas en cuanto a los derechos del consumidor

Dentro del Título preliminar, artículo 6 del Código llamado Políticas Públicas, su inciso 1 menciona que el Estado protege la salud y seguridad de los consumidores a través de una normativa apropiada y actualizada; en concordancia esta es una de las maneras en las cuales el ordenamiento jurídico se tiene que actualizar constantemente frente a nuevas amenazas (Congreso de la República, 2010).

En el capítulo 4 sobre Salud y seguridad de los consumidores dentro del artículo 25 del Código se hace mención al deber general de seguridad donde se menciona que los productos o servicios ofrecidos en el mercado no deben contener en condiciones normales o prevenibles, riesgo injustificado o no advertido para la salud o seguridad de los consumidores o sus bienes; ahora si bien este capítulo se encuentra enfocado prioritariamente al sector salud, es igual de importante el área de seguridad, si el servicio ofertado puede llegar a contener algún riesgo no justificado o no advertido respecto de los bienes del consumidor entonces se puede entender una vulneración de datos personales y/o sensibles dentro del sistema financiero (Congreso de la República, 2010).

Una de las maneras a través de las cuales el sistema financiero digital se mantiene actualizado se encuentra en el artículo 33 de la LGPD en sus incisos 3 y 4 respecto a las funciones de la ANPDP, las cuales son administrar y mantener actualizado el Registro Nacional de Protección de Datos Personales, y el de publicitar una relación actualizada de bancos de datos personales de administración pública y privada (Congreso de la República, 2011).

Otra forma a través de la cual el sistema financiero se mantiene debidamente actualizado es mediante la Central de Riesgos, artículo 158 de la LGSF donde la Superintendencia tiene en su cargo un sistema integrado de un registro de riesgos que contiene información consolidad y confidencial sobre los deudores de las empresas; esto acompañado del artículo 159 de la misma Ley sobre la obligación de suministrar la información relevante mencionar que las empresas del sistema financiero deben contribuir de manera periódica y oportuna la información para que este registro esté actualizado; es por todo lo expuesto anteriormente que este es otro mecanismo que posee el ordenamiento

jurídico para mantenerse actualizado respecto de los datos personales de la población (Congreso de la República, 1996).

Asimismo, en las disposiciones finales de la LGSF se hace mención a que toda publicación referente a dicha Ley para diversos actuados administrativos o de la misma Administración se pueden realizar de manera electrónica o virtual (Congreso de la República, 1996).

Respecto al ámbito nacional, el Decreto Supremo Nº 029-2021-PCM. Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo tiene por objeto, en su artículo 1, regular las actividades de gobernanza y gestión de las tecnologías digitales en las entidades de Administración Pública en materia de gobierno digital […] establecer las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, criterios, condiciones, mecanismos y plazos de implementación; en este mismo orden de ideas la estructura que se presenta podría ser extrapolada al resto de normas vistas, para tener un sistema financiero actualizado y que por lo tanto tenga las capacidades para protegerse y hacerle frente a posibles amenazas (Presidencia del Consejo de Ministros, 2021).

2.5.3. Medidas para solucionar los vacíos o problemas encontrados.

Como lo menciona el autor Eduardo (como se cita en Gamero, 2021) no se trata de legislar de nuevo, sino de llenar los vacíos que se aprecien, de la misma manera aclarar las especificidades que resulten convenientes en atención a las particularidades que refiere la IA; por consiguiente, no se trata de promulgar nuevas leyes en cada ocasión, sino tratar de cubrir la mayor cantidad de vacíos con la mejor legislación posible.

El desarrollo de políticas públicas que vayan dirigidas a la implementación de facilitadores de innovación en Perú es más que asequible, aunado a ello se alinearía con las estrategias de la nación en materia de innovación e inclusión financiera, es así cómo lo describe Lucía (como se cita en Suárez, 2021) al respecto de la innovación tecnológica en el sector financiero peruano.

Para Alexander (como se cita en Shukarenko, 2019) se deben considerar las herramientas tecnológicas para poder investigar delitos cibernéticos, con la previsión legal

que esta requiere en cada caso respectivo con el objetivo de garantizar los procesos correctos y efectivos, por lo tanto no solo basta con suplir los vacíos que se puedan encontrar, sino ir más allá y buscar la manera en la cual todos estos avances tecnológicos terminan sirviendo un propósito mayor para el Estado.

Desde un punto de vista preventivo, para los autores Leonidas y Nilton (como se cita en Carhuas y Velazco, 2024) son los ciudadanos y las instituciones quienes deben proteger estos datos de manera continua, para evitar ser anticipados, puesto que la legislación contiene vacíos legales, que hacen que no se sancionen estos actos y de igual manera no se presenta un soporte a nivel social para castigar estos delitos, por lo tanto se desprende que mientras la legislación peruana intenta ponerse al día frente al implacable paso de la tecnología es prioritario ser cauteloso y preventivo como ciudadano frente a la ciberseguridad.

Según la Resolución Nº 1040-2024 de la Comisión de Protección al Consumidor respecto a los principios de legalidad y de uniformidad menciona que servirán como criterio interpretativo para solucionar las vicisitudes que puedan darse en la aplicación de reglas de procedimiento, cómo medidas para la generación de otras disposiciones administrativas de índole general, y para satisfacer los vacíos en la legislación administrativa, por consiguiente se entiende que es parte de la labor del juez o entidad jurisdiccional suplir los vacíos que se encuentren en la norma (Presidencia del Consejo de Ministros, 2024).

2.6. Derecho comparado

2.6.1. Estados unidos

Este país constituye un caso particular ya que es la única potencia en carecer de un conjunto unificado de leyes nacionales de privacidad de datos, y es que Estados Unidos posee una disposición legal en esta temática: la Ley de Privacidad del Consumidor de California (CPA), la cual sólo tiene injerencia en el estado de California y está inspirada en el Reglamento general de protección de dato (GDPR) de la Unión Europea (Quesada & Zeniquel, 2020).

Del mismo modo, según Lindner (2023) no existe una ley integral de privacidad financiera que pueda proteger a los consumidores de la recopilación, el intercambio y la

venta de datos de los consumidores por parte de una empresa; la ley federal de privacidad financiera más reciente, la Ley Gramm-Leach-Bliley ("GLBA"), fue promulgada por el Congreso hace más de 20 años. Desde 1999 se han producido grandes cambios tecnológicos y financieros, y la ley de privacidad financiera debe actualizarse para seguir la carrera con la tecnología.

En la actualidad, Aunque existen normativas como el GDPR la Ley de informes de crédito justo (FCRA) o la privacidad del consumidor en california (CCPA) que limitan la libre divulgación de información confidencial por parte de las instituciones financieras también hay regulaciones como la Ley de Secreto Bancario de 1970 que obligan a estas entidades a compartir determinados datos financieros con organismos estatales con el fin de prevenir y combatir delitos financieros lo cual genera una tensión constante entre la protección de la privacidad y la necesidad de garantizar la integridad de las operaciones financieras (Chatzigiannis et al., 2023).

2.6.2. Unión europea

España

En la actualidad el Estado español se rige por la Constitución de 1978 la cual incorpora disposiciones orientadas a la protección de los datos personales de sus ciudadanos, en ese sentido el artículo 18.4 incluido en la sección dedicada a los derechos fundamentales y libertades públicas establece que la ley limitará el uso de la información para garantizar el honor la intimidad personal y familiar de los ciudadanos así como el pleno ejercicio de sus derechos esta disposición fue pionera e importante ya que dio lugar a la creación de diversas normas y reglamentos que aseguran hasta hoy una tutela efectiva de este derecho adaptándose progresivamente a los avances tecnológicos surgidos en las últimas décadas (Pachecho, 2019).

Asimismo, el derecho a la protección de datos también cuenta con respaldo en el ámbito penal específicamente dentro de los delitos relacionados con el descubrimiento y la revelación de secretos tal como se establece en el apartado 2 del artículo 197 del Código Penal donde se sancionan aquellas conductas que debido a su gravedad requieren una respuesta penal adecuada (Fernandez, 2017).

Del mismo modo, acorde con Morales (2020) la creación de la Agencia Española de Protección de Datos tiene su origen en la Ley de Protección de Datos de 1992, la cual representó un hito importante para el desarrollo normativo en España ya que su función

principal fue establecer límites claros en el tratamiento de datos personales tanto en el ámbito empresarial como en el de los ciudadanos y las entidades públicas actuando como un mecanismo esencial para evitar la libre circulación indiscriminada de datos y asegurar que toda actividad relacionada con su uso se rija por lo dispuesto en dicha ley.

Alemania

Actualmente las modalidades para obtener datos personales son más variados a diferencia del siglo pasado, por ello frente estas innovaciones el Estado Alemán ha adoptado medidas para contrarrestar aquellos actos que vulneren estos derechos, para ello creó "la Ley Federal de Protección de Datos (Federal Data Protection Act), es la normatividad vigente en Alemania, que existe desde 1977; es la ley principal que se encarga de desarrollar la legislación facultada para proteger los datos personales, dado que este derecho, no se encuentra regulado como tal dentro de la Constitución"; esto ha permitido una mayor tutela a los datos personales, más aún en esta era de las innovaciones tecnológicas que mantiene una relación con los datos personales mediante herramientas tecnológicas como los bancos de datos que forman parte de una entidad de carácter público o privado (Pachecho, 2019).

2.6.3. Latinoamérica

México

México cuenta con un régimen particular destinado a la protección del consumidor financiero el cual se encuentra principalmente regulado por el Estatuto Orgánico de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros conocida como la Comisión Nacional así como por la Ley de Protección y Defensa al Usuario de Servicios Financieros que establece mecanismos específicos para resguardar los derechos de quienes utilizan servicios financieros en el país (Gómez et al., 2024).

Siguiendo esta línea, acorde con Arellano (2021) en cuanto a la situación actual en México se puede señalar que las disposiciones vigentes a nivel nacional han contribuido al fortalecimiento del Derecho a la Protección de Datos Personales generando obligaciones concretas tanto para el sector público como para el sector privado en aquellos casos en que intervengan en el tratamiento de información como parte de sus actividades o procesos institucionales.

No obstante en lo que respecta a la protección de datos personales México aún enfrenta importantes desafíos ya que el reconocimiento de este derecho no se ha consolidado plenamente como un derecho fundamental sino que ha sido abordado mayormente desde una perspectiva sectorial, es importante señalar que la protección de los datos personales constituye un derecho autónomo e independiente del derecho a la intimidad como lo ha establecido claramente el modelo europeo el cual ha sido adoptado progresivamente por numerosos países comprometidos con la garantía efectiva de este derecho (Garcia, 2017).

2.7.Marco Legal

a) Legislación Internacional

a. **California Consumer Privacy Act (CCPA):** Ley estatal de California sobre privacidad del consumidor.
b. **Ley federal de privacidad financiera (2021):** Mencionada como la más reciente aprobada a nivel
c. **Constitución Española:** Artículo 18.4: Garantiza el uso de la informática para proteger el honor e intimidad personal.
d. **Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD):** Ley Española basada en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.
e. **Agencia Española de Protección de Datos (AEPD):** Entidad reguladora que vela por el cumplimiento de la normativa de datos personales.
f. **Bundesdatenschutzgesetz (BDSG):** Alemania, ley Federal de Protección de Datos, adaptada al RGPD.
g. **CONDUSEF (Mexico):** Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. No es legislación, pero es una entidad importante en la protección del consumidor financiero.
h. **Financiero: El artículo 15:** Derecho a la intimidad y a la protección de datos personales; y el Defensor del Consumidor Financiero es una figura creada para representar los intereses de los consumidores en el sistema financiero.
i. **La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP):** Regula el tratamiento de datos personales por parte de entidades privadas. Establece principios como el consentimiento, la

finalidad y la proporcionalidad, y garantiza los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición.

j. **Reglamento General de Protección de Datos (RGPD):** Aunque no es un tratado, es el marco más influyente a nivel global en protección de datos pero España y Alemania están bajo este reglamento

k. **Principios de la OCDE sobre la Privacidad (1980, revisados en 2013):** Establecen principios rectores sobre la protección de la privacidad y flujos transfronterizos de datos personales y es referencia importante en países como México, Japón, Chile.

l. **Declaración Universal de los Derechos Humanos (1948):** En el artículo 12: Protege el derecho a la privacidad, sin embargo, no vinculante como tratado específico de datos, pero base del derecho internacional.

m. **Pacto Internacional de Derechos Civiles y Políticos (1966):** El artículo 17: Prohíbe injerencias arbitrarias en la vida privada o correspondencia y Perú es parte de ello.

n. Ley marco de ciberseguridad. Chile. Para ampliar la definición de ciberseguridad.

o. **Tribunal Constitucional Pleno.** Sentencia Nº 142/2018. España. Ofrece una definición sobre ciberseguridad.

p. **Unión Internacional de Telecomunicaciones.** Otorga una definición sobre ciberseguridad a nivel internacional.

b) Legislación Nacional

a. **Constitución política del Perú:** En su artículo 2 inciso 6, reconoce el derecho fundamental de toda persona a la privacidad, a la protección de sus datos personales y al secreto de sus comunicaciones.

b. **Código de Protección y Defensa del Consumidor:** Establece los derechos fundamentales de los consumidores peruanos, incluyendo el derecho a la información, la privacidad y la protección de sus datos personales.

c. **Ley de Protección de Datos Personales:** Establece principios como la legalidad, consentimiento, calidad, seguridad y finalidad, y garantiza derechos como el acceso, rectificación, cancelación y oposición (derechos ARCO), protegiendo así la intimidad y dignidad de las personas frente al uso indebido de su información.

d. **Decreto Supremo N.º 003-2013-JUS – Reglamento de la Ley N.º 29733:** Desarrolla y precisa cómo debe aplicarse la Ley de Protección de Datos y define conceptos como consentimiento, tratamiento, encargado, etc.
e. **Directiva de Seguridad de la Información – Directiva N.º 002-2020-JUS/DGTAIPD:** Es emitida por la Autoridad Nacional de Protección de Datos Personales y establece medidas mínimas de seguridad que deben aplicar quienes manejan bases de datos.
f. **Ley N° 30999 – Ley de Ciberseguridad (2019):** Es el marco normativo nacional para proteger el ciberespacio peruano; obliga a entidades públicas y privadas a adoptar medidas de seguridad digital.
g. **Política Nacional de Ciberseguridad (aprobada por DS N.º 112-2020-PCM):** Documento de planificación que establece los objetivos y estrategias del Estado peruano hasta 2030 para mejorar la ciberseguridad
h. **Decreto Legislativo N.º 1182 – Acceso a datos conservados por operadores de telecomunicaciones:** Regula el acceso por parte de la policía a los datos de geolocalización para combatir delitos, con implicancias sobre la privacidad.
i. **Ley N° 26702 – Ley General del Sistema Financiero y del Sistema de Seguros:** Regula la actividad bancaria, supervisión de la SBS, y deberes de protección al usuario financiero.
j. **Reglamento de Gestión de la Seguridad de la Información de las Empresas del Sistema Financiero:** Es emitido por la Superintendencia de Banca, Seguros y AFP (SBS) (Resolución SBS N.º 504-2021) y establece estándares mínimos de seguridad de la información y protección de datos en entidades financieras.
k. **Ley N°28587 – Ley Complementaria a la Ley de Protección al Consumidor:** Refuerza la protección de los consumidores frente a prácticas abusivas.
l. **Ley N° 27806 – Ley de Transparencia y Acceso a la Información Pública:** Tiene implicancia indirecta en el manejo de información de los ciudadanos por parte de las entidades públicas.
m. **Ley que modifica el decreto legislativo 1141**, decreto legislativo de fortalecimiento y modernización del sistema de inteligencia nacional - sina

y de la dirección nacional de inteligencia - dini, a fin de regular la seguridad digital.

n. **Tribunal Constitucional.** Sentencia del Tribunal Constitucional Exp N° 02140-2020-PDH/TC.
o. **Decreto de urgencia** que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento.
p. **Decreto legislativo** que crea la autoridad nacional de transparencia y acceso a la información pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses.
q. **Reglamento del decreto legislativo N° 1412**, decreto legislativo que aprueba la ley de gobierno digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
r. Ley de Delitos Informáticos. Ley para prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

CAPÍTULO III

MARCO METODOLÓGICO

3.1. Enfoque

La presente investigación adoptó un enfoque mixto, combinando métodos cuantitativos y cualitativos para abordar de manera integral los desafíos jurídicos relacionados con la ciberseguridad, la protección de datos personales y su impacto en el derecho a la privacidad en el sistema financiero peruano. Por otro lado, el enfoque cualitativo se aplicó para explorar las percepciones de los consumidores y expertos en derecho y ciberseguridad sobre la protección de datos y la ciberseguridad en el sistema financiero. Se realizaron entrevistas en profundidad y grupos focales con consumidores afectados y expertos del sector financiero, así como análisis de casos específicos de violaciones de datos y su impacto en los derechos de privacidad. Este enfoque permitió contextualizar los resultados cuantitativos y profundizar en los aspectos normativos y sociales relacionados con la implementación de las leyes y su efectividad en la práctica.

El enfoque cuantitativo se utilizó para medir la efectividad de la Ley N° 29733 y otras normativas vigentes, así como su impacto en la realidad peruana. A través de la recolección de datos estadísticos, se analizaron variables como el número de sanciones impuestas por incumplimiento de las leyes, la cantidad de denuncias por vulneración de datos, y la implementación de medidas de seguridad por parte de las entidades financieras. Las hipótesis se centraron en evaluar si la legislación actual está siendo efectiva en la protección de los datos personales y si existió una correlación entre el cumplimiento normativo y la reducción de ciberataques en el sector financiero.

De esta manera, el enfoque mixto proporcionó una comprensión completa de cómo la legislación y las políticas actuales abordan la protección de datos y la ciberseguridad, y cómo estos afectaron a los consumidores en su vida diaria.

3.2. Nivel

La investigación presenta un nivel descriptivo–explicativo, en tanto se orienta, por un lado, a identificar, sistematizar y caracterizar las principales brechas jurídicas existentes en materia de ciberseguridad dentro del sistema financiero peruano y su incidencia en el derecho a la privacidad del consumidor, delimitando los elementos normativos, institucionales y contextuales del problema; y, por otro lado, a explicar las causas jurídicas que originan dichas deficiencias, particularmente aquellas vinculadas a vacíos normativos,

insuficiencias regulatorias y desajustes entre el avance tecnológico y el marco legal vigente, estableciendo así una relación entre estas y sus efectos en la tutela del derecho fundamental a la privacidad, desde una perspectiva jurídico-dogmática. Se combinaron datos cuantitativos (como estadísticas de denuncias y sanciones) con datos cualitativos (entrevistas a profesionales del derecho y consumidores), lo que permitió analizar tanto los resultados objetivos de la implementación de las leyes como las experiencias y percepciones de los involucrados en este proceso.

3.3. Método

La presente investigación ha sido Mixta, Dogmática porque se centró en un análisis jurídico de las normas, principios, doctrina, jurisprudencia de todo aquello relacionado con la protección de datos personales y ciberseguridad con un derecho comparado, asimismo fue Empírica porque el presente estudio incluyó casos concretos, sanciones a entidades financieras y denuncias sobre dicha problemática, con aquellos datos se pretendió sustentar y contextualizar la problemática.

La combinación del enfoque cuantitativo y cualitativo permitió abordar de manera completa tanto los aspectos estadísticos como las dimensiones sociales y perceptuales del fenómeno estudiado. El método empírico, al fundamentarse en la observación de situaciones reales y casos específicos, se articuló adecuadamente con el enfoque cuantitativo, ya que proporciona datos que pueden ser sistematizados y analizados numéricamente para evaluar tendencias y niveles de cumplimiento normativo.

Por su parte, el método dogmático, centrado en el estudio de normas jurídicas, principios doctrinales y jurisprudencia, se complementó con el enfoque cualitativo, permitiendo una comprensión más profunda sobre la forma en que los principales actores involucrados (como los consumidores y expertos en la materia) perciben la efectividad de la legislación vigente. Esta integración también facilitó el análisis del contexto normativo y permitió identificar si dichas percepciones coinciden o se distancian de lo establecido por el marco legal actual.

3.4. Unidades de estudio

Las unidades de estudio se han compuesto de consumidores del sistema financiero peruano que utilizan servicios digitales, entidades financieras responsables de la

implementación de las leyes de protección de datos y ciberseguridad, y las normas legales relevantes (Ley N° 29733, Ley N° 30618, Ley N° 30096, entre otras). Se usaron datos cualitativos (entrevistas a profesionales del derecho y consumidores), lo que permitió analizar tanto los resultados objetivos de la implementación de las leyes como las experiencias y percepciones de los involucrados en este proceso.

3.5. Técnicas

Se empleó como técnica la observación y encuesta.

3.6. Instrumentos

Cómo instrumentos, se consideraron:

La guía de observación documental: Ley N° 29733 (Ley de protección de datos personales), Decreto supremo N° 003-2013-JUS (Reglamento de la Ley de protección de datos personales), Ley N° 30096 (Ley de delitos informáticos), Ley N° 30999 (Ley de ciberdefensa) Código penal Peruano, Reglamento General de protección de datos (RGPD-Unión Europea), Ley N° 29571 (Código de protección y Defensa del consumidor), Ley de Privacidad del consumidor de California (CCPA), Ley Modelo de protección de datos personales de la OEA 2015, Declaración de Derechos en Internet ONU 2016, Resolución Directoral N° 2196-2020-ANPDP, Capital One EE.UU 2022.

Se aplicaron dos encuestas estructuradas con preguntas cerradas, con la finalidad de obtener información complementaria sobre la percepción de los actores involucrados respecto a la ciberseguridad y la protección de datos personales en el sistema financiero. La primera encuesta fue dirigida a consumidores jóvenes entre 20 y 30 años, considerados usuarios frecuentes de servicios financieros digitales, con el propósito de identificar su nivel de conocimiento, prácticas y percepción sobre la seguridad de su información personal. La segunda encuesta estuvo dirigida a profesionales del Derecho con experiencia laboral relevante, a fin de recoger sus apreciaciones sobre el estado de la regulación y los principales problemas en la protección jurídica de los datos personales.

Cabe precisar que los resultados obtenidos a partir de estas encuestas, no constituyen fundamento principal para la determinación de las brechas jurídicas, sino que cumplen una función ilustrativa y complementaria dentro del análisis, el cual se sustenta prioritariamente en el estudio dogmático, normativo y comparado.

CAPÍTULO IV

RESULTADOS

4.1.Evidencia comparativa, normativa y empírica

4.1.1. Jurisprudencia

La presente investigación a través de sus múltiples citas y descripciones mediante diversas fuentes normativas y jurisprudenciales, tanto a escala nacional e internacional mediante la comparación con otros ordenamiento jurídicos, con la finalidad de determinar si el marco legislativo peruano, en lo que respecta a ciberseguridad y protección de datos personales, ha logrado cumplir de manera eficaz con las demandas de una economía digitalizada y de su sistema financiero que cada vez se encuentra más dependiente de los datos sensibles de sus usuarios.

Por consiguiente, el análisis comparativo de mencionada jurisprudencia y de los antecedentes doctrinales citados, evaluando en qué ámbitos estos pueden confirmar la hipótesis central de que la normativa peruana sea efectivamente insuficiente para satisfacer las necesidades actuales del sistema financiero, y que en efecto sea justificable lo imperativo de una regulación más extensa y su constante actualización.

Como se ha mencionado anteriormente, el Tribunal Constitucional peruano a través de la Sentencia 06534-2006-PA/TC, reconoció la protección de datos personales como un derecho fundamental, vinculado estrechamente con la dignidad y la autodeterminación informativa. En esta jurisprudencia se ha constituido que el Estado no solo tiene la obligatoriedad de avalar el acceso a la información, sino que además, también la de salvaguardar la privacidad de los ciudadanos frente a vulneraciones factibles por parte de terceros, incluidas dentro de esto las entidades financieras, no obstante, a pesar de esta exploración, la sentencia deja en evidencia que la normativa presente en ese momento no ha sido suficiente, y que su desarrollo en lo que respecta a este derecho ha sido particular y reactivo, cuando en primer lugar debería de haber sido preventivo.

De igual manera, las estadísticas de la SBS mencionadas en el documento, haciendo referencia a las 22 214 denuncias entre 2018 y 2022 por vulneración de datos, denotan que el marco normativo de la Ley Nº 29733 y su reglamento no ha sido correctamente diligente en lo que respecta a su aplicación, y tampoco eficiente por parte de las empresas del sector del sistema financiero peruano. La jurisprudencia administrativa de la ANPDP también evidencia, lastimosamente, un severo nivel de inobservancia como las

sanciones al BBVA por incumplimiento a la LPDP, o la filtración de Interbank, ambos son ejemplo que dejan en evidencia al marco legal, y como este no cuenta con mecanismos puntuales con el objetivo de prevenir y a su vez de responder frente a estas situaciones. Las resoluciones administrativas sancionadoras son de suma importancia, no obstante, su impacto real en el condicionamiento de los actores en el mercado es reducido, no necesariamente las multas cumplen con un efecto disuasivo respecto a la ventaja económica obtenible a través del uso incorrecto o indebido de datos.

Esta realidad muestra que, aunque el ordenamiento jurídico peruano admite formalmente el derecho a la protección de datos personales y la seguridad digital, su capacidad práctica es reducida. Las normas existen, pero adolecen de mecanismos técnicos y de supervisión continua, que fuerce a las entidades del sistema financiero a adquirir estándares sólidos respecto a la ciberseguridad y cumplimiento normativo, caso que sí acontece en otras jurisdicciones.

Las similitudes y diferencias con otros sistemas jurídicos, ya desarrollada en la tesis, es primordial para probar la insuficiencia de la legislación nacional. En la Unión Europea, el Reglamento General de Protección de Datos, o GDPR, y la jurisprudencia del Tribunal de Justicia de la Unión Europea han solidificado de manera significativa el derecho a la autodeterminación informativa. Sentencias como el caso Google Spain SL, Google INC. v Agencia Española de Protección de Datos, o AEPD, C-131/12 del 2014, instituyeron el ahora conocido “derecho al olvido” y la obligación de las empresas tecnológicas de respaldar mecanismos efectivos para la eliminación de datos personales, esta decisión proyecta un enfoque preventivo y que busca garantizar estos derechos, situación que no se ve reflejada aún en el Perú.

En España la Sentencia del Tribunal Constitucional 292/2000, ya citada en la tesis, proveyó a los titulares de datos no solo sus derechos de acceso y corrección, sino de igual manera la oportunidad de demandar responsabilidades frente a terceros que afecten dichos derechos. Aun teniendo en consideración la antigüedad de esta jurisprudencia, es posible rescatar su proactividad y expansión siendo más vanguardista que la legislación peruana reciente, que no se ha avocado a la necesaria responsabilidad civil así como el derecho a la indemnización efectiva en las situaciones en las cuales ocurre esta vulneración de datos dentro del sistema financiero.

Mientras tanto en Alemania, a través de la Ley Federal de Protección de Datos y su jurisprudencia del Tribunal Constitucional Federal, se ha formulado un alto patrón de protección que toma como base el concepto de "autodeterminación informativa" desde el caso del Censo de 1983. Este mismo viene a ser el estandarte referente frente a cualquier tratamiento de datos para que este sea oportuno, con limitaciones y diáfano. A su vez, en el Perú, si bien la LPDP contempla principios similares como el de finalidad, proporcionalidad y consentimiento, su aplicación en la realidad peruana es imperfecta y carece del mismo desarrollo que le ha dado la jurisprudencia.

En un diferente orden de ideas, en Estados Unidos, aunque no exista como tal una ley federal integral para todos los estados, la jurisprudencia alrededor de la Ley Gramm-Leach-Bliley y la California Consumer Privacy Act han sido prueba suficiente que incluso en este sistema jurídico funcional por sectores, los jueces han reforzado la urgencia de comunicar a los consumidores frente a cualquier divulgación de sus datos sin previo consentimiento, así como para otorgar responsabilidades evidentes para las empresas. Si bien en el Perú han existido estos casos de divulgación de datos, la obligación de notificación no llega a la amplitud necesaria ni a los protocolos legislativos precisos para poder salvaguardar la reparación de los daños.

Queda en evidencia entonces mediante la comparación jurisprudencial internacional, que el Perú se encuentra con un desarrollo sumamente lento frente a estándares internacionales e inclusive regionales, todo esto en conjunto justifica que la legislación actual no es suficiente y debe ser complementada y suplida con disposiciones más específicas y que satisfagan las necesidades modernas.

La LPDP, el marco que ofrece la SBS y la Ley de Delitos Informáticos son progresos significativos, no obstante demuestran situaciones problemáticas en cuanto a su estructura que han sido identificados en la tesis y confirmados por la jurisprudencia, como la falta de mecanismos para la prevención y educación en la materia, el sector mayoritario de normas se han enfocado directamente en la sanción después del acto, lo cual no trae perjuicio por sí mismo, el problema radica en la inexistencia de programas nacionales concluyentes respecto a la formación en ciberseguridad para todos los consumidores, así como sobre sus obligaciones respecto a sus proveedores financieros y sus auditorías periódicas para con sus sistemas. Otro problema estructural que se evidencia es la carencia respecto de la especialización técnica en lo judicial y administrativo, a pesar de que dentro

del ordenamiento jurídico viven los procedimientos sancionadores, la jurisprudencia nacional ha demostrado que estas penalizaciones llegan tarde y en una gran cantidad de situaciones no generan precedentes vinculantes y al no existir tribunales especializados sobre la materia de ciberseguridad y datos personales, lo cual termina provocando inseguridad jurídica y poca similitud en este tema. Por consiguiente el último problema estructural viene a ser los vacíos normativos frente al raudo avance tecnológico, como lo indica la doctrina, la legislación nacional no ha considerado fenómenos revolucionarios actuales como la inteligencia artificial, el Big Data o la toma de decisiones por automatización, mientras tanto en la jurisprudencia extranjera esta se proyecta hacia la protección de datos frente a la discriminación algorítmica y la utilización de estos sin fines que hayan sido consentidos, cuando en Perú todavía no se regula este aspecto.

La evidencia mostrada en la tesis, así como la jurisprudencia analizada, permite colegir que sí existe una urgencia de una legislación más extensa y moderna en el Perú, principalmente por la tendencia global que busca mayores estándares, la comparación con las legislaciones europeas y norteamericanas denotan que los países más avanzados han insertado marcos más completos y que responden a la actualidad, para poder ingresar en la economía digital y ofertarse hacia la inversión extranjera, mientras que el Perú necesita ajustar y alinear su regulación bajo estos estándares, asimismo la protección efectiva de los consumidores debe ser prioridad, los casos de filtración de información y las sanciones a los bancos apuntan a que los consumidores peruanos se encuentran en una situación real de desprotección, sin contar con los organismos o medidas eficaces para su correcto control, regulación, sanción y reparación si correspondiere, se vulnera el derecho constitucional a la intimidad y autodeterminación informativa. Aunado a ello existe la obligación internacional, como miembro de organizaciones internacionales y compromisos adquiridos con la OCDE, el Perú se encuentra en la obligación de realizar una correcta adecuación al respecto de su legislación para ceñirse a estándares internacionales de protección de datos y ciberseguridad que han demostrado ser más rigurosos.

Por todo lo expresado en la revisión de jurisprudencia citada y su comparación con el derecho extranjero se confirma la hipótesis planteada, la legislación peruana en materia de ciberseguridad y protección de datos personales es insatisfactoria e insuficiente para garantizar y salvaguardar los derechos de los consumidores en el sistema financiero digital frente a las incipientes amenazas que van creciendo a pasos agigantados, la jurisprudencia

nacional reconoce el derecho, pero su eficiencia en la realidad peruana es reducida, en cambio la jurisprudencia comparada otorga ejemplos de legislaciones más protectores y que cumplen sus objetivos de manera puntual, es por lo mencionado anteriormente que el legislador peruano debe acelerar una reforma integral de la LPDP y sus normas relacionadas que se enfoque en la debida notificación respecto de divulgación de datos personales no consentida y ciberataques, mayores facultades a la ANPDP para realizar sus debidas auditorías así como sancionar de manera preventiva, aumentar el desarrollo jurisprudencial y la posibilidad de un tribunal especializado, incrementar la regulación específicamente sobre la IA y el Big Data y finalmente abordar la educación y concientización hacia la ciudadanía sobre la ciberseguridad y la importancia de la misma, a través de una legislación más amplia y eficaz se podrá garantizar una protección real frente a las nuevas amenazas dentro del sistema financiero digital, en el cual el derecho fundamental a la privacidad se ve cada vez más intimidado y vulnerable.

4.1.2. Doctrina

El desarrollo teórico presentado en la tesis ofrece múltiples visiones sobre la situación de la protección de datos y la ciberseguridad en Perú y en el mundo. Los diferentes autores mencionados abordan desde distintos puntos de vista el tema de la violación de datos en el sector financiero y sus efectos en el derecho a la privacidad de los consumidores. A continuación, se analiza la doctrina empleada en esta investigación, llevando a cabo una comparación crítica y una evaluación acerca de si realmente pone de manifiesto la carencia de normas adecuadas y la necesidad de contar con un marco legal más amplio y actualizado.

Al respecto de la doctrina nacional, el reconocimiento del problema y sus limitaciones recae, según varios autores peruanos citados en el texto, en la debilidad estructural de los consumidores ante el manejo incorrecto de sus datos por parte de las instituciones financieras. Alvarado (2016) afirma que la protección de la información es un principio clave de la LPDP, estableciendo que tanto los titulares como los responsables de los bancos de datos tienen el deber de asegurar la protección y el correcto manejo de esta información. No obstante, en la práctica, como se demuestra en la tesis y en los casos discutidos (filtraciones en Interbank y sanciones al BBVA), este principio es vulnerado por la carencia de mecanismos coercitivos y de una supervisión efectiva.

De manera similar, Flores (2021) examina la falta de especificidad en el Código de Protección y Defensa del Consumidor, comentando que el legislador no anticipó el avance tecnológico ni la magnitud de los crímenes cibernéticos, resultando en un marco normativo poco adaptable. Esta opinión doctrinal refuerza la noción de que las normas actuales no han evolucionado al mismo ritmo que la tecnología, dejando a los consumidores vulnerables frente a nuevas modalidades de fraude y violaciones de datos.

Asimismo, Gonzales et al. (2024) enfatizan la necesidad de que los datos sean verídicos, precisos y completos, así como la existencia de vías legales rápidas para corregir información errónea. Sin embargo, también coinciden en que, en la práctica, estas garantías son difíciles de llevar a cabo debido a la falta de protocolos claros en el sistema financiero. Esto revela una discrepancia entre la normativa y su implementación real, un aspecto recurrente señalado por varios autores.

Finalmente, autores como Dávalos y Mujica (2022) y Escobar (2022) exploran la dimensión social de la violación de datos, como la pérdida de confianza de los consumidores en el sistema financiero y la falta de un consentimiento informado efectivo. Escobar enfatiza la carencia de un procedimiento unificado y consolidado para la protección de datos en Perú, lo que fortalece la hipótesis de la tesis acerca de la insuficiencia normativa.

La doctrina nacional admite el problema, señala los vacíos en la normativa y sugiere que las leyes actuales, aunque sean necesarias, son insuficientes para enfrentar los retos de hoy frente a los estándares comparados y mejores prácticas, el estudio doctrinal no se restringe solo al ámbito nacional, sino que también integra valiosas perspectivas de carácter internacional. Por ejemplo, Olivos (2019) examina de qué manera diversas naciones han implementado regulaciones específicas frente a la invasión de la privacidad, subrayando la relevancia de la privacidad como un valor en la sociedad digital. Su análisis crítico señala la falta de una normativa robusta en Perú para abordar estas amenazas.

En cuanto a Quezada (2019) y Cueto (2019), ambos analizan, desde una perspectiva comparativa, las dificultades que enfrenta el derecho ante el avance de la tecnología. Quezada pone de manifiesto la debilidad de las normativas en Chile y otros países, destacando que la legislación comúnmente responde de manera tardía a los avances tecnológicos, lo que se asemeja a la situación en Perú. Cueto, por su parte, estudia el efecto del Big Data en el sector financiero, enfatizando la urgencia de contar con sistemas

adecuados para proteger los datos. Ambas perspectivas doctrinales son significativas ya que indican que el problema no es exclusivo de Perú, sino que tiene un carácter regional, lo que sugiere que se requieren reformas legislativas proactivas.

Otros autores mencionados, como Mubarak (2017) y Morales (2021), se enfocan en el consentimiento y los desafíos que presenta la inteligencia artificial para la protección de datos. Mubarak afirma que el consentimiento es fundamental para la protección de datos, pero este debe ser claro y consciente, algo que en la práctica no siempre ocurre en Perú. Morales alerta sobre los retos sin precedentes que plantea la IA, tales como el uso de datos sin el conocimiento previo de los propietarios y los sesgos presentes en los algoritmos. Estos análisis doctrinales evidencian que la legislación en Perú no aborda de manera adecuada los fenómenos emergentes. Finalmente, Gunn (2008) y Aftergood (2017) subrayan la ciberseguridad como una cuestión estratégica que se puede comparar con amenazas globales como el terrorismo o las armas de destrucción masiva. A pesar de que estos autores se enfocan en un contexto internacional, su visión refuerza la necesidad de priorizar la ciberseguridad en Perú.

Al hacer un análisis comparativo de toda la doctrina mencionada en la tesis, se observa una convergencia en varios aspectos esenciales, primero las lagunas normativas en la LPDP y legislaciones relacionadas, los autores están de acuerdo en que la norma vigente no se adapta adecuadamente al crecimiento tecnológico (Flores, 2021; Quezada, 2019), ni proporciona herramientas eficientes para prevenir y reparar (Escobar, 2022).

Sobre la ausencia de formación y cultura en ciberseguridad, autores como Mubarak, Dávalos y Mujica coinciden en la relevancia de educar e informar al consumidor, algo que no está asegurado de manera constante por la normativa. Al respecto de la urgencia de una regulación proactiva, la doctrina de otros países (Olivos, Cueto, Morales) demuestra que las mejores prácticas internacionales incluyen medidas preventivas, obligaciones de transparencia y auditorías, así como regulaciones específicas para nuevas tecnologías, aspectos que son inexistentes en la normativa peruana.

El estudio doctrinal presentado en la tesis efectivamente indica que las leyes en Perú son inadecuadas. A pesar de que la LPDP, la Ley de Delitos Informáticos y otras regulaciones han mostrado progreso, la doctrina resalta la falta de implementación real de las normativas vigentes (Alvarado, Gonzales et al.), la ausencia de mecanismos preventivos y punitivos que tengan un efecto disuasorio real (Escobar), la regulación

insuficiente de las nuevas tecnologías y fenómenos digitales (Morales, Mubarak), la falta en educación y concienciación (Dávalos y Mujica).

Además, la doctrina comparativa revela que naciones con marcos legales más extensos (como los europeos con el GDPR) han alcanzado una mejor protección de los derechos de los consumidores, sugiriendo que Perú debería seguir ese rumbo.

Al respeto de la necesidad de una legislación más completa la doctrina estudiada proporciona argumentos contundentes que respaldan la necesidad de una legislación más extensa y actualizada en Perú, primero la conformidad con estándares internacionales para cumplir con compromisos globales y atraer inversiones, Perú debería sincronizar su normativa con los estándares del GDPR y las prácticas internacionales más efectivas (Olivos, Quezada). Luego en lo que respecta a protección auténtica de los consumidores la doctrina expone que las filtraciones y el mal uso de datos generan desconfianza y afectan derechos fundamentales. Es necesaria una regulación más precisa, con obligaciones definidas y sanciones adecuadas. Además de la adaptación a nuevas tecnologías, los autores como Morales y Mubarak enfatizan la importancia de regular la inteligencia artificial, el Big Data y la toma de decisiones automatizadas, aspectos que no están contemplados en la legislación peruana vigente y finalmente el fortalecimiento institucional, como Escobar y Flores recalcan la importancia de establecer una autoridad reguladora que cuente con mayores poderes y recursos para realizar auditorías y aplicar sanciones de manera efectiva.

Es por lo expuesto que la totalidad de la doctrina mencionada en la tesis evidencia de manera clara que la legislación peruana en el ámbito de ciberseguridad y protección de datos es insatisfactoria e insuficiente. La doctrina no solo identifica los problemas existentes, sino que también propone directrices para la mejora legislativa, una mayor especificidad en las normas, capacitación en ciberseguridad, adaptación a nuevas tecnologías y fortalecimiento de las instituciones responsables de la protección de datos.

La demanda de una legislación más integral no es opcional, sino una necesidad derivada de los desafíos tecnológicos, económicos y sociales actuales. Perú debe aprender de las experiencias comparativas y de la crítica doctrinal para actualizar su marco legal y asegurar efectivamente el derecho fundamental a la privacidad y la seguridad de los consumidores en el ámbito financiero digital.

4.1.3. Resultado de consumidores

En otro apartado, se realizaron encuestas tanto a nivel de consumidores como de profesionales que llevan años de experiencia en el campo laboral, donde en un principio se esperaba encontrar una sociedad sin mucha información al respecto o mecanismos poco claros sobre cómo proceder frente a la vulneración de sus derechos, en la encuesta realizada a los consumidores donde el 96.4% poseen educación universitaria se demostró que, si bien en su totalidad conocen el concepto de dato personal y consideran en su mayoría que el sistema financiero, a través de sus entidades como bancos o financieras deben proteger sus datos personales.

Tabla 1

¿Sabes que es un dato personal?

	Frecuencia	Porcentaje
Sí	51	100%
Total	51	100%

Nota. Elaboración propia. 2025

De la tabla anterior, el resultado muestra que el 100% de los encuestados conocen la definición de un dato personal, lo que evidencia un nivel uniforme en cuanto a la compresión sobre dicha definición en torno a la protección de la información. Este hallazgo resulta positivo en cuanto a que representa un punto de partida relevante para el ejercicio de sus derechos en materia de privacidad y seguridad digital.

Tabla 2

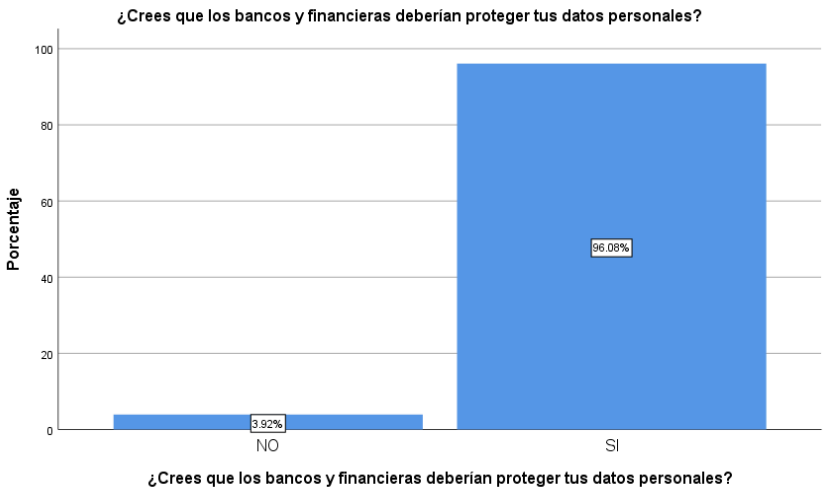
¿Crees que los bancos y financieras deberían proteger tus datos personales?

	Frecuencia	Porcentaje
NO	2	3.9
SI	49	96.1
Total	51	100.0

Nota: Elaboración propia. 2025

Figura 1

¿Crees que los bancos y financieras deberían proteger tus datos personales?



Nota: Elaboración propia. 2025

De la tabla y figura anterior, los resultados reflejan que el 96.1% de los encuestados consideran que los bancos y entidades financieras tienen la obligación de proteger los datos personales, lo que demuestra una obligación generalizada de que dichas instituciones financieras deben asumir una obligación en cuanto a la tutela de derechos. Por el contraste, un 3.9% manifestó lo contrario, sin embargo, se presenta una mayoría sobre la responsabilidad recaída en el sistema financiero en cuanto a la gestión segura y adecuación de la información personal.

Tabla 3

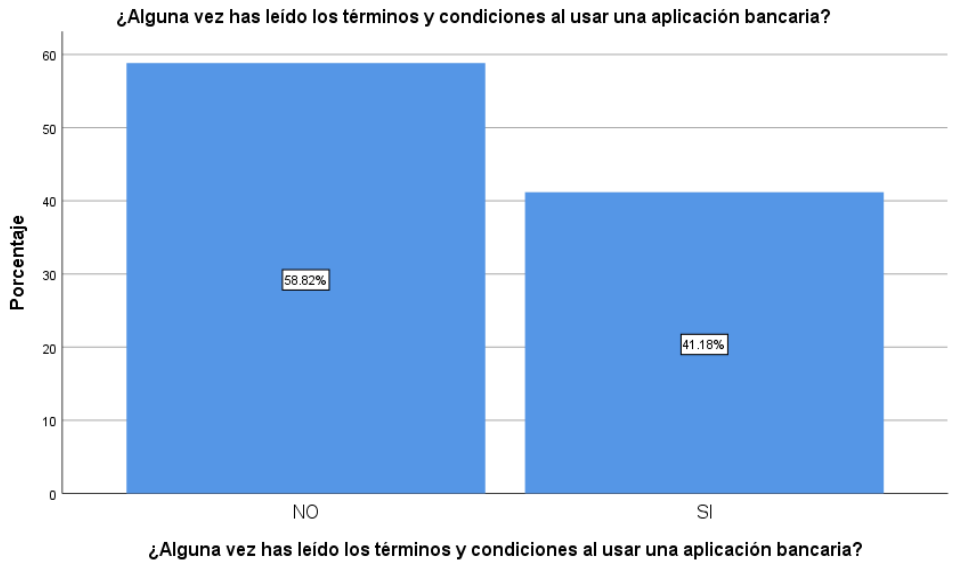
¿Alguna vez has leído los términos y condiciones al usar una aplicación bancaria?

	Frecuencia	Porcentaje
NO	30	58.8
SI	21	41.2
Total	51	100.0

Nota: Elaboración propia. 2025

Figura 2

¿ Alguna vez has leído los términos y condiciones al usar una aplicación bancaria?



Nota: Elaboración propia. 2025

De la tabla y figura anterior solo el 58.8% ha leído los términos y condiciones de los aplicativos bancarios, mientras que el 41.1% no lo ha hecho, lo cual es preocupante porque la mayoría de ellos ya son profesionales y son claro reflejo de cómo se encuentra esta parte de la sociedad. Asimismo, se revela una marcada tendencia a la aceptación de contratos de adhesión sin una lectura previa, lo que refuerza la problemática de la asimetría de la información entre consumidor y las instituciones financieras, debilitando así el consentimiento informado y colocando al consumidor en una posición de vulnerabilidad.

Tabla 4

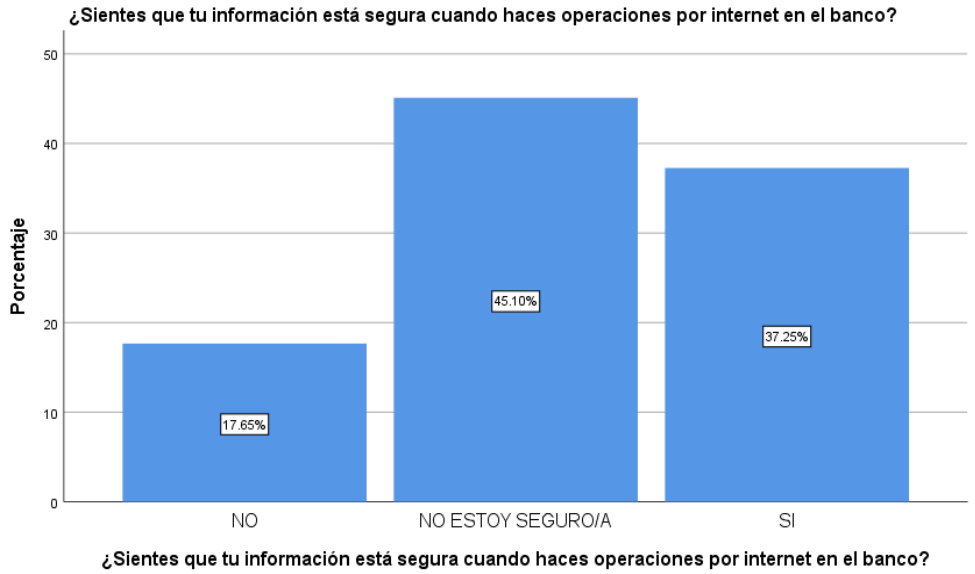
¿Sientes que tu información está segura cuando haces operaciones por internet en el banco?

	Frecuencia	Porcentaje
No	9	17.6
No estoy seguro/a	23	45.1
Sí	19	37.3
Total	51	100.0

Nota: Elaboración propia. 2025

Figura 3

¿Sientes que tu información está segura cuando haces operaciones por internet en el banco?



Nota: Elaboración propia. 2025

De la tabla y figura anterior, se indica que sólo el 37.3% de los encuestados se sienten seguros de realizar una operación bancaria en línea, mientras que por el contrario, el 45.1% señaló no estar seguro y un 17.6% afirmó no sentirse seguro. Todo ello refleja la desconfianza en la seguridad bancaria digital, evidenciando la percepción masiva de vulnerabilidad de los usuarios frente a estos servicios o mecanismos digitales ante posibles riesgos de fraude o filtración de datos personales. Por lo que se revela la necesidad de fortalecer las medidas de protección implementadas por las instituciones financieras como transparencia a los consumidores para generar confianza en estos servicios.

Tabla 5

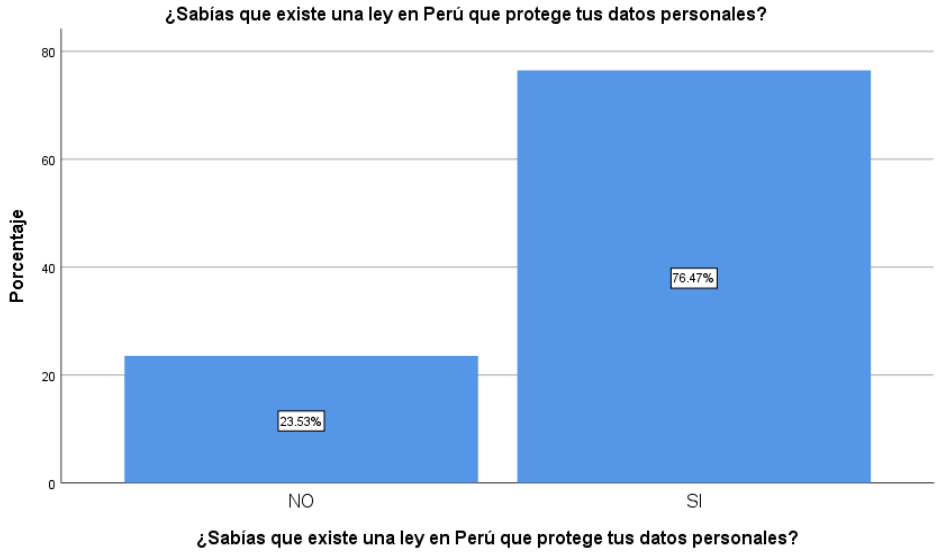
¿Sabías que existe una ley en Perú que protege tus datos personales?

	Frecuencia	Porcentaje
NO	12	23.5
SI	39	76.5
Total	51	100.0

Nota. Elaboración propia. 2025

Figura 4

¿Sabías que existe una ley en Perú que protege tus datos personales?



Nota. Elaboración propia. 2025

De la tabla y figura anterior se tiene que un 76.5% conoce la existencia de una ley para proteger los datos personales en Perú, lo cual, si bien es un avance significativo, deja en evidencia que el 23.5% restante no tiene conocimiento sobre la existencia de una ley que les faculte para proteger sus datos personales frente a las amenazas existentes.

Tabla 7

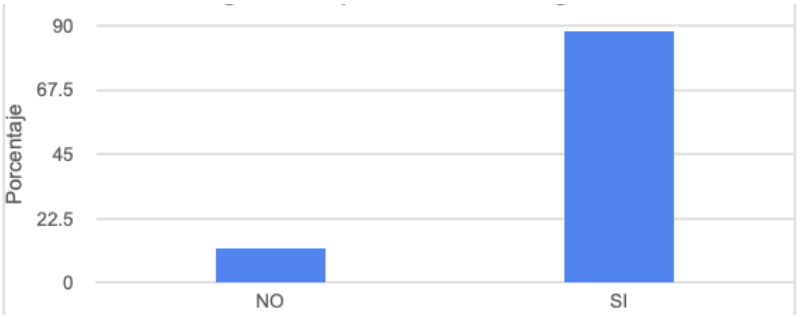
¿Sabes qué es la ciberseguridad?

	Frecuencia	Porcentaje
No	6	11.8
Sí	45	88.2
Total	51	100.0

Nota. Elaboración propia. 2025.

Figura 6

¿Sabes qué es la ciberseguridad?



Nota. Elaboración propia. 2025.

Tanto de la tabla como de la figura anterior se tiene que un 89.3% ha considerado que tiene conocimiento sobre el término ciberseguridad, y en consecuencia un 11.8% no tiene pleno conocimiento al respecto.

Tabla 8

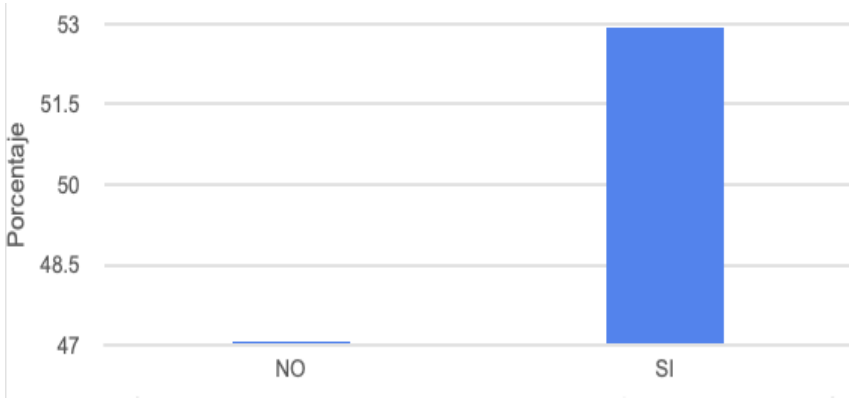
¿Sabes que puedes pedir al banco que te diga qué datos tiene sobre ti?

	Frecuencia	Porcentaje
No	24	47.1
Sí	27	52.9
Total	51	100.0

Nota. Elaboración propia. 2025.

Figura 7

¿Sabes que puedes pedir al banco que te diga qué datos tiene sobre ti?



Nota. Elaboración propia. 2025.

De la tabla y figura anterior se denota que solo un 52.9% sabe que tiene la potestad de solicitar a entidades financieras la información que estas tengan sobre los consumidores, y aunque una gran mayoría reporta no haber tenido problemas con el mal uso de su información por parte de empresas del sistema financiero, hay individuos que tienen conocimiento sobre las filtraciones de datos, y un sector ha presentado reclamos por la insistencia que presentan estas entidades con las llamadas telefónicas cuando los consumidores no han dado su información personal como el número telefónico ni su consentimiento para recibir este tipo de llamadas, lo cual ya constituye un mal uso de su información en primera instancia, no obstante eso deja en evidencia que el 47.1% no tiene conocimiento sobre esto y por lo tanto este sector se encuentra en una situación de mayor vulnerabilidad e incertidumbre porque no se puede proteger lo que se desconoce.

Tabla 9

¿Ha tenido alguna vez un problema con un banco por mal uso de su información?

	Frecuencia	Porcentaje
Gastos no reconocidos, reclamo, respuesta satisfactoria.	1	2.0
Mi información va a empresas terceras y luego estas me llaman a cada rato	1	2.0
No	46	90.2
Reclame	1	2.0
Si, simplemente levanté un reclamo puesto que varias entidades llamaban de forma constante a mi número	1	2.0
Sí, una vez tuve un problema porque usaron mi información y aparecieron compras que yo no hice. Llamé al banco, bloquearon mi tarjeta y me ayudaron a solucionarlo. Desde ahí tengo más cuidado con mis datos y dónde los pongo.	1	2.0
Total	51	100.0

Nota: Elaboración propia. 2025

De la tabla anterior, por otro lado si bien un 90.2% de los entrevistados menciona que no ha tenido un problema con las entidades financieras como los bancos, esto no necesariamente indica que el problema sea inexistente o irrelevante, han habido una gran

cantidad de filtraciones a lo largo de los últimos 5 años, y si bien las entidades financieras puedan contar con algunos protocolos de contingencia, es deber del Estado salvaguardar esa información sensible mediante mecanismos y sistemas funcionales antes de que ocurra una filtración como método preventivo y no exclusivamente como un método resarcitorio del daño.

Tabla 10

¿Te gustaría recibir más información por parte del Estado o empresas del sistema financiero sobre cómo proteger tus datos?

	Frecuencia	Porcentaje
Sí	51	100.0
Total	51	100.0

Nota. Elaboración propia. 2025.

De la tabla anterior se puede rescatar que el sector de consumidores, un 100% de los entrevistados estarían de acuerdo en recibir más información sobre cómo proteger sus datos ya sea por parte del Estado o por empresas del sector financiero, esto denota un profundo interés no sólo en poseer más información sino también en la voluntad de querer realizar un cambio relevante.

4.1.4. Resultado de profesionales

Tabla 11

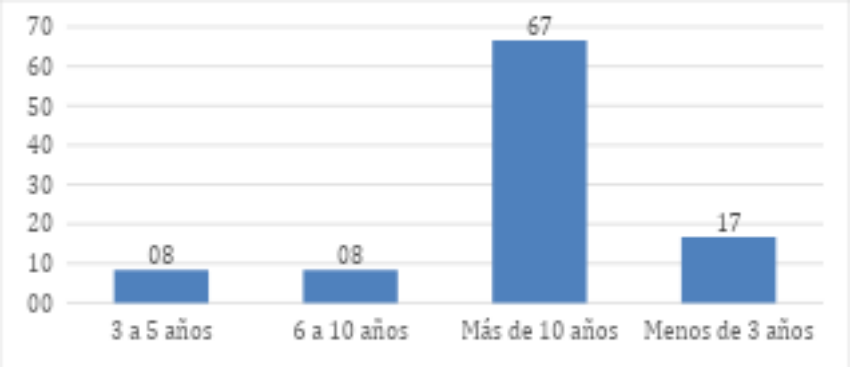
¿Cuántos años de experiencia tiene en su sector?

	Frecuencia	Porcentaje
3 a 5 años	1	8,3
6 a 10 años	1	8,3
Más de 10 años	8	66,7
Menos de 3 años	2	16,7
Total	12	100,0

Nota: Elaboración propia. 2025

Figura 8

¿Cuántos años de experiencia tiene en su sector?



Nota: Elaboración propia. 2025

De la tabla y figura anterior, respecto a la encuesta realizada a profesionales con amplia experiencia en el derecho, un 66.7% tienen más de 10 años de experiencia en su sector en áreas de ciberseguridad, derecho financiero, derecho de protección al consumidor, privacidad y protección de datos, derecho administrativo, civil, entre otros. Para este grupo se les cuestionó sobre cuál consideraban que era el principal riesgo cibernético en el sistema financiero peruano, donde un 33.3% respondieron que el fraude electrónico y el robo de credenciales, un 25% consideró las fugas o filtraciones de datos sensibles de los clientes y otro 25% siente que es un tema de ingeniería social, es decir suplantación de identidad, llamadas falsas de teléfono, etc.

Tabla 12

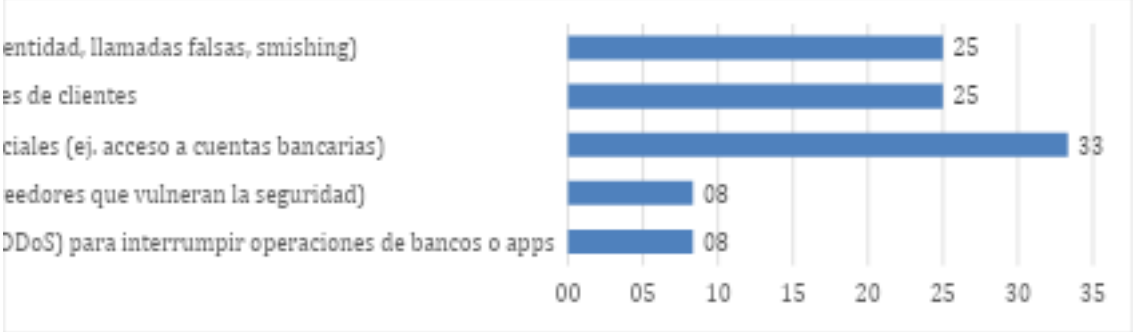
¿Cuál considera que es el principal riesgo cibernético en el sistema financiero peruano?

	Frecuencia	Porcentaje
Ataques de denegación de servicio (DDoS) para interrumpir operaciones de bancos o apps	1	8,3
Ataques internos (empleados o proveedores que vulneran la seguridad)	1	8,3
Fraude electrónico y robo de credenciales (ej. acceso a cuentas bancarias)	4	33,3
Fugas o filtraciones de datos sensibles de clientes	3	25,0
Ingeniería social (suplantación de identidad, llamadas falsas, smishing)	3	25,0
Total	12	100,0

Nota: Elaboración propia. 2025

Figura 9

¿Cuál considera que es el principal riesgo cibernético en el sistema financiero peruano?



Nota: Elaboración propia. 2025

De la tabla y figura anterior, se muestra que el 33.3 % de los expertos encuestados identificó el fraude electrónico y el robo de credenciales (como el acceso indebido a cuentas bancarias), como el principal riesgo cibernético en el sistema financiero peruano. A ello se suma que un 25% señaló como amenaza prioritaria las fugas o filtraciones de datos sensibles de clientes y otro 25% destacó la ingeniería social, como la suplantación de identidad o llamadas falsas, estas prácticas que aprovechan la falta de cultura digital en la sociedad. Por otro lado, un 8.3 % mencionó los ataques de denegación de servicio (DDoS)

y otro 8.3 % los ataques internos cometidos por empleados o proveedores. Todo esta interpretación nos evidencia que los encuestados perciben al fraude electrónico y a la pérdida de datos sensibles como los riesgos más graves, lo que coincide con las amenazas más frecuentes reportadas en el sector financiero no solo a nivel nacional, de esta manera se ve reflejado la necesidad de reforzar tanto la seguridad tecnológica como la captación de los consumidores.

Tabla 13

¿Cree que las entidades financieras peruanas cuentan con protocolos de ciberseguridad suficientes para proteger los datos de sus clientes?

	Frecuencia	Porcentaje
No	3	25,0
Parcialmente	9	75,0
Total	12	100,0

Nota: Elaboración propia. 2025

Figura 10

¿Cree que las entidades financieras peruanas cuentan con protocolos de ciberseguridad suficientes para proteger los datos de sus clientes?



Nota: Elaboración propia. 2025

De la tabla y figura anterior, los expertos coincidieron en señalar que los protocolos de ciberseguridad implementados por las entidades financieras peruanas resultan insuficientes. El 75% consideró que estos mecanismos son parcialmente suficientes para proteger los datos de los consumidores, mientras que por el contrario el 25% afirmó que no

se cumple con los estándares necesarios. Sin embargo, ninguno de los expertos señaló que estos protocolos fueran completamente suficientes. Esta percepción se vincula con la falta de un marco normativo que sea robusto y actualizado.

Tabla 14

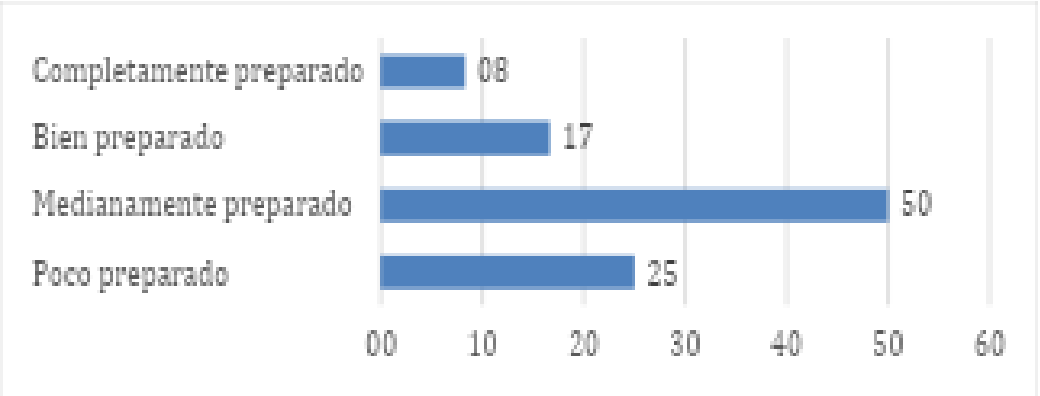
¿Qué tan preparado considera al sistema financiero peruano para responder ante un ciberataque masivo?

	Frecuencia	Porcentaje
Poco preparado	3	25,0
Medianamente preparado	6	50,0
Bien preparado	2	16,7
Completamente preparado	1	8,3
Total	12	100,0

Nota: Elaboración propia. 2025

Figura 11

¿ Qué tan preparado considera al sistema financiero peruano para responder ante un ciberataque masivo?



Nota: Elaboración propia. 2025

De la tabla y figura anterior, según la valoración de los expertos, el sistema financiero peruano contempla un nivel limitado en cuanto a la preparación para enfrentar un ciberataque masivo. el 50% califica como medianamente preparado, mientras que un 25% lo considera como poco preparado. Solo un 17 % lo percibe como bien preparado y apenas un 8% lo identifica como completamente preparado. Todos estos resultados reflejan

una apreciación crítica, donde algunos expertos reconocen la existencia de avances en infraestructura digital, pero la insuficiencia en cuanto a la capacidad de respuesta ante un ataque masivo. Esta percepción de los expertos coincide con las observaciones de la fragmentación institucional de nuestras leyes, donde las competencias dispersas entre varias instituciones dificultan una respuesta coordinada.

Tabla 15

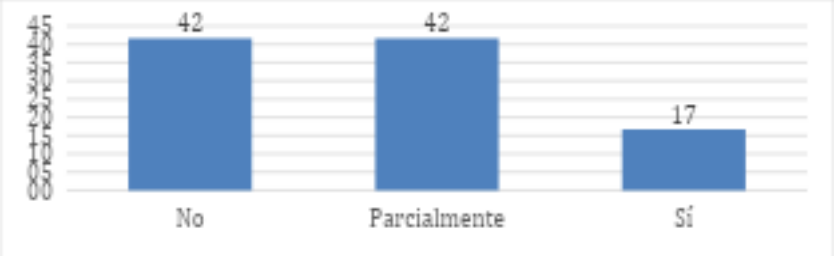
¿La legislación peruana actual es suficiente para enfrentar los desafíos de ciberseguridad en el sistema financiero?

	Frecuencia	Porcentaje
No	5	41,7
Parcialmente	5	41,7
Sí	2	16,7
Total	12	100,0

Nota: Elaboración propia. 2025

Figura 12

¿La legislación peruana actual es suficiente para enfrentar los desafíos de ciberseguridad en el sistema financiero?



Nota: Elaboración propia. 2025

De la tabla y figura anterior, los resultados evidencian que la mayoría de los expertos consideran insuficiente a la normativa peruana para enfrentar los desafíos de ciberseguridad en el sistema financiero. El 42% afirmó que la legislación no es suficiente, mientras que el otro 42% sostuvo que lo es parcialmente, pero únicamente el 17% indicó que efectivamente, lo es. Esto revelaría un consenso crítico sobre las limitaciones de la Ley N° 29733 la cual, hoy resulta no ser suficiente frente a las amenazas digitales que cada

vez son más sofisticadas. estas valorizaciones coinciden con lo señalado por Bermudez (2024) quien sostiene que la implementación de la norma es ineficaz.

Tabla 16

¿Qué normativa considera más relevante en la protección de los datos frente a ciberataques?

	Frecuencia	Porcentaje
Código de Defensa de Consumidor	1	8,3
Ley de Protección de Datos Personales (Ley 29733)	5	41,7
Ley de Protección de Datos Personales (Ley 29733), Código de Defensa de Consumidor	1	8,3
Ley de Protección de Datos Personales (Ley 29733), Normas internacionales (ISO, NIST, GDPR adaptada)	1	8,3
Ley de Protección de Datos Personales (Ley 29733), Normativa de la SBS (Superintendencia de Banca, Seguros y AFP), Por aplicación supletoria debería ser el Código Civil y por aplicación directa la Constitución.	1	8,3
Normativa de la SBS (Superintendencia de Banca, Seguros y AFP), Código de Defensa de Consumidor	2	16,7
Todas las anteriores	1	8,3
Total	12	100,0

Nota: Elaboración propia. 2025

De la tabla anterior, los resultados muestran que la Ley N° 29733 fue considerada por el 41.7% de los expertos como la normativa más relevante en cuanto a la protección frente a los ciberataques, los que confirman el rol central de la regularización de la privacidad en nuestro marco normativo. Sin embargo, el 16.7% señaló a la SBS junto con el código de defensa del consumidor como instrumentos igualmente importantes frente a la protección de estos derechos. Asimismo, algunos expertos (8.3%) calificaron a la combinación de la Ley N° 29733 con el código de defensa del consumidor, otros la aplicación complementaria de normas internacionales (ISO, NIST y el GDPR) y por último un 8.3% sostuvo que todas las normativas anteriormente señaladas deberían de aplicarse conjuntamente, evidenciando que algunos tienen una visión integral de la norma.

Tabla 17

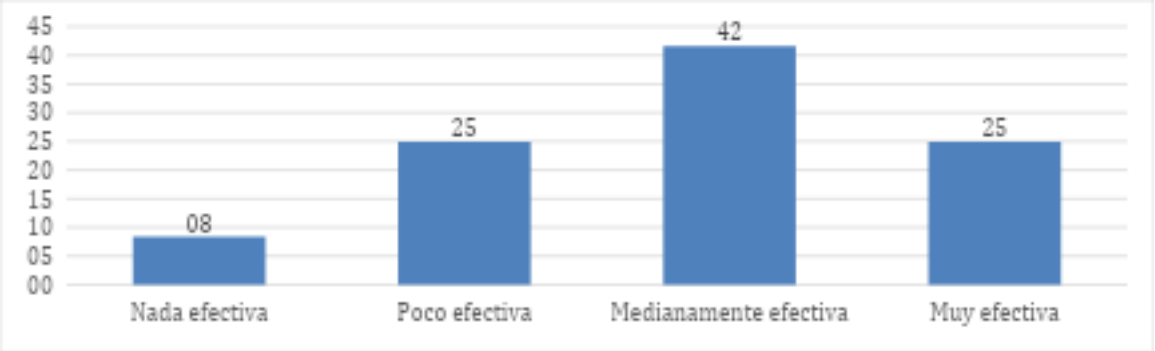
¿Qué tan efectiva considera la supervisión de la SBS en la protección de la privacidad del consumidor ante incidentes de ciberseguridad?

	Frecuencia	Porcentaje
Nada efectiva	1	8,3
Poco efectiva	3	25,0
Medianamente efectiva	5	41,7
Muy efectiva	3	25,0
Total	12	100,0

Nota: Elaboración propia. 2025

Figura 13

¿ Qué tan efectiva considera la supervisión de la SBS en la protección de la privacidad del consumidor ante incidentes de ciberseguridad?



Nota: Elaboración propia. 2025

De la tabla y figura anterior un 66.7% considera efectiva la supervisión de la SBS en la protección de la privacidad del consumidor ante incidentes de ciberseguridad al menos dentro de un espectro que va de efectiva y medianamente efectiva, y solamente un 8.3% considera que no es efectiva en su totalidad, mientras que un 25% ve que es poco efectiva, no obstante y en ese mismo orden de ideas el 75% considera que entidades financieras tienen un respeto pleno por la privacidad del consumidor de manera parcial, es decir que no se consideran respetados a plenitud ni lo consideran como una falta plena al respeto de la privacidad del consumidor, mientras que un 16.7% consideran que no respeta la privacidad del cliente a plenitud, lo cual denota cuanto menos una incertidumbre al

respecto si es que no la antes mencionada falta de confianza en el sector financiero al vincularse con lo digital.

Tabla 18

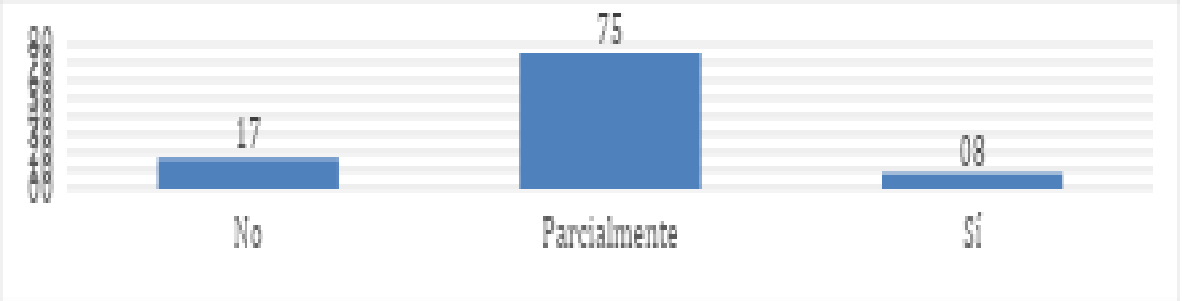
¿Las medidas de ciberseguridad implementadas por las entidades financieras respetan plenamente la privacidad del consumidor?

	Frecuencia	Porcentaje
No	2	16,7
Parcialmente	9	75,0
Sí	1	8,3
Total	12	100,0

Nota: Elaboración propia. 2025

Figura 14

¿Las medidas de ciberseguridad implementadas por las entidades financieras respetan plenamente la privacidad del consumidor?



Nota: Elaboración propia. 2025

De la tabla y figura anterior se tiene que un 75% considera que las medidas de ciberseguridad implementadas por las entidades financieras respetan parcialmente la privacidad del consumidor, mientras que un 16.7% tiene la certeza que estás entidades no toman medidas de ciberseguridad para garantizar a plenitud la privacidad del consumidor, mientras que por otro lado solamente un 8.3% tiene la plena seguridad que efectivamente se toman las medidas apropiadas para proteger la privacidad del consumidor, de todo lo expuesto se entiende que en conjunto un 91.7% considera que sus datos no son cuidados a plenitud o que lo hacen de manera parcial por lo tanto existe la mencionada desconfianza en el sistema financiero y la manera en la cual pretende salvaguardar los datos de sus clientes y consumidores por lo tanto es imperativo no solo trabajar en restaurar esta

confianza en el sistema, sino que a su vez otorgar protocolos más claros y precisos para el consumidor, así como medidas de acción para proteger sus derechos si estos se ven vulnerados.

Tabla 19

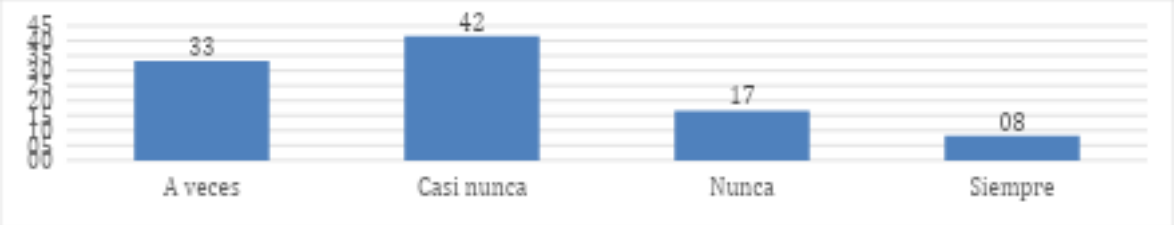
¿Los consumidores son informados de manera clara cuando ocurre una vulneración de sus datos personales?

	Frecuencia	Porcentaje
A veces	4	33,3
Casi nunca	5	41,7
Nunca	2	16,7
Siempre	1	8,3
Total	12	100,0

Nota: Elaboración propia. 2025

Figura 15

¿Los consumidores son informados de manera clara cuando ocurre una vulneración de sus datos personales?



Nota: Elaboración propia. 2025

De la tabla y figura anterior un 41.7% considera que los consumidores casi nunca son informados cuando ocurre una vulneración de sus datos personales, un 33.3% menciona que esto ocurre a veces, y un 16.7% alega que nunca, únicamente un 8.3% considera que esto ocurre siempre, la problemática acá radica en que siempre que ocurra alguna vulneración de los datos personales del consumidor este debe ser informado lo antes posible si acaso no de manera inmediata, y si bien no existe como tal la obligación mencionada, un 91,7% de los entrevistados considera que sí debería de existir, con solo un 8.3% mencionando que se encuentran de acuerdo de manera parcial sobre este aspecto.

Tabla 20

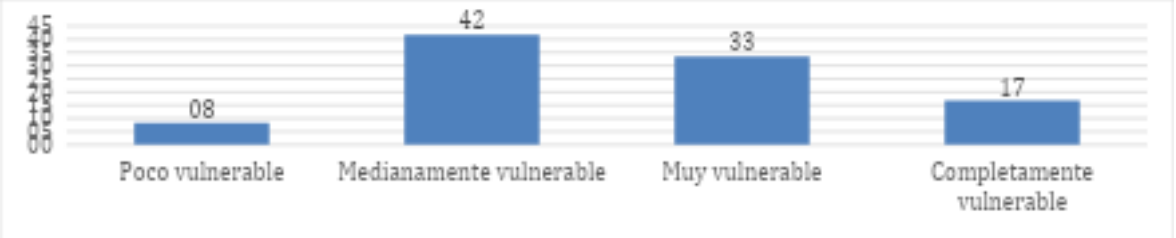
¿Qué tan vulnerable considera el derecho a la privacidad del consumidor frente a amenazas cibernéticas en el Perú?

	Frecuencia	Porcentaje
Poco vulnerable	1	8,3
Medianamente vulnerable	5	41,7
Muy vulnerable	4	33,3
Completamente vulnerable	2	16,7
Total	12	100,0

Nota: Elaboración propia. 2025

Figura 16

¿Qué tan vulnerable considera el derecho a la privacidad del consumidor frente a amenazas cibernéticas en el Perú?



Nota: Elaboración propia. 2025

De la tabla y figura anterior un 16.7% considera seriamente vulnerable el derecho a la privacidad del consumidor frente a amenazas cibernéticas en el Perú, mientras que un 33.3% lo considera muy vulnerable, y un 41.7% lo considera medianamente vulnerable, como se puede evidenciar es lógico entender que el derecho a la privacidad se encuentra cuanto menos en constante amenaza de ser vulnerado y por lo visto anteriormente no se cuenta con los mecanismos ni organismos suficientes para poder tutelar correctamente este derecho.

Tabla 22

¿Debería existir una obligación legal de notificación inmediata a los usuarios tras incidentes de ciberseguridad que afectan sus datos?

	Frecuencia	Porcentaje
Parcialmente	1	8,3
Sí	11	91,7
Total	12	100,0

Nota: Elaboración propia. 2025

Figura 18

¿Debería existir una obligación legal de notificación inmediata a los usuarios tras incidentes de ciberseguridad que afectan sus datos?



Nota: Elaboración propia. 2025

De la tabla y figura anterior se responde de manera categórica que un 91.7% considera que debería existir la obligación legal de notificación inmediata a los usuarios tras incidentes de ciberseguridad que afecten sus datos, mientras que sólo un 8.3% considera que esta obligación debería ser parcial, de lo cual es correcto inferir que es deber prioritario incluir esta obligación dentro de la normativa nacional, esta inclusión a su vez permite salvaguardar los derechos del consumidor cuando estos sean vulnerados y la correcta comunicación y transparencia les permitirá tomar las decisiones pertinentes al respecto de cómo proceder con su información filtrada, como actualizar contraseñas, redes

de seguridad o inclusive desistir de cierto servicio o producto si ha vulnerado sus datos personales al ser víctima de un ataque cibernético.

Tabla 23

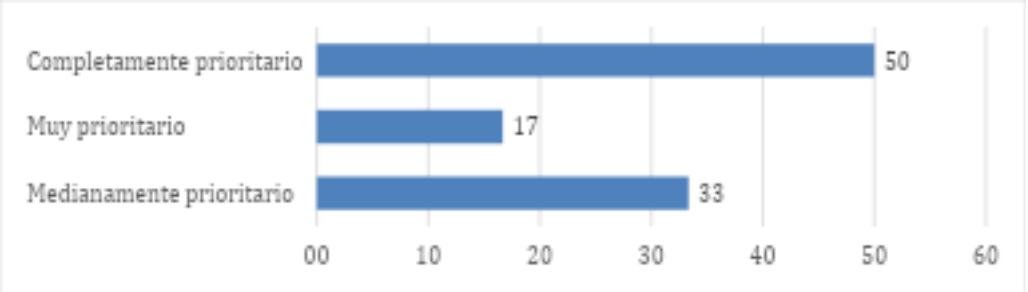
¿Qué tan prioritario considera que es para el Estado fortalecer la ciberseguridad para proteger la privacidad del consumidor?

	Frecuencia	Porcentaje
Medianamente prioritario	4	33,3
Muy prioritario	2	16,7
Completamente prioritario	6	50,0
Total	12	100,0

Nota: Elaboración propia. 2025

Figura 19

¿Qué tan prioritario considera que es para el Estado fortalecer la ciberseguridad para proteger la privacidad del consumidor?



Nota: Elaboración propia. 2025

De la tabla y figura anterior un 50% de los entrevistados considera que es completamente prioritario para el Estado fortalecer la ciberseguridad para proteger la privacidad del consumidor, mientras que un 16.7% considera que es moderadamente prioritario y un 33.3% considera que es medianamente prioritario, de esto se puede rescatar que ni un solo entrevistado consideró que esto sea una prioridad menor o que no lo sea, por lo tanto, es notoria la urgencia al respecto, como se ha mencionado anteriormente en la descripción del problema.

Tabla 24

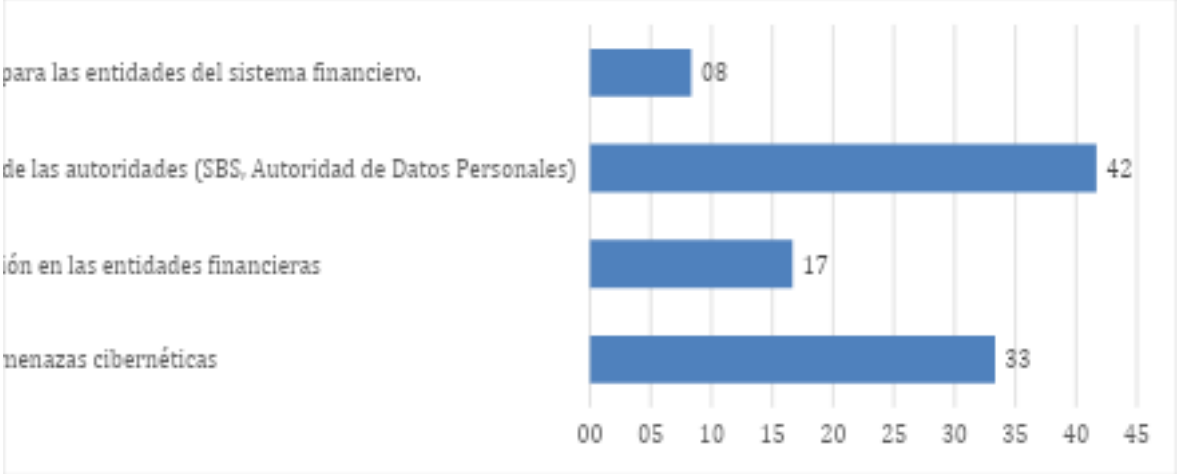
¿Cuál considera que es el principal desafío jurídico en la protección de datos personales en el sistema financiero peruano?

	Frecuencia	Porcentaje
Desactualización tecnológica frente a nuevas amenazas cibernéticas	4	33,3
Escasa cultura de cumplimiento y concientización en las entidades financieras	2	16,7
Insuficiente supervisión y sanciones por parte de las autoridades (SBS, Autoridad de Datos Personales)	5	41,7
No existen mecanismos de coacción suficiente para las entidades del sistema financiero.	1	8,3
Total	12	100,0

Nota: Elaboración propia. 2025

Figura 20

¿Cuál considera que es el principal desafío jurídico en la protección de datos personales en el sistema financiero peruano?



Nota: Elaboración propia. 2025

De la tabla y figura anterior un 41.7% considera que el principal desafío jurídico en la protección de datos personales en el sistema financiero peruano es la insuficiente supervisión y sanciones por parte de las autoridades (SBS, ANPDP), un 16.7% considera la escasa cultura de cumplimiento y concientización en las entidades financieras, un 33.3% lo atribuye a la desactualización tecnológica frente a nuevas amenazas cibernéticas y por último un 8.3% considera que no existen mecanismos de coacción suficiente para las

entidades del sistema financiero, todos aspectos que han sido trabajados y profundizados en la presente investigación.

Tabla 25

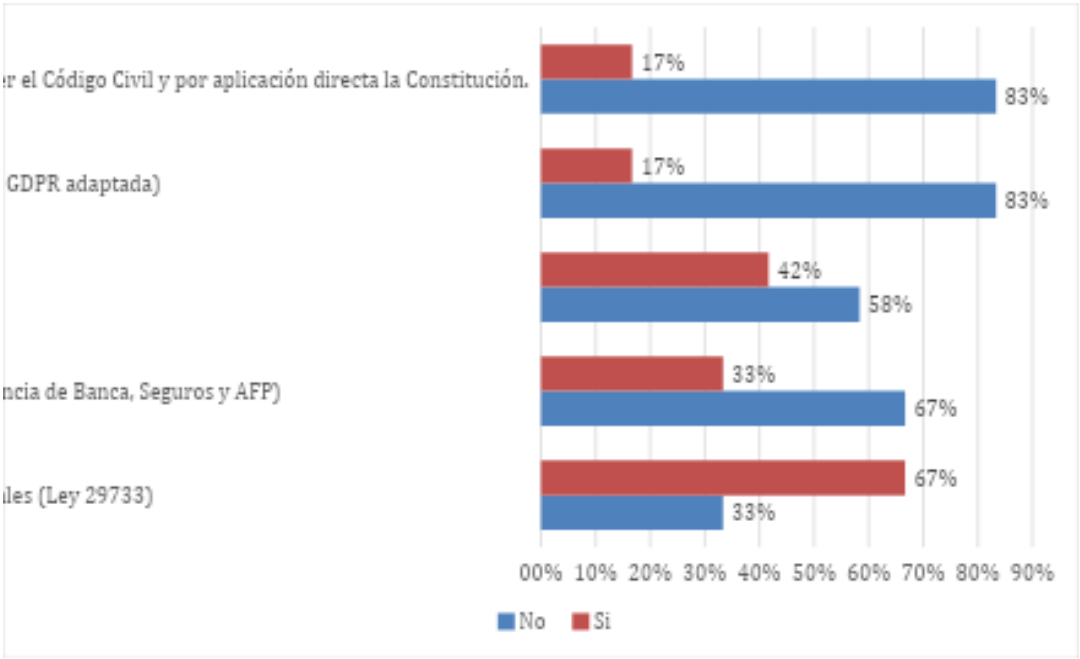
¿Qué normativa considera más relevante en la protección de los datos frente a ciberataques?

	No	Sí
Ley de Protección de Datos Personales (Ley 29733)	33,3%	66,7%
Normativa de la SBS (Superintendencia de Banca, Seguros y AFP)	66,7%	33,3%
Código de Defensa de Consumidor	58,3%	41,7%
Normas internacionales (ISO, NIST, GDPR adaptada)	83,3%	16,7%
Por aplicación supletoria debería ser el Código Civil y por aplicación directa la Constitución.	83,3%	16,7%

Nota: Elaboración propia. 2025

Figura 21

¿Cuál considera que es el principal desafío jurídico en la protección de datos personales en el sistema financiero peruano?



Nota: Elaboración propia. 2025

De la tabla y figura anterior se desprende que un 66.7% considera que la normativa más relevante frente a ciberataques es la LPDP, seguida de un 41.7% que considera al Código de Defensa del Consumidor, seguido por un 33,3% que respalda la opción de la normativa otorgada por la SBS, dejando finalmente a las Normas internacionales (ISO, NIST, GDPR adaptada) y a la aplicación supletoria debería ser el Código Civil y por aplicación directa la Constitución con un 16,7% respectivamente, de todo ello se colige que conforme a los principios del derecho existe una primacía de la norma específica frente a la normativa general, por lo tanto aquellas que sean más puntuales y pertinentes a según qué casos serán las óptimas para su debido uso frente a ciberataques, teniendo en consideración los aspectos tratados como la protección de datos e información del consumidor en el sistema financiero esto demuestra que las normas utilizadas para el desarrollo han sido propicias para enfrentar la problemática.

4.2. Efectividad de la Ley N.º 29733 y normativas vigentes en materia de protección de datos personales y ciberseguridad en el ámbito financiero.

4.2.1. Evaluación normativa y alcance de la Ley N.º 29733 y su Reglamento (D.S. 003-2013-JUS)

La Ley N° 29733 y su Reglamento constituyen la base normativa de la protección de los datos personales en el Perú, pero su alcance dentro del sistema financiero resulta poco frente al avance tecnológico y la complejidad de los nuevos riesgos digitales que vemos y veremos con el pasar del tiempo. Desde nuestra perspectiva crítica y dentro del marco de nuestra investigación, se evidencia que la ley mencionada, pese a su intento de ser protectora, no logra garantizar de manera efectiva la privacidad del consumidor financiero, por lo que su estructura requiere de una actualización integral la cual se pueda adecuar a los desafíos contemporáneos de la ciberseguridad.

Dentro de los principios mencionados por la ley, tenemos a mencionar el de consentimiento que busca otorgar al ciudadano el poder de decidir sobre el uso de la información, pero en la práctica se ha vuelto un requisito formal; los consumidores dentro del sistema financiero suelen aceptar estos términos y condiciones sin llegar a comprender con totalidad el alcance de lo que en verdad están autorizando, de esta manera se convierte al consentimiento en una figura simbólica más que en un acto informado, por lo que se

demuestra que dicho principio no cumple con su propósito esencial de proteger la autonomía del titular del dato frente a la presión tecnológica y contractual del sistema financiero

Sobre el principio de finalidad, el cual es destinado a garantizar que los datos se utilicen solo para el propósito informado, el mismo se ve vulnerado por el uso de información con fines secundarios, como los de marketing o análisis de comportamiento comercial, porque en la práctica las entidades financieras han ampliado su tratamiento de datos más allá del propósito informado, aprovechando los vacíos de la ley y la escasa fiscalización estatal. Esto reflejaría la falta de los límites claros y los mecanismos de control debilitando así la confianza del consumidor.

En cuanto al principio de proporcionalidad, que busca que el tratamiento de los datos sea adecuado y no excesivo, el mismo carece de criterios objetivos. Dentro del sistema financiero, se ha permitido la recolección en grandes cantidades de información "seguridad del cliente", cuando en la realidad se invade la esfera privada del consumidor. Desde nuestro análisis, esta ambigüedad presentada da a entender que la ley no prevé salvaguardas técnicas ni parámetros de evaluación, y que en su eficacia dependería únicamente de la buena fe de las entidades en cuanto a que den un buen control normativo y real.

Por último, sobre el principio de seguridad resultaste ser el más crítico. Aunque nuestra ley exige medidas para prevenir accesos indebidos de gente ajena o filtraciones, las vulneraciones de datos en bancos y financieras evidencias que no hay un nivel suficiente de estándares ni auditorías obligatorias. La protección de datos se debe de tratar como una política de ciberseguridad activa; por lo que todo ello resulta en que la debilidad de este principio es incompatible con la masiva cantidad de riesgos actuales y demuestra que el marco legal actual carece de una buena actualización tecnológica y supervisión técnica.

Desde nuestra perspectiva la ley requiere de una actualización integral que incorpore estándares internacionales, integre a la ciberseguridad como un eje transversal y reconozca que la protección de datos personales es hoy un pilar del derecho a la privacidad y la confianza del consumidor en el sistema financiero peruano.

La aplicación por parte de las entidades financieras es limitada y principalmente formal, porque, aunque los bancos y financieras reconozcan la existencia de los derechos

materia de protección de datos personales, en la práctica se han dado casos que se cumplen para evitar sanciones y no formarán parte como una cultura institucional de ciberseguridad y respeto a la privacidad del consumidor.

Un claro ejemplo mencionado es el caso de Banco Interbank del año 2024, donde se filtraron información sensible de miles de usuarios incluyendo nombres, números de tarjeta y datos de identificación. De igual forma con el BBVA Perú que fue sancionado por la Autoridad Nacional de Protección de datos personales al incumplir el principio de consentimiento y no adoptar medidas suficientes de seguridad. Ambos casos reflejan que, aunque la normativa exige protocolos técnicos y organizativos, las entidades no los aplican con la rigurosidad necesaria ni comunican oportunamente las vulneraciones a los afectados.

Asimismo, mencionamos la asimetría informativa entre los consumidores y los bancos, siendo otro obstáculo. Al tener cláusulas de consentimiento muy extensas y poco claras teniendo en cuenta que la mayoría de las personas suele evitar leerlos por varios motivos como la falta de preocupación, escasez de conocimiento legal, entre otros.

En los últimos años, la ANPDP ha intensificado la fiscalización, a comparación de años más atrás, donde impuso sanciones que evidencian las deficiencias de las entidades financieras sobre el cumplimiento de la Ley N° 29733.

En el 2020 se sancionó al Banco de Credito del Peru con una multa de S/ 166,000.00 (40 UIT) por no garantizar la confidencialidad de los datos de sus clientes luego de un ataque cibernético permitiera el acceso no autorizado a números de tarjetas, cuentas y saldos.

Igualmente, con la misma entidad financiera, hubo una sanción por un monto mayor de aproximadamente S/ 300,000.00 por el tratamiento inadecuado de datos biométricos faciales de usuarios en el uso del libro de reclamaciones virtual.

Si bien lo anterior pareciera en montos gigantescos en términos legales, ello no genera al final un efecto disuasorio real frente a las grandes entidades financieras, cuyos ingresos superan ampliamente todos estos montos sancionados.

Tabla 26

Comparación normativa y percepción de los encuestados

Aspecto normativo (Ley y artículo)	Percepción de los encuestados	Comentario crítico
Ley N.º 29733, Art. 9: Garantiza el principio de seguridad y el deber del titular del banco de proteger los datos personales con medidas adecuadas.	Tabla 4: Sólo el 37.3% de los consumidores siente que su información está segura al hacer operaciones por internet.	Existe una gran brecha entre el principio de seguridad garantizado por ley y la percepción real de los usuarios sobre la banca digital. Esto revela una necesidad de reforzar medidas técnicas y de comunicación.
Ley N.º 29733, Art. 18: Derecho de acceso del titular a saber qué información tienen las entidades sobre él.	Tabla 8: Sólo el 52.9% sabe que puede solicitar esta información al banco.	La falta de conocimiento debilita el ejercicio de los derechos. La norma existe, pero no hay mecanismos suficientes de difusión o educación por parte del Estado ni de las empresas.
Ley N.º 29733, Art. 5: Exige consentimiento previo, informado y libre para el tratamiento de datos personales.	Tabla 3: Solo el 58.8% ha leído términos y condiciones de apps bancarias.	Aunque la ley exige consentimiento informado, en la práctica este suele ser automático y poco comprendido. Es necesario revisar la efectividad de los mecanismos de obtención de consentimiento.
Ley N.º 29733, no contempla notificación obligatoria al titular ante incidentes.	Tabla 19: 41.7% dice que 'casi nunca' se informa sobre vulneraciones.	Este vacío normativo es crítico. La ley no exige transparencia en incidentes de ciberseguridad, lo que agrava la desconfianza del usuario.
D.S. 003-2013-JUS, Art. 7 y Ley 29733, Art. 6: Establece el principio de finalidad: los datos deben usarse sólo para lo que fueron recolectados.	Tabla 9: Casos reportados de llamadas persistentes de terceros, sin consentimiento.	Evidente desalineación entre la ley y la práctica de muchas entidades que transfieren datos sin justificación. Necesita regulación y fiscalización más estricta.

4.2.2. Análisis de las normas complementarias y su coherencia con la Ley N.º 29733

La Ley N.° 29733 como el eje de nuestra estructura de análisis, establece los pilares rectores en tratamiento y protección de datos personales, sin embargo, para la efectividad de su objetivo se tienen diversos cuerpos normativos que operan en paralelo, entre ellos, la Ley N.° 29571 y la Ley N.° 30618.

Desde una perspectiva crítica, la Ley N° 29571 resulta ser un complemento necesario en lo referido al derecho a la información del consumidor, que reconoce cómo se usan sus datos personales en los servicios contratados. En sí, las disposiciones sobre la transparencia en las relaciones de consumo, el consentimiento informado y la obligación de atención de reclamos proporcionan un marco de exigencia que refuerza el principio de la finalidad y el consentimiento que está presente en la Ley N.°29733. De esta manera, cuando un entidad del sistema financiero recoge los datos personales de un consumidor con fines contractuales, también este está obligado por el la Ley N° 29571 a informar con transparencia el uso y responder debidamente ante cualquier reclamo del titular o uso indebido de la información. Por lo que la Ley N.° 29571 aborda la protección de datos de una manera general pero sin una relación directa ni articulada con la Ley N.° 29733, no hay una coordinación formal entre INDECOPI y la ANPDP, cada una puede actuar por separado y exigir cosas diferentes al mismo banco, del mismo modo no existe un solo canal para reclamos sobre datos personales y consumo financiero, por ejemplo, si un consumidor siente que su banco mal utilizó sus datos, puede ir a INDECOPI al reclamar un mal servicio o en su defecto a la ANPDP por violacion a la privacidad, pero no hay un indicio que indique claramente cual es el camino correcto.

Por su parte, la Ley N.° 30618, que declara de interés nacional la seguridad digital, busca fortalecer tanto en el sector privado y público la capacidad de hacer frente a los riesgos derivados del cibercrimen, incluyendo el robo de la información y el ataque a las infraestructuras críticas. Esta Ley se vincula con la Ley N.° 29733 a través del principio de seguridad de los datos, al imponer a las entidades financieras la obligación de implementar medidas técnicas para proteger el entorno digital. Sin embargo, esta Ley está enfocada en defensa nacional e institucional, y no en la protección directa de los datos personales en los consumidores, por lo que su complementariedad es más técnica que jurídica, y no cuenta

con mecanismos de coordinación regulatoria que permite una acción conjunta entre la ANPDP y el Centro Nacional de Seguridad Digital.

En conclusión, si bien tanto el Código de Protección y Defensa del Consumidor como la Ley de Seguridad Digital aportan elementos importantes para reforzar la protección de los datos personales, ya sea desde la defensa de los derechos de los usuarios frente a las entidades financieras o desde el enfoque técnico de la ciberseguridad, su desarrollo normativo y su aplicación operativa aún se muestran desconectados de la Ley N.º 29733. Esta falta de articulación entre los marcos legales genera vacíos que, lejos de proteger de forma efectiva la privacidad del consumidor en el entorno financiero digital, pueden traducirse en contradicciones o respuestas fragmentadas por parte del Estado. A la luz de los hallazgos de esta investigación, resulta urgente avanzar hacia un sistema legal más coordinado orientado a salvaguardar, de manera integral y coherente, los datos personales de los consumidores.

Aunque el Perú cuenta con la Ley N.º 29733 desde 2011, complementada por normas como el Código de Protección y Defensa del Consumidor (Ley N.º 29571) y la Ley de Seguridad Digital (Ley N.º 30618), persisten vacíos normativos significativos que afectan la protección efectiva de los datos personales, especialmente en el sector financiero. Estos vacíos son particularmente preocupantes dada la creciente digitalización de servicios y el uso intensivo de tecnologías como inteligencia artificial, biometría y plataformas en la nube.

Uno de los principales vacíos normativos está relacionado con el tratamiento automatizado de datos personales mediante inteligencia artificial. La legislación peruana actual no regula adecuadamente la toma de decisiones automatizadas, como la asignación de puntajes crediticios por parte de bancos a través de algoritmos opacos. Esta omisión deja a los ciudadanos sin mecanismos efectivos para cuestionar decisiones que pueden tener efectos significativos sobre sus derechos económicos. Incluso el nuevo reglamento propuesto para la Ley N.º 29733 ha sido criticado por no incluir disposiciones específicas sobre IA y perfilamiento automatizado, un aspecto considerado urgente por expertos.

Otro grave vacío se refiere al uso de datos biométricos. Aunque la Ley 29733 considera estos datos como sensibles, no existe una regulación específica que determine cuándo, cómo y con qué límites pueden ser utilizados. En el ámbito financiero, los bancos han adoptado prácticas de autenticación biométrica, como el reconocimiento facial, sin

contar con un marco jurídico detallado que establezca garantías de proporcionalidad y seguridad. El caso del BCP en 2024, sancionado por exigir la captura de rostro e imagen de DNI a usuarios que solo deseaban registrar un reclamo, ejemplifica el abuso derivado de esta falta normativa.

Además, la comercialización ilegal de bases de datos personales en mercados informales como Polvos Azules o la avenida Wilson evidencia la ineficiencia del sistema para frenar estas prácticas ilícitas. Se siguen vendiendo datos sensibles de clientes bancarios sin consecuencias significativas, lo cual mina la confianza ciudadana en la protección institucional de su privacidad. Este tráfico ocurre frente a la inacción de las autoridades competentes y pone en evidencia una ausencia de penalidades reales y efectivas para quienes trafican con información privada.

Las transferencias internacionales de datos representan otro punto débil. Aunque el artículo 15 de la Ley 29733 exige garantías de protección en los países receptores, hasta 2024 no existía una lista clara de países adecuados ni cláusulas contractuales modelo. La reciente Guía de Transferencias Internacionales marca un avance, pero no soluciona completamente el vacío, ya que muchas operaciones de bancos peruanos aún se realizan sin supervisión efectiva sobre los datos que cruzan fronteras.

Asimismo, la falta de coordinación entre la ANPDP, la SBS e INDECOPI genera duplicidades, ineficiencias y, sobre todo, zonas grises en la respuesta institucional ante incidentes. El caso Interbank mostró cómo estas entidades actuaron sin una estrategia común, demostrando la necesidad urgente de crear mecanismos de colaboración formal, como protocolos de intervención conjunta o sistemas de intercambio de información ante vulneraciones de datos. El consentimiento digital sigue siendo una figura débil. El marco normativo ha tolerado durante años formas imprecisas y generalizadas de consentimiento, como casillas premarcadas o cláusulas ocultas. Aunque las reformas recientes promueven el consentimiento por finalidad, aún no existe una normativa clara sobre los derechos frente a decisiones tomadas exclusivamente por sistemas automatizados. Esto deja a los usuarios expuestos a prácticas de perfilamiento sin garantías suficientes.

Por todo ello, los vacíos normativos detectados comprometen el ejercicio pleno del derecho a la privacidad en el entorno financiero digital. La legislación debe actualizarse con urgencia para regular nuevas tecnologías, proteger datos sensibles como los biométricos, impedir el tráfico ilegal de información personal, garantizar la seguridad en

transferencias internacionales y coordinar efectivamente a las autoridades competentes. Solo así será posible brindar una protección real y efectiva a los ciudadanos en una economía cada vez más digitalizada y dependiente del tratamiento de datos personales. La Ley N.º 29733 ha constituido un marco jurídico importante para la protección de datos personales en el Perú. No obstante, su estructura normativa ha comenzado a mostrar serias limitaciones ante los rápidos cambios tecnológicos que atraviesan actualmente el sector financiero. Tecnologías como la inteligencia artificial (IA), el big data, blockchain y los servicios bancarios digitales han introducido nuevos escenarios para los que la ley no ofrece respuestas precisas ni suficientes.

En lo que respecta a la IA, el marco legal vigente no contempla el uso de decisiones automatizadas ni obliga a los responsables del tratamiento a justificar el funcionamiento de los algoritmos utilizados. Esto abre la puerta a posibles prácticas opacas, especialmente cuando se evalúa la solvencia o el riesgo crediticio de una persona mediante sistemas automatizados sin intervención humana. Por otro lado, el manejo de grandes volúmenes de datos –propio del big data– choca con el principio de finalidad y la exigencia de consentimiento informado y previo. En la práctica, esto dificulta que las entidades financieras puedan aplicar análisis predictivos o reutilizar información sin incurrir en posibles infracciones.

En el caso de los datos biométricos, aunque la ley los considera información sensible y exige un tratamiento proporcional y con consentimiento explícito, la aplicación real es deficiente. Prueba de ello es la reciente sanción impuesta a una entidad financiera por haber solicitado información biométrica de manera innecesaria, lo que evidenció fallas en el cumplimiento efectivo de la normativa. Con respecto a la tecnología blockchain, los retos son más profundos. La naturaleza descentralizada de esta herramienta dificulta enormemente el ejercicio de derechos fundamentales como la cancelación de datos o la identificación de los responsables del tratamiento, lo que deja sin efecto varias de las garantías que protege la Ley 29733.

En términos de ciberseguridad, la normativa peruana había mostrado vacíos importantes hasta hace poco. Sin embargo, las recientes propuestas de modificación al reglamento incluyen medidas más claras, como la obligación de reportar incidentes de seguridad en un plazo de 48 horas, lo que representa un avance relevante. Finalmente, el desarrollo de procesos automatizados, el uso de servicios en la nube y la implementación

progresiva del open banking plantean retos adicionales. Aunque se han introducido disposiciones sobre portabilidad de datos y estándares técnicos, aún no existe un marco normativo robusto que regule las condiciones de interoperabilidad, los derechos de los usuarios y la responsabilidad de las plataformas involucradas.

Tabla 27

Comparación normatividad y experiencia de los profesionales

Normatividad y artículo	Percepción de los profesionales	Comentarios Críticos
Ley N.º 29733, art. 22 y Reglamento D.S. N.º 003-2013-JUS, art. 47: No hay obligación clara de notificación inmediata ante incidentes.	El 41.7% indica que los consumidores 'casi nunca' son informados de vulneraciones, y el 33.3% que 'a veces'. (Tabla 19)	Se requiere modificar el marco legal para incluir deberes explícitos de notificación al titular afectado.
Ley N.º 29733, art. 1: Garantiza el derecho a la privacidad y protección frente al uso indebido de datos.	El 75% señala que las entidades sólo respetan 'parcialmente' la privacidad del cliente. (Tabla 18)	Este derecho constitucional es vulnerado sistemáticamente por falta de aplicación efectiva y fiscalización real.
Ley N.º 29733, artículo 7: Requieren consentimiento para el tratamiento, pero no abordan IA ni tecnologías emergentes.	El 33.3% identifica la desactualización normativa como principal problema; 41.7% menciona debilidad en supervisión. (Tabla 15)	Se evidencia un rezago importante del marco legal frente a tecnologías como IA o big data.
Constitución Política del Perú, art. 2 inciso 6: Garantiza el derecho fundamental a la privacidad.	El 33.3% lo considera 'muy vulnerable' y el 16.7% 'completamente vulnerable'. (Tabla 20)	El derecho a la privacidad es percibido como frágil frente al avance tecnológico sin regulación actualizada.
Normas dispersas: Ley 29733, Ley 29571, Ley N.º 30618 sobre seguridad digital.	Solo el 41.7% reconoce a la Ley 29733 como marco rector; hay percepción de fragmentación normativa. (Tabla 25)	Se requiere un marco normativo articulado y moderno que aborde los retos digitales integradamente.

4.3. Responsabilidad del consumidor en la protección de su información personal en el sistema financiero digital

El consumidor desempeña un rol clave en la salvaguarda de su información personal en el entorno financiero digital, actuando no sólo como un titular de derechos, sino también como un participante activo en la mitigación de riesgos. A pesar de que las instituciones financieras deben establecer medidas de protección, una porción considerable de las infracciones proviene de conductas inseguras de los propios usuarios, como el empleo de contraseñas poco seguras, la falta de comprobación de páginas web o la entrega de información a terceros sin autorización. Por ello, examinar su papel implica reconocer que la defensa de la privacidad no puede depender exclusivamente de la legislación o de las entidades, sino que también necesita del comportamiento consciente del consumidor.

Ante ello, se tiene como ejemplo la Resolución N° 0286-2022/PS2 del Expediente N° 0028-2022/PS2, texto del cual se cita lo siguiente: *"Si bien el banco se encuentra obligado a adoptar medidas de seguridad para la autorización de operaciones con tarjeta no presente, ninguna acción resultará eficaz si es propio consumidor omite su deber de custodia";* significa ello que es el consumidor quien tiene que actuar de forma diligente al proteger sus datos personales y no permitir que ningún tercero acceda a la sensibilidad de ellos, pues esto según la jurisprudencia resulta en responsabilidad del consumidor; por tanto, la precaución por parte del Banco se encuentra en sus páginas oficiales, y es el consumidor quien pudo evitar ello al ser más diligente (INDECOPI, 2022).

Asimismo, es INDECOPI quien, con su fin de la fomentación de un mercado idóneo para el consumidor, no puede concluir que la falta de diligencia del consumidor sea un eximente de responsabilidad, esto por cuanto es evidente la situación beneficiosa de la relación comercial con los proveedores bancarios y las obligaciones que este último tiene dentro del principio de idoneidad.

Sin embargo, no se quiere únicamente responsabilizar ante cualquier conducta a los proveedores, entendemos que la asimetría de información es muy alta y que los consumidores requieren siempre estar protegidos pero, responsabilizar siempre al proveedor es un hecho con altos costos, como lo afirma Bullard (2010) *"Asumir que el consumidor puede ser protegido en cualquier caso, sin importar su nivel de diligencia, es asumir que tendrán una suerte de seguro contra su propia irresponsabilidad, brindado por lo proveedores. Si el proveedor debe responder incluso en supuestos de consumidores descuidados, se estaría elevando los costos que los proveedores tendrían que asumir para cubrir dicho seguro (...)".*

En este contexto, es esencial impulsar iniciativas que refuercen su responsabilidad y educación, tales como campañas informativas sobre seguridad financiera, programas de alfabetización digital accesibles, recordatorios frecuentes sobre prácticas recomendadas, requerimiento de autenticación fuerte y sistemas claros para reportar problemas. Estas iniciativas, alineadas con un marco regulatorio actualizado, ayudarían a cerrar brechas de conocimiento y promover un uso seguro y responsable de los servicios financieros digitales.

4.3.1. Nivel de conocimiento y prácticas del consumidor frente a la protección de datos

En ámbitos internacionales, los consumidores presentan conocimientos predominantemente superficiales sobre la protección de sus datos personales, la preocupación de estos por asegurar su privacidad no se refleja en sus prácticas, evidenciando un comportamiento no preventivo, compartiendo información sensible sin evaluar adecuadamente los riesgos, lo que usualmente se ve en los casos de vulneración de datos personales, lo que muestra una contradicción entre la percepción del peligro y la conducta efectiva (Pinto, 2025). Tal como lo afirma Dommeyer y Gross (2003), el conocimiento de los consumidores sobre la protección de datos personales es deficiente; si bien existen indicios de conciencia acerca de los riesgos derivados del tratamiento de información personal, la mayoría de los usuarios carece de una comprensión cabal de los instrumentos legales y de las medidas técnicas y administrativas disponibles para salvaguardar sus derechos. Ello significa que existe una gran brecha entre el conocimiento declarado por los consumidores y las prácticas del día, que aunque se conocen ciertas medidas de seguridad, no se aplican en su totalidad.

El grado de comprensión y las acciones de los consumidores en relación con la protección de datos presentan una situación variada, en la cual el reconocimiento de conceptos como “datos sensibles”, “medidas de seguridad” o “ciberataques” suele ser escaso, a pesar de que los usuarios se involucran cotidianamente con servicios financieros digitales. Las encuestas llevadas a cabo muestran que numerosos consumidores dan su consentimiento informado sin examinar los términos, lo aceptan por costumbre o no entienden completamente el alcance de las autorizaciones que ofrecen a las entidades financieras. Esto muestra que el consentimiento, en su uso actual, actúa más como un procedimiento administrativo que como un auténtico recurso para la autodeterminación en

cuanto a la información. De estos hallazgos, se hace evidente que la efectividad del consentimiento informado no solo depende de la claridad y accesibilidad de la información proporcionada por las organizaciones, sino también del nivel de alfabetización digital y legal del consumidor. Para mejorar estas prácticas, es necesario fortalecer la educación sobre la privacidad, simplificar las notificaciones sobre el tratamiento de datos y fomentar una cultura de verificación activa antes de dar permiso para cualquier uso de información personal.

Tabla 28

Comparación entre normatividad y percepción de profesionales

Normatividad y artículo	Percepción de los profesionales	Comentario crítico
Ley N.º 29733 – Ley de Protección de Datos Personales, art. 12(consentimiento informado y finalidad del tratamiento).	El **58.8%** de los encuestados declara que **no ha leído** los términos y condiciones al usar aplicaciones bancarias, mientras que solo el **41.2%** afirma haberlos leído.	El bajo nivel de lectura revela que el consentimiento informado opera como una formalidad, sin garantizar la comprensión real del usuario. Esto evidencia que la autodeterminación informativa está debilitada y que el consentimiento otorgado no cumple plenamente con los estándares exigidos por la Ley.
Ley N.º 29571 – Código de Protección y Defensa del Consumidor, arts. 1, 2 y 74(derecho a la información y transparencia contractual).	La mayoría de los encuestados, pese a ser profesionales, acepta contratos de adhesión sin revisarlos, reflejando una brecha	La regulación exige claridad, pero en la práctica los términos suelen ser extensos, técnicos y poco amigables. Esto limita la capacidad del consumidor para comprender riesgos digitales, fortalecer su autocuidado y ejercer control real sobre el tratamiento de sus datos.

Lund et al. (2026) mencionan en su artículo "Validación de una escala para medir la alfabetización en privacidad de datos personales entre estudiantes universitarios" que, la protección de los datos personales no depende únicamente de la existencia de un marco normativo, depende del nivel de comprensión que poseen los consumidores sobre el tratamiento de su información. Ello surge del concepto de ***Alfabetización en protección de datos personales,*** que hace referencia a la capacidad del individuo para entender, pensar y mitigar los riesgos asociados al usar sus datos personales; por lo que, un bajo nivel de alfabetización en nuestro país limita nuestro ejercicio de derechos y favorece a prácticas riesgosas, ello evidencia la necesidad de lo mencionado en el apartado anterior, reforzar la educación en materia de privacidad.

4.3.2. Estrategias de fortalecimiento del rol del consumidor y cultura digital segura

El fortalecimiento del papel del consumidor en la salvaguarda de su información personal requiere una cultura digital segura; para lograrlo, los programas de educación financiera y digital promovidos por instituciones como la SBS, Indecopi y Asbanc son fundamentales. El análisis de estas iniciativas indica que, si bien han obtenido progresos en la alfabetización básica, todavía persiste una diferencia entre la información proporcionada y las conductas efectivas de los usuarios.

La SBS impulsa la realización de cursos y campañas sobre seguridad en las operaciones bancarias digitales, mientras que INDECOPI se ocupa de la protección de datos desde la perspectiva de los derechos del consumidor, y por su parte, Asbanc elabora materiales educativos que explican riesgos comunes como el phishing y el robo de identidad. No obstante, la extensión de estos programas sigue siendo reducida y frecuentemente no se traduce en modificaciones de comportamiento duraderas.

Según lo mencionado por Pattanayak et al. (2025), sostienen que la protección al consumidor debe de fundamentarse en tres pilares fundamentales: Protección de datos personales, la educación digital y una regulación adaptada a nuevas tecnologías; la asimetría de información influye bastante en el enfrentamiento de riesgos, lo que hace necesario no solo fortalecer de cierta manera puntos estratégicos del marco normativo, sino el desarrollo de capacidades para comprender y gestionar la información contenida, por lo

que el consumidor dejará de ser una sujeto pasivo y asumirá un rol más importante, uno activo dentro de la protección de sus datos, contribuyendo de esta forma a la consolidación de una cultura digital segura.

Un estudio más detallado indica que estas estrategias deben ser coordinadas, simplificar su lenguaje y centrarse en métodos participativos que posibiliten al consumidor reconocer riesgos diarios y establecer hábitos seguros de forma continua. De este modo, podrán establecerse como instrumentos eficaces para fomentar una cultura digital responsable en el ámbito financiero.

Tabla 28

Comparativa sobre la supervisión estatal

Normatividad y artículo	Percepción de los profesionales	Comentario crítico
Circular N.º G-140-2018 de la SBS Establece lineamientos mínimos para la gestión de la seguridad de la información, incluyendo monitoreo, respuesta a incidentes y protección de datos.	Según los resultados de la encuesta, 66.7% considera que la supervisión de la SBS es al menos medianamente efectiva. Un 25% la percibe poco efectiva y un 8.3% nada efectiva.	Aunque la norma establece obligaciones claras, la percepción de efectividad es moderada. Esto sugiere que la supervisión se cumple más en el plano formal que en impactos visibles para el consumidor, especialmente frente a incidentes de ciberseguridad.
Ley N.º 29733 – Ley de Protección de Datos Personales, arts. 28 y 32(deber de seguridad y responsabilidad del titular del banco de datos).	Un 75% de los encuestados considera que las entidades financieras solo respetan la privacidad del consumidor de manera parcial. Un 16.7% opina que no la respetan plenamente.	La brecha entre regulación y experiencia del usuario refleja desconfianza en la capacidad del sistema financiero para garantizar privacidad frente a riesgos digitales, pese a la existencia de normas robustas.
Ley N.º 29571 – Código de Protección y Defensa del Consumidor, arts. 62 y 75(deber de idoneidad y protección de información sensible).	La percepción general indica incertidumbre sobre la efectividad real de las medidas adoptadas por las entidades financieras y el grado de protección que reciben los consumidores.	La norma exige protección adecuada, pero los incidentes y la percepción ciudadana muestran que aún existen vacíos en la aplicación práctica, especialmente en la comunicación de riesgos, transparencia y respuesta ante incidentes.

4.4. Debilidades estructurales y amenazas cibernéticas en el sistema financiero peruano y su impacto en la privacidad

4.4.1. Principales vulnerabilidades del sistema financiero digital peruano

Según lo mencionado por Mansilla Pizarro (2020), todo lo que conlleva el proceso de digitalización del sistema financiero peruano ha generado, como se reitera varias veces, una brecha enorme de seguridad, caracterizada por la falta de correspondencia entre el avance tecnológico a grandes pasos y la capacidad efectiva de la protección de la información, como lo son la expansión de servicios de banca digital, billeteras electrónicas y plataformas Fintech, las cuales han ido incrementado la superficie posible de un ataque cibernético. Por lo que, la normativa que va de la mano con aquellas innovaciones tecnológicas, en muchos casos resultó insuficiente frente a los ataques como el phishing y la suplantación de identidad, advirtiéndose una vulneración a la privacidad del consumidor al generar una exposición, un uso indebido y la pérdida de control sobre su información personal, afectando la confianza en el sistema financiero.

Asimismo, son diversas investigaciones académicas que han identificado que el sistema financiero peruano presenta vulnerabilidades estructurales vinculadas a la gestión de la seguridad de la información de los activos digitales. Tal como lo menciona Tasarriego, se ha señalado que las entidades del sistema financiero enfrentan las debilidades vinculadas con la inadecuada gestión de riesgos, la insuficiente implementación de marcos de ciberseguridad y la falta de mecanismos eficaces para el monitoreo constante de incidentes cibernéticos. Ello resulta en patrones de vulnerabilidad en el tratamiento de datos personales, incrementando así la exposición del sistema financiero a amenazas como accesos no autorizados, filtraciones de información y ataques informáticos, afectando directamente a la seguridad y privacidad fundamental de los consumidores (Casariego Palomino, 2025).

Una mayor banca digital sería igual a una mayor superficie de ataque, esto resulta interesante de analizar, porque es un pensamiento que dentro del contexto del consumidor suena muy atractivo de pensar, ya que mientras más banca digital se contemple dentro del sistema financiero, más desarrollo y beneficios traerá consigo; sin embargo, si bien ello resultó en una expansión de servicios bancarios a través de plataformas digitales, permitiendo más interacción con los usuarios, también significó un aumento de amenazas cibernéticas, debido a que mientras más banca digital se disponga dentro de un sistema

financiero, mayor será la presencia de fraudes digitales orientados al robo de información y dinero mediante técnicas como el phishing y el malware, evidenciando nuevamente vulnerabilidades estructurales en seguridad de los servicios financieros digitales y un impacto directo en la privacidad del consumidor (Garcia, 2021).

El estudio de los incidentes de ciberseguridad informados en entidades como Interbank, BBVA y Scotiabank muestra patrones similares en relación con vulnerabilidades técnicas y deficiencias en la gestión de riesgos, lo que permite realizar una evaluación crítica del cumplimiento de las normas requeridas por la SBS en la Circular N. º G-140-2018. Los incidentes, que abarcaron paradas de servicios, accesos inapropiados y afectaciones temporales en la disponibilidad de plataformas digitales, demuestran que, aunque las instituciones financieras han adoptado medidas de seguridad de acuerdo con la normativa vigente, su implementación efectiva muestra fallas en aspectos como la supervisión en tiempo real, la reacción ante incidentes, la comunicación con los usuarios y la capacidad operativa de recuperación. El análisis de estos acontecimientos indica que el cumplimiento formal no garantiza siempre un nivel de protección eficaz, especialmente ante ataques complejos o vulnerabilidades relacionadas con proveedores tecnológicos externos. Por lo tanto, el análisis de la Circular G-140-2018, en relación con estos casos, posibilita llegar a la conclusión de que, aunque define un conjunto sólido de responsabilidades, su eficacia está ligada a la habilidad de las entidades para implementar una gestión de riesgos que sea dinámica y que se ajuste al ritmo de cambio de las amenazas digitales.

Tabla 29

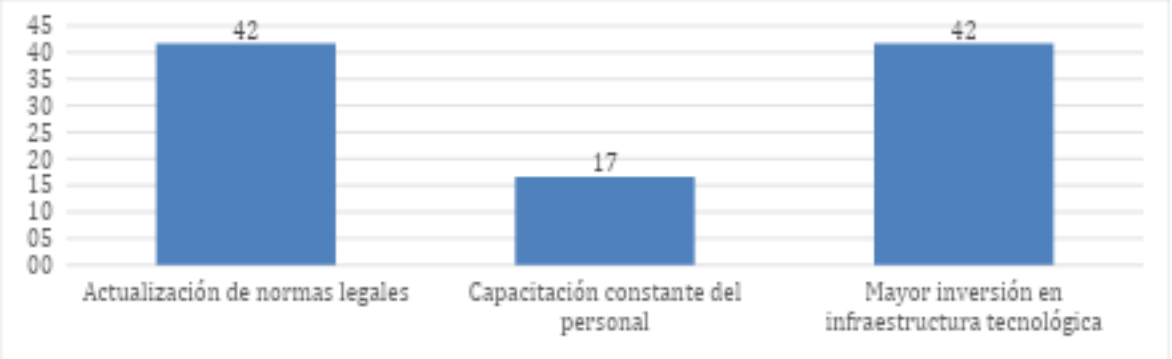
¿Qué medidas son más urgentes para fortalecer la ciberseguridad en el sistema financiero peruano?

	Frecuencia	Porcentaje
Actualización de normas legales	5	41,7
Capacitación constante del personal	2	16,7
Mayor inversión en infraestructura tecnológica	5	41,7
Total	12	100,0

Nota: Elaboración propia. 2025

Figura 17

¿Qué medidas son más urgentes para fortalecer la ciberseguridad en el sistema financiero peruano?



Nota: Elaboración propia. 2025

De la tabla y figura anterior, si bien un 41.7% de los profesionales considera que una de las medidas más urgentes para fortalecer la ciberseguridad en el sistema financiero peruano es una mayor inversión en infraestructura tecnológica, otro 41.7% considera que efectivamente la actualización de normas legales es de los temas más urgentes a nivel nacional, lo cual se encuentra dentro de lo explicado en la descripción del problema y denota la premura al respecto de la materia.

4.4.2. Consecuencias jurídicas de las vulneraciones a la privacidad del consumidor

El estudio de los incidentes de seguridad cibernética en el sistema financiero de Perú permite reconocer un impacto directo y posible en dos derechos fundamentales clave: la privacidad y el derecho a la autodeterminación informativa. La privacidad se pone en riesgo cuando la información personal o financiera, incluidos aspectos relacionados con los hábitos de compra o formas de actuar, se hace pública o puede ser utilizada sin permiso. Asimismo, la autodeterminación informativa se ve afectada cuando el consumidor pierde el control sobre el uso, la circulación o el almacenamiento de sus datos, ya sea a causa de brechas de seguridad, fallos en los sistemas de protección o falta de adecuadas medidas de seguridad adoptadas por las entidades financieras. Estos escenarios no solo crean riesgos económicos, sino también repercusiones en la vida personal del usuario, que pueden manifestarse en la pérdida de confianza, vulnerabilidad ante fraudes o

manipulaciones digitales, y un menoscabo en el principio de transparencia en el manejo de sus datos.

Ante este tipo de violaciones, las sanciones aplicadas por las autoridades administrativas deben ser analizadas conforme a los principios de razonabilidad y proporcionalidad, especialmente en el contexto de la supervisión llevada a cabo por la Autoridad Nacional de Protección de Datos Personales y la SBS. El principio de razonabilidad requiere que la penalización esté relacionada de manera lógica y adecuada con el nivel de gravedad del incumplimiento, teniendo en cuenta la naturaleza de la información afectada, el alcance del daño y el comportamiento de la entidad tanto antes como después del incidente.

Como lo analiza Montes Sánchez (2024), el marco jurídico en materia de protección de datos resulta, como se ha evidenciado, en insuficiente frente a los riesgos del sistema financiero digital, debido a la gran brecha que existe entre el inminente avance tecnológico y la capacidad que se tiene para dar respuesta por parte de la normativa, aun existiendo mecanismos como la responsabilidad civil y sanciones administrativas, las cuales son meramente de carácter reactivo, limitando la eficacia del mismo para prevenir vulneraciones al derecho de privacidad del consumidor. El énfasis de la asimetría de la información entre usuarios y entidades financieras dificulta una tutela de derechos efectiva, lo que por consecuencia, requiere un nuevo enfoque preventivo que tenga como prioridad unir la regulación, la educación digital y la supervisión, con el objetivo de garantizar la protección real de los derechos mencionados en nuestro sistema financiero peruano.

En dicho sentido, el uso indebido de la información del consumidor no solo trae como consecuencia sanciones administrativas impuestas a estas entidades, sino también la obligación de efectuar reparaciones civiles. No obstante, como advierte Letona (2025), esta eficacia que puede darse dentro de los mecanismos anteriormente mencionados, dependerá de la capacidad que tenga el sistema jurídico para adaptarse a los nuevos desafíos de la constante digitalización, siendo necesario fortalecer la regularización y garantizar la tutela efectiva de privacidad del consumidor frente a los riesgos inminentes.

De igual forma advierte Callirgos Silva (2024) que, el marco jurídico vigente no responde de forma suficiente a la complejidad de los nuevos escenarios tecnológicos y financieros, debido a la gran cantidad de tratamiento de datos y rápida evolución de

amenazas cibernéticas; situación que genera un escenario donde el consumidor, para proteger sus derechos, dependerá más de la capacidad de las entidades para autorregularse que de un control efectivo por parte de la normativa del estado.

4.5 Comparación del marco regulatorio peruano con legislaciones extranjeras

4.5.1 Modelos comparados: Unión Europea (RGPD), Estados Unidos y Latinoamérica

4.5.1.1 Estados unidos

Este país constituye un caso particular ya que es la única potencia en carecer de un conjunto unificado de leyes nacionales de privacidad de datos, y es que Estados Unidos posee una disposición legal en esta temática: la Ley de Privacidad del Consumidor de California (CPA), la cual sólo tiene injerencia en el estado de California y está inspirada en el Reglamento general de protección de dato (GDPR) de la Unión Europea (Quesada & Zeniquel, 2020).

Del mismo modo, según Lindner (2023) no existe una ley integral de privacidad financiera que pueda proteger a los consumidores de la recopilación, el intercambio y la venta de datos de los consumidores por parte de una empresa; la ley federal de privacidad financiera más reciente, la Ley Gramm-Leach-Bliley ("GLBA"), fue promulgada por el Congreso hace más de 20 años. Desde 1999 se han producido grandes cambios tecnológicos y financieros, y la ley de privacidad financiera debe actualizarse para seguir la carrera con la tecnología.

En la actualidad, Aunque existen normativas como el GDPR la Ley de informes de crédito justo (FCRA) o la privacidad del consumidor en california (CCPA) que limitan la libre divulgación de información confidencial por parte de las instituciones financieras también hay regulaciones como la Ley de Secreto Bancario de 1970 que obligan a estas entidades a compartir determinados datos financieros con organismos estatales con el fin de prevenir y combatir delitos financieros lo cual genera una tensión constante entre la protección de la privacidad y la necesidad de garantizar la integridad de las operaciones financieras (Chatzigiannis et al., 2023).

4.5.1.2 Unión Europea

A. España

En la actualidad el Estado español se rige por la Constitución de 1978 la cual incorpora disposiciones orientadas a la protección de los datos personales de sus ciudadanos, en ese sentido el artículo 18.4 incluido en la sección dedicada a los derechos fundamentales y libertades públicas establece que la ley limitará el uso de la información para garantizar el honor la intimidad personal y familiar de los ciudadanos así como el pleno ejercicio de sus derechos esta disposición fue pionera e importante ya que dio lugar a la creación de diversas normas y reglamentos que aseguran hasta hoy una tutela efectiva de este derecho adaptándose progresivamente a los avances tecnológicos surgidos en las últimas décadas (Pachecho, 2019).

Asimismo, el derecho a la protección de datos también cuenta con respaldo en el ámbito penal específicamente dentro de los delitos relacionados con el descubrimiento y la revelación de secretos tal como se establece en el apartado 2 del artículo 197 del Código Penal donde se sancionan aquellas conductas que debido a su gravedad requieren una respuesta penal adecuada (Fernandez, 2017).

Del mismo modo, acorde con Morales (2020) la creación de la Agencia Española de Protección de Datos tiene su origen en la Ley de Protección de Datos de 1992, la cual representó un hito importante para el desarrollo normativo en España ya que su función principal fue establecer límites claros en el tratamiento de datos personales tanto en el ámbito empresarial como en el de los ciudadanos y las entidades públicas actuando como un mecanismo esencial para evitar la libre circulación indiscriminada de datos y asegurar que toda actividad relacionada con su uso se rija por lo dispuesto en dicha ley.

B. Alemania

Actualmente las modalidades para obtener datos personales son más variados a diferencia del siglo pasado, por ello frente estas innovaciones el Estado Alemán ha adoptado medidas para contrarrestar aquellos actos que vulneren estos derechos, para ello creó “la Ley Federal de Protección de Datos (Federal Data Protection Act), es la normatividad vigente en Alemania, que existe desde 1977; es la ley principal que se encarga de desarrollar la legislación facultada para proteger los datos personales, dado que este derecho, no se encuentra regulado como tal dentro de la Constitución”; esto ha permitido una mayor tutela a los datos personales, más aún en esta era de las innovaciones tecnológicas que mantiene una relación con los datos personales mediante herramientas

tecnológicas como los bancos de datos que forman parte de una entidad de carácter público o privado (Pachecho, 2019).

4.5.1.3 Latinoamérica

C. México

México cuenta con un régimen particular destinado a la protección del consumidor financiero el cual se encuentra principalmente regulado por el Estatuto Orgánico de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros conocida como la Comisión Nacional así como por la Ley de Protección y Defensa al Usuario de Servicios Financieros que establece mecanismos específicos para resguardar los derechos de quienes utilizan servicios financieros en el país (Gómez et al., 2024).

Siguiendo esta línea, acorde con Arellano (2021) en cuanto a la situación actual en México se puede señalar que las disposiciones vigentes a nivel nacional han contribuido al fortalecimiento del Derecho a la Protección de Datos Personales generando obligaciones concretas tanto para el sector público como para el sector privado en aquellos casos en que intervengan en el tratamiento de información como parte de sus actividades o procesos institucionales.

No obstante en lo que respecta a la protección de datos personales México aún enfrenta importantes desafíos ya que el reconocimiento de este derecho no se ha consolidado plenamente como un derecho fundamental sino que ha sido abordado mayormente desde una perspectiva sectorial, es importante señalar que la protección de los datos personales constituye un derecho autónomo e independiente del derecho a la intimidad como lo ha establecido claramente el modelo europeo el cual ha sido adoptado progresivamente por numerosos países comprometidos con la garantía efectiva de este derecho (Garcia, 2017).

4.5.2 Evaluación de la aplicabilidad del derecho comparado al contexto peruano

La evaluación del derecho comparado en materia de protección de datos personales y ciberseguridad demuestra que la adopción de estándares internacionales no garantiza totalmente una protección efectiva de la privacidad del consumidor en los entornos digitales. Ante ello, Vasco Delgado et al. (2025) sostienen que, si bien el 89% de las legislaciones latinoamericanas han sido diseñadas siguiendo el modelo del RGPD, siguen

con las grandes brechas en su implementación, dando a conocer que aún persisten bajos niveles de cumplimiento empresarial, la insuficiente inversión en seguridad digital y la limitada educación financiera y/o digital de los usuarios respecto de la protección de datos personales. Manifestando así que se tiene un fenómeno de recepción normativa deficiente, por el cual la similitud formal de los marcos jurídicos no se traduce en una protección material efectiva, especialmente en sectores expuestos, como lo es en este caso, el sistema financiero.

Asimismo, Alvarado (2016) señala que la normativa peruana de protección de datos personales impone a los responsables del tratamiento la obligación de implementar medidas técnicas, organizativas y legales orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información; sin embargo, se advierte que la efectividad de la normativa de dichas medidas dependen de una gestión activa de los riesgos y del cumplimiento real del principio de seguridad, y que la falta de cumplimiento de este genera responsabilidad y dará sanciones. Por todo ello, la problemática según el autor no se centra únicamente en la existencia de normas, sino en la aplicación efectiva dentro del contexto que se encuentre el sistema jurídico caracterizado por sus limitaciones institucionales y tecnológicas.

Las leyes estadounidenses Gramm-Leach-Bliley Act (GLBA, 1999), California Consumer Privacy Act (CCPA, 2020) y Colorado Privacy Act (CPA, 2023) representan referentes modernos en materia de privacidad financiera y protección de datos personales, cuya implementación serviría como modelo útil para el Perú. La GLBA obliga a las entidades financieras y aseguradoras a informar de manera transparente a sus clientes sobre el uso de sus datos, y a permitirles negarse a que su información sea compartida con terceros (opt-out), además de exigir la adopción de medidas administrativas, técnicas y físicas que garanticen la seguridad de la información. En el contexto peruano, aplicar este tipo de disposiciones fortalecería la confianza en el sistema financiero y protegería el derecho constitucional a la intimidad establecido en el artículo 2, inciso 6, de la Constitución.

Por otro lado, la CCPA amplía los derechos de los consumidores al reconocerles la posibilidad de conocer, eliminar o impedir la venta de sus datos personales, evitando además cualquier trato desigual por ejercer dichos derechos. Incorporar principios similares en la legislación nacional complementaría los derechos ARCO contemplados en

la Ley N° 29733, reforzando el principio de legalidad y la autodeterminación informativa al establecer deberes concretos de transparencia y responsabilidad para las empresas. Asimismo, la CPA de Colorado, inspirada en el Reglamento General de Protección de Datos europeo (RGPD), introduce avances como el derecho a la portabilidad de datos, el consentimiento previo y expreso para el manejo de información sensible, y la obligación de realizar evaluaciones de impacto en privacidad (DPIA) antes de efectuar tratamientos de datos con alto nivel de riesgo. Su aplicación en el sector financiero digital peruano elevaría los estándares de ciberseguridad y fortalecería la confianza de los usuarios en las plataformas bancarias y fintech.

Desde el punto de vista constitucional, la incorporación de estos modelos resulta plenamente coherente con los principios que rigen el ordenamiento jurídico peruano. Refuerza el derecho a la intimidad personal y familiar, garantiza el principio de legalidad al establecer reglas claras sobre el uso de los datos personales y promueve la seguridad jurídica mediante la delimitación precisa de las obligaciones de las entidades financieras. A su vez, consolida el principio de igualdad ante la ley (art. 2.2 Const.) al evitar cualquier forma de discriminación contra quienes decidan ejercer su derecho a la privacidad. En conjunto, la implementación de estos estándares contribuiría a modernizar el marco normativo nacional y a garantizar una protección más efectiva de los derechos digitales y financieros de los ciudadanos peruanos.

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea (Reglamento 2016/679), vigente desde 2018, es considerado hoy el modelo más completo y exigente en materia de protección de datos personales y privacidad digital. Reconoce este derecho como parte esencial de la dignidad humana y establece un marco amplio que combina obligaciones claras, sanciones severas y aplicación más allá del territorio europeo. Su influencia ha sido determinante a nivel mundial, y su posible adaptación al contexto peruano resultaría coherente con nuestra Constitución, fortaleciendo la seguridad jurídica, la confianza de los ciudadanos y la transparencia en el sistema financiero digital.

El RGPD incorpora el principio de responsabilidad proactiva (accountability), que obliga a las organizaciones a no solo cumplir la norma, sino también a demostrar ese cumplimiento mediante políticas internas, registros y gestión de riesgos. A ello se suma el principio de privacidad desde el diseño y por defecto, que exige que la protección de los datos se integre desde la creación de los productos o servicios tecnológicos. En el Perú,

aplicar estos lineamientos significa que bancos y empresas fintech gestionen la información personal de forma más segura, anticipándose a los riesgos y garantizando una protección efectiva del derecho a la intimidad.

Entre sus principales aportes destacan los nuevos derechos reconocidos a los titulares de los datos, como el derecho a la portabilidad, que facilita trasladar la información personal de una entidad a otra, y el derecho al olvido digital, que permite solicitar la eliminación de datos antiguos o perjudiciales, equilibrando la privacidad con la libertad de expresión. El RGPD también impone la obligación de notificar las brechas de seguridad a la autoridad y a los afectados dentro de las 72 horas, fomentando la transparencia y la confianza en el entorno digital. Además, establece la figura del Delegado de Protección de Datos (DPO) en entidades públicas y privadas que manejen grandes volúmenes de información, garantizando el cumplimiento continuo de la normativa. Finalmente, su régimen sancionador —con multas de hasta 20 millones de euros o el 4% de los ingresos globales— y su alcance internacional obligan incluso a empresas extranjeras a respetar sus disposiciones.

Desde el punto de vista constitucional, adoptar los principios del RGPD sería plenamente compatible con el marco jurídico peruano. Reafirma el derecho a la intimidad y a la autodeterminación informativa reconocido en el artículo 2, inciso 6, de la Constitución, fortalece el principio de legalidad al imponer reglas precisas sobre el tratamiento de los datos y contribuye a la seguridad jurídica al establecer estándares claros para las entidades financieras y tecnológicas. Asimismo, garantiza la igualdad ante la ley (art. 2.2 Const.) al asegurar que todos los ciudadanos puedan ejercer sus derechos digitales de forma equitativa.

Actualizar la Ley N.º 29733 siguiendo el modelo europeo permitiría al Perú alcanzar los estándares internacionales de protección de datos, mejorar la confianza de los usuarios en los servicios financieros digitales y elevar la competitividad del país. A largo plazo, esta modernización podría incluso facilitar el reconocimiento de la Unión Europea como país con “nivel adecuado de protección”, favoreciendo el intercambio internacional de información y asegurando una defensa más sólida de los derechos digitales y financieros de los peruanos.

México se ha convertido en referente en la región por sus avances en la protección de datos personales, ofreciendo modelos que podrían orientar al Perú en la mejora de su

legislación, sobre todo ante el crecimiento del sistema financiero digital. En el caso de México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), vigente desde 2010, presenta un esquema sólido sustentado en los derechos ARCO (acceso, rectificación, cancelación y oposición) y en la obligación de contar con un Aviso de Privacidad. Este documento permite que las personas sepan quién usa sus datos, con qué propósito y cómo pueden ejercer sus derechos. Incorporar un modelo similar en el Perú fortalecería el principio de información recogido en la Ley N.º 29733, generando mayor transparencia en el vínculo entre entidades financieras y consumidores. Asimismo, México exige la implementación de medidas de seguridad técnicas y administrativas, y la comunicación de incidentes o filtraciones de datos, lo que contribuye a la prevención de fraudes y a la confianza digital. A esto se suma la labor del INAI, una autoridad autónoma con capacidad sancionadora, figura que el Perú podría imitar dotando de mayor independencia y recursos a su propia autoridad de protección de datos. Estas disposiciones encajan perfectamente con los principios constitucionales peruanos, pues refuerzan el derecho a la intimidad (art. 2.6), la seguridad jurídica y la legalidad al establecer mecanismos concretos de control.

Desde el punto de vista constitucional, el modelo mexicano resulta plenamente compatible con el orden jurídico peruano. Se apoya en la autodeterminación informativa, la protección de la vida privada y el principio de legalidad, todos reconocidos por la Constitución (arts. 2.6 y 200.3). Su adopción fortalecería la transparencia, la igualdad ante la ley (art. 2.2) y la confianza de los ciudadanos en el sistema financiero digital. Aplicar medidas como avisos de privacidad accesibles, protocolos de seguridad, mecanismos de notificación de brechas, sanciones efectivas y límites claros en el manejo de datos crediticios permitiría al Perú desarrollar un marco legal moderno y preventivo, coherente con sus principios constitucionales y con las demandas de la sociedad digital actual.

Tabla 29

Comparativa de normatividad peruana e internacional

Criterios	Normativa Peruana	Normas Internacionales
Sanción	La Ley N.º 29733 establece sanciones leves, graves y muy graves, con multas hasta 100 UIT. La aplicación corresponde a la Autoridad Nacional de Protección de Datos Personales (MINJUS).	El RGPD impone multas de hasta 20 millones de euros o el 4% de la facturación global; el INAI mexicano también aplica sanciones altas. EE.UU. (GLBA/CCPA) impone sanciones proporcionales al daño causado.
Requisitos de seguridad cibernética	Se exige adoptar medidas técnicas y organizativas razonables para garantizar la confidencialidad y seguridad (art. 9 Ley 29733), pero sin protocolos técnicos específicos.	El RGPD y la GLBA imponen programas integrales de seguridad, evaluaciones de riesgo, cifrado, control de acceso y notificación de brechas. México exije medidas administrativas, técnicas y físicas, además de la comunicación de vulneraciones.
Derechos del titular (ARCO)	Reconoce los derechos de acceso, rectificación, cancelación y oposición, similares a los estándares internacionales.	El RGPD, la CCPA y la CPA amplían los derechos con portabilidad, olvido digital y no venta de datos. México exige avisos claros para el ejercicio de estos derechos.
Aviso o política de privacidad	Solo obliga a informar al titular (art. 18), sin formato estándar.	En México y la UE es obligatorio un Aviso de Privacidad accesible que detalle identidad, finalidad, transferencias y contacto del DPO.
Consentimiento para el tratamiento	Debe ser expreso e inequívoco para todo dato personal (art. 12), salvo excepciones (art. 14).	México admite consentimiento tácito para datos no sensibles; el RGPD y CPA exigen consentimiento explícito; EE.UU. aplica modelos opt-in/opt-out.

Notificación de brechas de seguridad	Recientemente se aplicó mediante Decreto Supremo N.° 016-2024-JUS la implementación de este, pero al ser nuevo no se tiene mucha información de su actuar y eficiencia	El RGPD obliga a notificar en 72 horas a la autoridad y a los afectados; México exige aviso inmediato en casos graves.
Autoridad de control y supervisión	La Dirección General de Protección de Datos (MINJUS) depende del Ejecutivo y tiene recursos limitados.	El INAI (México), las autoridades europeas es autónoma y con poder sancionador, garantizando mayor eficacia.
Transferencias internacionales de datos	Permitidas solo a países con nivel adecuado de protección o con consentimiento del titular.	El RGPD regula mediante cláusulas tipo, decisiones de adecuación y normas corporativas. México tiene requisitos similares.
Responsabilidad proactiva (accountability)	No está desarrollada expresamente, aunque se deduce del deber de seguridad.	El RGPD la convierte en obligación: las empresas deben demostrar cumplimiento mediante registros, políticas y DPIA.
Delegado de Protección de Datos (DPO)	Recientemente se aplicó mediante Decreto Supremo N.° 016-2024-JUS la implementación de este, pero al ser nuevo no se tiene mucha información de su actuar y eficiencia	El RGPD exige DPO en entidades públicas o que traten datos a gran escala y México avanza en su adopción.
Enfoque sectorial financiero	Regulado por la SBS y normas sobre secreto bancario.	EE.UU. (GLBA) tiene normas específicas para datos financieros, con reglas de conservación y confidencialidad.

4.6. Propuesta de Ente Supervisor

La presente propuesta tiene como finalidad instituir un Ente Rector en materia de Ciberseguridad y Protección de Datos Personales en el Sistema Financiero — con investidura, capacidad sancionadora y función pedagógica hacia el ciudadano — que opere en el marco del ordenamiento jurídico peruano, en armonía con el principio constitucional de protección de la privacidad (art. 2, inc. 6 de la Constitución Política del Perú) y sin generar barreras innecesarias a la inversión privada.

4.6.1. Fundamentación jurídica de la propuesta

A. Exposición de motivos

a) Insuficiencia del régimen actual

El sistema financiero peruano opera en un entorno de acelerada digitalización que contrasta con la lentitud de su marco normativo. La Ley N.° 29733, promulgada en el año 2011 y reglamentada en 2013, fue concebida en un contexto tecnológico radicalmente distinto al actual, cuando la banca digital, las billeteras electrónicas y el procesamiento masivo de datos mediante inteligencia artificial no habían alcanzado la penetración que hoy exhiben. El resultado es un régimen jurídico que reconoce derechos en el papel, pero carece de los mecanismos institucionales, procedimentales y sancionadores necesarios para hacerlos efectivos. La evidencia empírica recogida en la presente investigación es elocuente: más de 22,000 denuncias ante la ANPDP contra entidades como Interbank, BBVA y Scotiabank, con sanciones que no superan las 100 UIT (equivalentes a S/ 525,000) frente a entidades cuyos ingresos anuales se miden en miles de millones de soles. Esta brecha entre la norma y la realidad constituye la premisa fundamental que justifica la presente propuesta.

b) La dificultad probatoria del consumidor

El régimen de responsabilidad civil ordinario exige que quien reclama un daño acredite la conducta antijurídica, el nexo causal y el perjuicio sufrido. En el contexto de las vulneraciones de datos personales en entornos financieros digitales, esta carga resulta manifiestamente inequitativa: el consumidor carece de acceso a los sistemas, registros y logs internos de la entidad financiera que permitirían demostrar el origen y alcance de la brecha de seguridad. La asimetría tecnológica y

de información entre el ciudadano y una institución financiera de gran escala convierte el ejercicio del derecho al resarcimiento en una ilusión práctica. Esta dificultad probatoria se agrava por la fragmentación institucional vigente: el consumidor que sufre una vulneración de sus datos personales en el contexto financiero no tiene claro si debe acudir a la ANPDP, a INDECOPI, a la SBS o al Poder Judicial. La ausencia de una ventanilla única genera desistimiento, desinformación y, en última instancia, impunidad para las entidades infractoras.

c) El riesgo creado en entornos digitales

Las entidades financieras que operan en el entorno digital asumen voluntariamente el beneficio económico derivado del tratamiento masivo de datos personales de sus clientes. Este beneficio genera, correlativamente, una posición de garante respecto de la seguridad de dicha información. Bajo la teoría del riesgo creado — recogida en el ámbito peruano por el artículo 1970 del Código Civil — quien introduce en la sociedad una actividad generadora de riesgos especiales debe responder objetivamente por los daños que de ella se deriven, independientemente de la existencia de culpa. El tratamiento de millones de registros financieros sensibles mediante plataformas digitales expuestas a actores maliciosos sofisticados es, per se, una actividad de riesgo especial que justifica este estándar de responsabilidad.

B. Identificación de la brecha normativa

El siguiente análisis sistematiza lo que regula y lo que omite la Ley N.° 29733 y su normativa conexa, con énfasis en los vacíos directamente vinculados a las brechas de seguridad en el sistema financiero digital:

Ámbito normativo	Lo que sí regula la Ley N.° 29733	Vacío o deficiencia identificada
Consentimiento informado	Art. 5: exige consentimiento previo, informado y libre para el tratamiento de datos.	No prevé mecanismos de consentimiento específicos para entornos digitales ni cláusulas de adhesión en aplicaciones bancarias.
Notificación de incidentes	No existe disposición expresa de notificación al titular de datos ni a la autoridad competente ante una brecha de seguridad.	Vacío crítico: el RGPD exige notificación en 72 horas.
Régimen sancionador	Art. 38: multas de hasta 100 UIT (≈ S/ 525,000).	Carece de efecto disuasorio real frente a entidades con facturaciones millonarias. Sin proporcionalidad respecto al daño causado ni al tamaño económico del infractor.
Supervisión de terceros	Art. 16: referencia general al encargado del tratamiento.	No regula expresamente la supervisión de proveedores tecnológicos externos (cloud, procesadores de pago, fintechs) que acceden a datos sensibles de consumidores.
Derecho al olvido digital	Art. 20: reconoce el derecho de cancelación en bancos de datos específicos.	No contempla el derecho al olvido en el entorno financiero digital ni en plataformas de terceros. Contradicción con el principio constitucional de protección a la intimidad.
Inteligencia artificial	No existe regulación alguna sobre el uso de algoritmos o IA en el tratamiento de datos financieros.	Vacío normativo absoluto frente al uso creciente de scoring crediticio algorítmico, análisis de comportamiento financiero y perfilamiento de consumidores.
Autoridad competente	ANPDP: fiscaliza el cumplimiento de la ley. SBS: supervisa riesgos operacionales.	Fragmentación institucional: sin coordinación formal entre ANPDP, SBS, INDECOPI, PCM/CNSD, DINI y PNP Cibercrimen. El consumidor no sabe a dónde acudir.

Nota: Elaboración propia en base al análisis normativo comparado. 2025.

4.6.2. Configuración del régimen de responsabilidad reforzada

I. Creación, Naturaleza Jurídica y Adscripción Institucional

La SUCYBER se concibe como un organismo público técnico especializado, con personería jurídica de derecho público interno, autonomía técnica, funcional y presupuestal, en línea con el modelo institucional de la Superintendencia de Banca, Seguros y AFP (SBS), recogido en la Ley General del Sistema Financiero (Ley N.° 26702). Su creación requeriría de una ley orgánica o decreto legislativo delegado, en el marco de las facultades conferidas al Poder Ejecutivo por el Congreso de la República.

Denominación oficial	Superintendencia de Ciberseguridad y Protección de Datos del Sistema Financiero — SUCYBER
Naturaleza jurídica	Organismo público técnico especializado con autonomía funcional, técnica y administrativa
Adscripción	Ministerio de Economía y Finanzas (MEF), bajo supervisión del Consejo de Ministros
Financiamiento	Presupuesto público + aportes regulatorios de las entidades supervisadas (modelo SBS)
Sede principal	Lima, con oficinas descentralizadas en Arequipa, Trujillo, Cusco y Piura
Marco normativo base	Constitución Política del Perú (art. 2 inc. 6), Ley N.° 26702, Ley N.° 29733, Ley N.° 30618, Ley N.° 27658 (Modernización del Estado)

La adscripción al MEF responde a la necesidad de articular la política de ciberseguridad financiera con la política económica nacional, garantizando que las decisiones regulatorias sean compatibles con los objetivos de inclusión financiera, fomento de la inversión privada y competitividad del sistema financiero peruano. A efectos de no duplicar competencias, la SUCYBER coordinará obligatoriamente con la SBS — que continuará ejerciendo la supervisión prudencial — y con la ANPDP — que mantendrá competencia residual sobre sectores no financieros — bajo un protocolo de actuación conjunta establecido por Decreto Supremo.

II. Principios Rectores de la SUCYBER

El diseño institucional de la SUCYBER se inspira en los siguientes principios, que orientan tanto su actuación regulatoria como su relacionamiento con el ciudadano y el sector privado:

Principio	**Contenido**	**Fundamento normativo**
Proporcionalidad	Las medidas regulatorias y sanciones deben ser proporcionales al riesgo creado, al daño causado y al tamaño económico del sujeto obligado. Se evitarán requisitos que generen barreras de entrada innecesarias a la innovación.	Art. IV LPAG; art. 230 LPAG; RGPD art. 83
Accesibilidad ciudadana	Toda comunicación institucional, reglamento o procedimiento administrativo de la SUCYBER deberá redactarse en lenguaje claro, comprensible para el ciudadano común, sin tecnicismos difíciles.	Ley N.° 31419; Política de Modernización del Estado (DS 004-2013-PCM)
Neutralidad tecnológica	La regulación no privilegiará ni discriminará tecnologías específicas, favoreciendo la innovación y la libre competencia en el mercado fintech.	Política Nacional de Transformación Digital (2024)
Transparencia y rendición de cuentas	La SUCYBER publicará anualmente un informe de gestión, estadísticas de incidentes reportados, sanciones impuestas y estado de cumplimiento del sector.	Ley N.° 27806 (Transparencia y Acceso a la Información Pública)
Cooperación institucional	Actuación coordinada con la SBS, ANPDP, INDECOPI, PCNSD, DINI y PNP-Cibercrimen, bajo protocolos formales que eliminen la fragmentación actual.	Ley N.° 27658 (Modernización del Estado)

No regresividad en derechos	Ninguna norma emitida por la SUCYBER podrá reducir el nivel de protección de los derechos fundamentales a la privacidad e intimidad ya reconocidos.	Constitución Política, art. 2 inc. 6; art. 44

III. Funciones y Atribuciones de la SUCYBER

A. Función regulatoria y normativa

La SUCYBER ostentará potestad normativa para dictar reglamentos de obligatorio cumplimiento para todas las entidades del sistema financiero sujetas a su supervisión, incluyendo bancos, cajas municipales, financieras, empresas de seguros, AFP, plataformas fintech y proveedores de servicios de pago. Esta potestad se ejercerá mediante reglamentos de desarrollo, circulares y guías técnicas, con sujeción estricta al principio de jerarquía normativa y a la habilitación legal que provea su ley de creación. A diferencia de la regulación técnica compleja que caracteriza normas como la Circular SBS G-140-2018, los instrumentos normativos de la SUCYBER observarán el principio de lenguaje claro: cada obligación deberá poder expresarse de forma comprensible para el empresario, el operador y el ciudadano, sin perjuicio de los anexos técnicos especializados de uso interno.

Dentro de sus funciones, la SUCYBER estará facultada para:

- Dictar estándares mínimos de ciberseguridad para el sistema financiero.
- Aprobar el Reglamento de Notificación de Incidentes de Seguridad, estableciendo un plazo máximo de 72 horas desde la detección de la brecha.
- Regular el uso de inteligencia artificial y algoritmos en el tratamiento de datos financieros, exigiendo auditorías periódicas y explicabilidad.
- Establecer el marco de evaluación de riesgos de proveedores tecnológicos externos que accedan a datos de consumidores financieros.
- Actualizar periódicamente (cada 2 años) sus reglamentos para evitar la obsolescencia normativa frente al avance tecnológico.

B. Función supervisora y de fiscalización

La SUCYBER ejercerá supervisión permanente sobre el cumplimiento del marco normativo en materia de ciberseguridad y protección de datos personales por parte de las entidades financieras supervisadas. Esta supervisión se articulará con la SBS — que

conserva la supervisión prudencial y financiera — mediante un protocolo de actuación conjunta, evitando duplicidades y cargas regulatorias innecesarias.

Dentro de las funciones de supervisión y fiscalización, la SUCYBER podrá:

- Practicar inspecciones ordinarias y extraordinarias a las entidades supervisadas.
- Requerir información, documentación y acceso a sistemas ante la detección de posibles incidentes.
- Supervisar el cumplimiento de los planes de gestión de riesgos cibernéticos y los planes de continuidad de negocio.
- Verificar la adecuada gestión de proveedores tecnológicos externos (outsourcing de datos).

C. Función sancionadora

La SUCYBER estará investida de plena potestad sancionadora administrativa, ejercida a través de un procedimiento sancionador que garantice el derecho al debido proceso, la contradicción y la proporcionalidad de las sanciones. El régimen sancionador se diseñará con criterios disuasorios reales, tomando como referencia el modelo del RGPD europeo en cuanto a proporcionalidad, sin que ello implique trasladar automáticamente su escala a la realidad peruana.

Las sanciones podrán ir acompañadas de medidas correctivas obligatorias (planes de acción con plazos definidos) y, en casos de extrema gravedad, de la suspensión temporal de la autorización para operar servicios digitales que involucren el tratamiento de datos personales. La determinación de la sanción considerará siempre los criterios de razonabilidad, proporcionalidad y efecto disuasorio real, garantizando que no resulte más económico incumplir que invertir en seguridad.

Tipo de infracción	**Supuesto**	**Sanción máxima**
Leve	Incumplimiento formal: falta de registro de actividades de tratamiento, retraso en la notificación de incidentes de menor entidad.	Hasta 50 UIT (≈ S/262,500)
Grave	Tratamiento de datos sin base legal, falta de implementación de medidas mínimas de	De 50 a 200 UIT

	seguridad, cesión no autorizada de datos a terceros.	(≈ S/ 1,050,000)
Muy grave	Vulneración masiva de datos personales con afectación a consumidores, reincidencia, ocultamiento de incidentes, uso no autorizado de datos biométricos o financieros sensibles.	De 200 a 1,000 UIT o hasta el 2% de los ingresos anuales de la entidad, lo que resulte mayor (≈ hasta S/ 5.25M o más)

D. Función de atención ciudadana y concientización

La SUCYBER asumirá como función estratégica la educación, concientización e información al consumidor financiero. Este es el elemento que la distingue cualitativamente de la ANPDP y la SBS: ser el referente ciudadano al que cualquier peruano pueda acudir cuando sienta que sus datos personales o su seguridad digital en el sistema financiero han sido vulnerados.

Mecanismo	Descripción
Portal ciudadano 'Mi Dato Seguro'	Plataforma digital de fácil uso y lenguaje accesible, donde el ciudadano puede presentar denuncias, consultar el estado de su queja, conocer sus derechos y acceder a guías prácticas de seguridad digital financiera.
Línea gratis 0800-SUCYBER	Línea telefónica gratuita de atención 24/7 para reportar incidentes en tiempo real, con protocolo de derivación urgente cuando se detecte fraude activo o robo de identidad financiero.
Campañas anuales de concientización	Al menos dos campañas nacionales por año, en coordinación con el MEF, MINEDU y municipalidades, orientadas a difundir derechos del consumidor financiero digital en lenguaje llano, incluidos formatos accesibles para adultos mayores y personas con discapacidad.

Sello 'SUCYBER Verificado'	Certificación voluntaria de buenas prácticas de ciberseguridad y protección de datos para entidades financieras, que podrán exhibirla como señal de confianza ante el consumidor y como factor favorable en procedimientos sancionadores.
Informe anual de transparencia	Publicación anual de estadísticas de incidentes reportados, sanciones impuestas, tipos de vulneraciones más frecuentes y nivel de cumplimiento del sector, en formato de acceso público y lenguaje ciudadano.

IV. Elementos del Régimen de Responsabilidad Reforzada

La SUCYBER administrará el siguiente régimen de responsabilidad especial para las entidades del sistema financiero, que opera de forma complementaria — y con prevalencia en el ámbito sectorial — respecto al régimen civil ordinario y al régimen administrativo sancionador general:

A. Supuesto de Aplicación

El régimen de responsabilidad reforzada se activa ante la ocurrencia de incidentes de seguridad entendidos como cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de datos personales de consumidores financieros. Los supuestos de aplicación incluyen, de manera enunciativa y no limitativa:

- Acceso no autorizado a bases de datos financieras por parte de terceros.
- Filtración, divulgación o publicación indebida de datos personales o financieros.
- Pérdida, alteración o destrucción no autorizada de información de consumidores.
- Suplantación de identidad facilitada por deficiencias de seguridad de la entidad.
- Uso no autorizado de datos biométricos, financieros o de comportamiento del consumidor.

Texto propuesto — Artículo X (Supuesto de aplicación):
Las entidades del sistema financiero serán responsables por los daños y perjuicios ocasionados a los consumidores como consecuencia de incidentes de seguridad que impliquen la vulneración de datos personales, incluyendo, entre otros, accesos no autorizados, filtraciones, pérdida, alteración o divulgación

indebida de información. Esta responsabilidad es independiente de la acción sancionadora administrativa que corresponda a la SUCYBER.

B. Naturaleza de la Responsabilidad

La responsabilidad establecida es de naturaleza objetiva, en concordancia con la teoría del riesgo creado recogida en el artículo 1970 del Código Civil peruano y con el modelo europeo del RGPD (arts. 82 y 83). Ello significa que el consumidor afectado no está obligado a demostrar dolo o negligencia de la entidad financiera: basta con acreditar la existencia del incidente, los datos comprometidos y el daño sufrido. Este estándar se justifica por la posición privilegiada que ocupan las entidades financieras en el control de la infraestructura tecnológica donde se producen las vulneraciones.

Texto propuesto — Artículo Y (Naturaleza de la responsabilidad):
La responsabilidad establecida en el presente artículo es de carácter objetivo, por lo que no será necesario acreditar dolo o culpa por parte de la entidad financiera, bastando la existencia del daño y su vinculación con el tratamiento de datos personales en el marco de sus actividades.

C. Inversión de la Carga de la Prueba

En coherencia con la naturaleza objetiva de la responsabilidad y con la asimetría de acceso a la información que caracteriza la relación consumidor-entidad financiera, la carga de la prueba se invierte: es la entidad financiera quien debe demostrar que el incidente no le es imputable. Esta inversión no es arbitraria: la entidad financiera es quien tiene acceso directo a los registros técnicos, logs del sistema, protocolos de seguridad y auditorías internas que permiten reconstruir el origen y alcance de cualquier vulneración.

Texto propuesto — Artículo Z (Carga de la prueba):
Corresponde a la entidad financiera acreditar que el incidente de seguridad no le es imputable, demostrando el cumplimiento efectivo de los estándares de seguridad exigibles y la adopción de medidas idóneas para prevenir la ocurrencia del evento. La entidad financiera deberá conservar durante un mínimo de cinco (5) años los registros técnicos, logs de sistema y auditorías de seguridad que permitan verificar dicho cumplimiento.

D. Causales de Exoneración

El régimen objetivo no implica responsabilidad absoluta. La entidad financiera podrá exonerarse total o parcialmente cuando acredite fehacientemente la concurrencia de alguna de las siguientes causales, interpretadas de manera restrictiva por la SUCYBER:

Texto propuesto — Artículo W (Causales de exoneración):
La entidad financiera solo podrá exonerarse de responsabilidad cuando acredite de manera fehaciente la concurrencia de caso fortuito o fuerza mayor, o el cumplimiento integral de estándares técnicos de seguridad reconocidos, junto con la implementación efectiva de mecanismos de prevención, detección y respuesta frente a incidentes de ciberseguridad. La exoneración deberá ser declarada expresamente por la SUCYBER en el marco del procedimiento administrativo correspondiente.

Causal	**Descripción**	**Carga probatoria**
Caso fortuito o fuerza mayor	Eventos externos, imprevisibles e irresistibles que hayan causado directamente la vulneración, sin que medida alguna razonablemente exigible hubiera podido prevenirla.	La entidad debe demostrar la inevitabilidad del evento y la ausencia de negligencia previa en sus sistemas de seguridad.
Cumplimiento integral de estándares certificados	La entidad deberá acreditar el cumplimiento íntegro de los estándares técnicos de seguridad establecidos por la SUCYBER mediante certificación por auditor independiente acreditado, junto con la implementación efectiva de mecanismos de prevención, detección y respuesta ante incidentes.	Certificado vigente de auditor independiente acreditado ante SUCYBER + registros de los planes de respuesta a incidentes activados.
Culpa exclusiva del	Cuando el incidente sea consecuencia directa de la conducta imprudente del propio consumidor (ej.: compartición	Corresponde a la entidad probar de manera fehaciente la

afectado	voluntaria de credenciales, instalación deliberada de software malicioso).	conducta del consumidor, sin que esta exoneración sea aplicable cuando la entidad omitió advertirle oportunamente sobre los riesgos.

CONCLUSIONES

Primera conclusión: Se concluye que los desafíos jurídicos de la ciberseguridad en el sistema financiero peruano evidencian limitaciones estructurales en el marco normativo vigente, las cuales inciden de manera directa en la tutela insuficiente del derecho fundamental a la privacidad del consumidor. En particular, se advierte una brecha entre el alcance de las disposiciones legales actuales y las exigencias derivadas del entorno digital, lo que pone en cuestión la eficacia del presente sistema jurídico para responder a los riesgos asociados al tratamiento de datos personales en el ámbito financiero.

Segunda conclusión: Se concluyó que la efectividad de la Ley N° 29733 y demás normas conexas como del Código de Protección y Defensa del Consumidor (Ley N.º 29571), como la Ley de Seguridad Digital (Ley N.º 30618), el Decreto Legislativo N.º 1353 y su reglamento (D.S. N.º 003-2013-JUS) establecen un marco general de protección de datos personales; sin embargo, presentan limitaciones en su aplicación frente a escenarios propios del entorno financiero digital, especialmente en lo referido a la gestión de incidentes de ciberseguridad, la supervisión de actores involucrados en el tratamiento de datos y la respuesta jurídica ante vulneraciones, lo que evidencia una insuficiencia en la protección efectiva del derecho a la privacidad.

Tercera conclusión: Se establece que, en el modelo actual de protección de datos personales en el sistema financiero, el consumidor ocupa una posición de vulnerabilidad estructural derivada de la asimetría informativa y tecnológica frente a las entidades financieras, lo que limita su capacidad real de control sobre el tratamiento de su información personal y reduce la eficacia de los mecanismos de consentimiento y autodeterminación informativa previstos en la normativa vigente.

Cuarta conclusión: Se identifica que las principales debilidades del sistema financiero peruano en materia de ciberseguridad se vinculan con vacíos normativos y limitaciones regulatorias frente a riesgos emergentes, tales como el tratamiento automatizado de datos, la intervención de terceros tecnológicos y las nuevas modalidades de fraude digital, lo que genera escenarios de afectación al derecho a la privacidad que no se encuentran plenamente cubiertos por el marco jurídico actual.

Quinta conclusión: Se concluye que, en comparación con otros ordenamientos jurídicos, tales como el europeo, el sistema jurídico peruano presenta un menor desarrollo en la regulación de la protección de datos en entornos digitales complejos, particularmente

en aspectos vinculados a la responsabilidad de los agentes, los mecanismos de control y la gestión de riesgos, lo que evidencia la necesidad de estándares más avanzados que permitan una tutela más efectiva del derecho a la privacidad en el ámbito financiero.

Sexta conclusión: Se identificó que la fragmentación normativa, los vacíos regulatorios y la dispersión institucional en materia de privacidad financiera justifican la creación de un ente rector especializado: la SUCYBER. Este organismo, adscrito al MEF y con autonomía, centralizaría funciones actualmente dispersas, contaría con potestad sancionadora más eficaz (hasta 1,000 UIT o 2% de ingresos) y promovería la educación del consumidor. La propuesta busca fortalecer la seguridad jurídica sin afectar la inversión. Se concluye que su implementación permitiría superar la desarticulación normativa, reforzar la responsabilidad de las entidades financieras y garantizar una protección efectiva del derecho a la privacidad conforme a estándares internacionales.

Séptima conclusión: Los resultados estadísticos obtenidos de consumidores y profesionales del derecho reflejan la magnitud de las brechas existentes en materia de ciberseguridad y protección de datos en el sistema financiero peruano. Si bien el 96.1% de consumidores utiliza aplicaciones bancarias digitales, apenas el 37.3% se siente seguro al operar en línea, y solo el 52.9% conoce su derecho a solicitar información sobre el uso que el banco da a sus datos personales. A su vez, el 75% de los profesionales consultados estima que las medidas adoptadas por las entidades financieras son insuficientes para proteger la privacidad del consumidor, y el 91.7% considera que debería existir una obligación legal de notificación de incidentes. Estos resultados configuran un escenario de vulnerabilidad estructural que demanda una respuesta institucional integral. Se concluye que los datos empíricos recogidos en la presente investigación corroboran la existencia de una brecha significativa entre el nivel de protección que la normativa peruana reconoce formalmente al consumidor financiero digital y el que este efectivamente recibe en la práctica, evidenciando la necesidad urgente de fortalecer los mecanismos de supervisión, sanción y educación ciudadana en materia de ciberseguridad y protección de datos personales en el sistema financiero peruano.

RECOMENDACIONES

Primera recomendación: Se recomienda realizar un reforzamiento normativo conjuntamente con la modernización de la Ley N° 29733 – Ley de Protección de Datos Personales, con el fin de abordar los desafíos jurídicos en cuanto a la digitalización en el sistema financiero y garantizar la tutela de derechos a la privacidad del consumidor. Estas reformas deben de incluir expresamente el derecho al olvido digital, la obligatoriedad de notificación de incidentes de seguridad en un plazo máximo de 72 horas, la regulación del uso de algoritmos e inteligencia artificial, y una revisión periódica que impida que la norma quede obsoleta, porque estamos en una materia donde el derecho tiene que avanzar a la par de la sociedad.

Segunda recomendación: Para fortalecer la efectividad de la Ley N° 29733 y demás normas conexas como del Código de Protección y Defensa del Consumidor (Ley N.º 29571), la Ley de Seguridad Digital (Ley N.º 30618), el Decreto Legislativo N.º 1353 y su reglamento (D.S. N.º 003-2013-JUS), se recomienda poner como lineamiento de la normativa peruana los estándares internacionales en materia de protección de datos, adoptando en casos necesarios los mecanismos como las cláusulas contractuales, las certificaciones de adecuación y los estándares de cifrado y seguridad digital recomendados por la OCDE e ISO.

Tercera recomendación: Se recomienda hacer un fortalecimiento tanto de la educación como de la cultura digital del consumidor, debido a que ambos constituyen el pilar frágil dentro del ecosistema financiero. Para esto, se recomiendo implementar un plan nacional de educación digital, el mismo que contempla 3 niveles: 1. En la educación primaria y secundaria se incorporarán nociones, conceptos e ideas sobre la privacidad y ciberseguridad, conforme al art. 33 de la Ley 29733; 2. En la educación universitaria, obligar a las universidades e institutos a incluir dentro de las mallas curriculares cursos sobre privacidad y ciberseguridad en las carreras de Derecho, Economía e ingeniería, mientras que en las demás carreras implementar charlas informativas obligatorias respecto al tema; 3. A nivel ciudadano, promover campañas de concientización digeridas por los principales organismos (SBS e INDECOPI) para la prevención de fraudes como el phishing, malware y robo de identidad. Asimismo, se recomienda la creación de una plataforma virtual única administrada para la autoridad competente en la protección de datos personales, que tendrá como objetivo el facilitar el ejercicio de los derechos ARCO,

evitando así que el consumidor tenga que acudir entidad por entidad para garantizar su tutela de derechos.

Cuarta recomendación: Se recomienda establecer la obligación legal expresa para todas las entidades del sistema financiero sin excepción, en cuanto a la implementación de estándares reforzados de seguridad y protección de datos personales, incorporando siempre el principio de responsabilidad proactiva al tratamiento de información sensible de los consumidores, debido a ello las entidades deberán acreditar dicho cumplimiento con diferentes medidas técnicas y organizativas, fomentando diversas campañas a los consumidores para evitar la mala diligencia del consumidor.

Quinta recomendación: Para elevar el nivel regulatorio del Perú a los estándares internacionales, se recomendaría fomentar alianzas tanto públicas como privadas sobre la ciberseguridad, todo ello permitiría compartir información en tiempo real sobre las amenazas presentes, desarrollar centros de innovación tecnológica y formar especialistas en la materia. Del mismo modo, se debe incorporar un sistema de auditorías algorítmicas independientes, con el fin de verificar el cumplimiento de transparencia y la falta de sesgos en los servicios o mecanismos de las instituciones financieras que usen inteligencia artificial.

Las alianzas para auditorías de algoritmos en el sistema financiero de Perú podrían establecerse principalmente con organizaciones que tienen un alto grado de uso de tecnologías automatizadas y decisiones digitales. Entre las entidades más relevantes se encuentran Banco de la Nación, BCP, Interbank, BBVA, Scotiabank y, así como Cajas Municipales y cooperativas altamente digitalizadas. En el ámbito regulador, la SBS y Indecopi jugarían un papel fundamental en la supervisión, validación de informes y garantía de estándares de transparencia y protección del consumidor. Estas colaboraciones facilitan la revisión de modelos de riesgo, evaluación crediticia y procedimientos de atención automatizados, disminuyendo sesgos, aumentando la confianza y mejorando la calidad de las prácticas relacionadas con la protección de datos en el sector financiero.

Sexta recomendación: Se recomienda la creación de la Superintendencia de Ciberseguridad y Protección de Datos del Sistema Financiero (SUCYBER), organismo técnico especializado adscrito al Ministerio de Economía y Finanzas, con autonomía funcional y potestad sancionadora proporcional al tamaño económico de las entidades infractoras. La SUCYBER centralizaría las competencias hoy dispersas entre la ANPDP, la

SBS, INDECOPI y la PCM, estableciendo un régimen de responsabilidad objetiva para las entidades financieras ante brechas de seguridad, e implementaría a su vez mecanismos de atención ciudadana accesibles, como el portal digital, una línea gratuita y campañas anuales de concientización en un lenguaje claro para que cualquier consumidor sepa a dónde acudir cuando sienta vulnerada su privacidad financiera. Su diseño debe priorizar normas predecibles y proporcionadas que generen confianza en el ciudadano sin desincentivar la inversión privada en el sector.

REFERENCIAS BIBLIOGRÁFICAS

24th Annual Global CEO Survey. (2021, 10 03). *A leadership agenda to take on tomorrow*. https://www.pwc.com/gx/en/ceo-survey/2021/reports/pwc-24th-global-ceo-survey.pdf

Aftergood, S. (2017, Julio 06). The Cold War Online. *Nature*. https://www.nature.com/articles/547030a

Aguilar, A. (2021, Enero 25). *Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior*. Scielo Chile. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-37692021000100169

Alvarado, F. J. (2016). La gestión de la Seguridad de la Información en el régimen peruano de Protección de Datos Personales.

Andrés, M. (2023). Los principios estructurales del reglamento general de protección de datos. *Actualidad Jurídica Iberoamericana*, (20). oemmndcbldboiebfnladdacbdfmadadm/https://roderic.uv.es/rest/api/core/bitstreams/d2b92140-2266-4eb6-8fd1-8608c52f79ac/content

Astorga Aguilar, C., & Schmidt Fonseca, I. (2019, Octubre 30). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. *Revista Electrónica Educare*, *23*. https://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S1409-42582019000300339

Autoridad Nacional de Proteccion de Datos Personales. (2020). *Resolución Directoral N.° PAS: BANCO BBVA PERÚ S.A*. https://cdn.www.gob.pe/uploads/document/file/3716608/RD%202196-2020-JUS/DGTAIPD-DPDP.pdf?v=1664825539

Agencia española proteccion datos. (2023). https://www.aepd.es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido

Bermudez Hercilla, M. d. G. (2024). “La protección de los datos personales, frente a la vulneración al derecho a la intimidad, en el sistema financiero- bancario de Lima-Perú, 2023.” *Facultad de Derecho y Ciencias Humanas Universidad Tecnológica del Perú*.

Borbúa, V. (2017, Junio). *Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa*. SciELO Ecuador. Retrieved July 15, 2025, from http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-42992017000200031

Bullard, A. (2010). *¿Es el consumidor un idiota? El falso dilema entre el consumidor razonable y el consumidor ordinario*. *Revista de la Competencia y la Propiedad Intelectual, 6*(10). https://revistas.indecopi.gob.pe/index.php/rcpi/article/view/76/74

CapitalOne. (2022). https://www.capitalone.com/digital/facts2019/es/faq/

Chavez, R. (2022). *SBS recibió 22 mil denuncias contra entidades financieras y halló responsabilidad en 50 casos*. Ojo Publico. https://ojo-publico.com/3839/miles-denuncias-registradas-y-pocas-sanciones-la-banca-el-peru

Čihák, M., Demirgüč-Kunt, A., Feyen, E., & Levine, R. (n.d.). *Nber working paper series financial development in 205 economies, 1960 TO 2010 Martin Čihák Asli Demirgüč-Kunt Erik Feyen Ro*. National Bureau of Economic Research | NBER. Retrieved July 15, 2025, from https://www.nber.org/system/files/working_papers/w18946/w18946.pdf

Callirgos Silva, S. R. (2024). *Responsabilidad civil derivada de la vulneración del derecho al honor en las redes sociales: necesidad de una norma especial en el Perú* [Tesis de licenciatura, Universidad Antonio Ruiz de Montoya]. https://repositorio.uarm.edu.pe/server/api/core/bitstreams/82c21d77-9823-463d-bebd-94f748661e90/content

Casariego Palomino, J. M. (2025). *Ciberseguridad e intermediación financiera* [Trabajo de suficiencia profesional para optar el título de Economista, Universidad de Piura]. https://pirhua.udep.edu.pe/backend/api/core/bitstreams/7a40e0bc-8f14-4b40-83f4-fea8e42355e9/content

Comisión Económica para América Latina y el Caribe. (2024). *Gestión de datos de investigación*. https://biblioguias.cepal.org/c.php?g=495473&p=4398118

Comisión Europea. (2023, abril 19). *Qué es la Inteligencia Artificial*. Plan de recuperación, transformación y resiliencia. Retrieved mayo 11, 2025, from https://planderecuperacion.gob.es/noticias/que-es-inteligencia-artificial-ia-prtr

Congreso de la Republica. (2011). *Ley de Protección de Datos Personales*. El peruano. https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20N%C2%BA%2029733.pdf.pdf?v=1618338779

Congreso de la República. (2011). *Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros*. https://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/8CEF5E01E937E76105257A0700610870/$FILE/26702.pdf

Congreso de la Republica. (2011, julio 3 *Ley de Protección de Datos Personales*. El peruano. https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20N%C2%BA%2029733.pdf.pdf?v=1618338779

Congreso de la República. (2017, Julio 27). *Decreto de urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento*. https://app-vlex-com.ezproxy.ucsm.edu.pe/search/inPlanOnly:1+fulltext_in_plan:1+date:2020-01-01..+content_type:9+jurisdiction:PE/ciberseguridad/vid/834822041

Congreso de la República. (2017, Julio 27). *Ley que modifica el decreto legislativo 1141, decreto legislativo de fortalecimiento y modernización del sistema de inteligencia nacional - SINA y de la dirección nacional de inteligencia - DINI, a fin de regular la seguridad digital*. https://www.leyes.congreso.gob.pe/Documentos/2016_2021/ADLP/Normas_Legales/30618-LEY.pdf

CONGRESO DE LA REPÚBLICA. (2017, Julio 27). *ley que modifica el decreto legislativo 1141, decreto legislativo de fortalecimiento y modernización del sistema de inteligencia nacional - sina y de la dirección nacional de inteligencia - dini, a fin de regular la seguridad digital*. https://app-vlex-com.ezproxy.ucsm.edu.pe/vid/689100377

Congreso de la República. (2018, Spetiembre 14). *Decreto legislativo que crea la autoridad nacional de transparencia y acceso a la información pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses*. https://app-vlex-com.ezproxy.ucsm.edu.pe/vid/941606709

Congreso de la República. (2023, Junio 21). *Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo*.

https://app-vlex-com.ezproxy.ucsm.edu.pe/search/inPlanOnly:1+fulltext_in_plan:1+jurisdiction:PE/ambito+de+aplicación+ciberseguridad/vid/923553632

Congreso de la República. (2024, Septiembre 09). *Ley que declara de interés nacional y necesidad pública la creación del comité de alto nivel de ciberseguridad del estado peruano*. https://app-vlex-com.ezproxy.ucsm.edu.pe/search/inPlanOnly:1+fulltext_in_plan:1+date:2020-01-01..+content_type:14+jurisdiction:PE/ciberseguridad/vid/1049124277

Congreso de la República. (2024, Septiembre 09). *Proyecto de Ley Nº 01776/2021-CR* [Ley que garantiza la ejecución de operaciones de ciberseguridad y seguridad digital a través de un centro nacional de ciberseguridad]. https://app-vlex-com.ezproxy.ucsm.edu.pe/vid/1049124277

Congreso de la República. (2025, Abril 30). *Ley de Delitos Informáticos*. https://app-vlex-com.ezproxy.ucsm.edu.pe/search/inPlanOnly:1+fulltext_in_plan:1+jurisdiction:PE/ley+30096/vid/578578930

Congreso de la República. (2025, Enero 13). *Proyecto de Ley Nº 09906/2024-CR, Ley de seguridad digital o ciberseguridad.* https://app-vlex-com.ezproxy.ucsm.edu.pe/search/inPlanOnly:1+fulltext_in_plan:1+date:2020-01-01..+content_type:14+jurisdiction:PE/ciberseguridad/vid/1065179381

Congreso de la República. (n.d.). *Código de Protección y Defensa del Consumidor*. https://app-vlex-com.ezproxy.ucsm.edu.pe/search/jurisdiction:PE+inPlanOnly:1+fulltext_in_plan:1/protecci%C3%B3n+al/vid/401594897

Congreso de la República. (n.d.). *Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros*. https://app-vlex-com.ezproxy.ucsm.edu.pe/vid/808573649

Congreso Nacional de Chile. (2024, 04 08). In *Ley Marco de Ciberseguridad*. Chile. https://latam-tirantonline-com.ezproxy.ucsm.edu.pe/latam/documentoLatam/show/35214514?searchtype=substring&general=ciberseguridad&tolgeo=LATAM&paises=&index=0

Cueto Vazquez, M. (2019). Big data en la banca y sus implicaciones para el futuro.

Davalos, A., & Mujica, M. (2024, Septiembre). *Ciberseguridad y vulneración de datos personales en entidades financieras, lima 2022*. Universidad Autónoma del Perú.

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

Dommeyer, C. J., & Gross, B. L. (2003). *What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies*. *Journal of Interactive Marketing, 17*(2), 34–51. https://doi.org/10.1002/dir.10053

Eguiguren Praeli, F. J. (2015). El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú. *Thēmis*.

Equipo Grou. (2019). *El impacto de la tecnología en el sector financiero*. GROU. https://www.grou.com.mx/blog/el-impacto-de-la-tecnologia-en-el-sector-financiero

Escobar, a. (n.d.). *Las llamadas comerciales efectuadas por entidades financieras y la vulneración del derecho constitucional a la protección de datos personales.* Universidad Cesar Vallejo. Retrieved 2022, from https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/114312/Escobar_MAL-SD.pdf?sequence=1&isAllowed=y

Estado Peruano. (1993). *Constitución Política del Perú*. https://app-vlex-com.ezproxy.ucsm.edu.pe/search/jurisdiction:PE+inPlanOnly:1+full text_in_plan:1/cómo+se+protegen+los+derechos+del+consumidor/vid/42814763

Federal Bureau of Investigation. (2020). *Internet Crime Report*. https://www.ic3.gov/AnnualReport/Reports/2020_IC3Report.pdf

Flores Flores, P. (2021). El auge del comercio electrónico: Reflexiones y discusiones entorno a la contratación y la protección al consumidor. *Foro Jurídico*, (19). Revistas PUCP. https://revistas.pucp.edu.pe/index.php/forojuridico/article/view/24729

Fojón Chamorro, E., & Sanz Villalba, Á. F. (2016, Junio 18). Ciberseguridad en España: una propuesta para su gestión. *Real Instituto Elcano*. https://media.realinstitutoelcano.org/wp-content/uploads/2010/06/ari102-2010-fojon-sanz-ciberseguridad-espana.pdf

Franco García, D., & Quintanilla Perea, A. (2020, Junio-Noviembre). La protección de datos personales y el derecho al olvido en el Perú. A propósito de los estándares internacionales del Sistema Interamericano de los Derechos Humanos. *Revista de la Facultad de Derecho PUCP*, *84*, 271-414. https://revistas.pucp.edu.pe/index.php/derechopucp/article/view/22113/21464

García, A. (2022). *La banca digital: Innovación tecnológica en la inclusión financiera en el Perú*. *Industrial Data, 24*(2), 99–120. https://doi.org/10.15381/idata.v24i2.20351

Gil, S., & Pasquel, J. (2021). *Competencias para el liderazgo efectivo de la transformación digital en empresas del sistema financiero*. Lima, Lima, Perú.

oemmndcbldboiebfnladdacbdfmadadm/https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/19762/Liderazgo%20Efectivo-Transformación%20Digital%20-%20Sistema%20Financiero-GIL.pdf?sequence=1&isAllowed=y

Gonzales, K., Gutierrez, G., & Linares, D. (2024). *Breve análisis sobre Big Data y la protección al usuario del Sistema Bancario Venezolano*.

Gregg, M. (2024). *¿Qué es la ciberseguridad?* https://www.ibm.com/es-es/topics/cybersecurity

Gunn, A. (2008). Mr. Obama? Don't forget the cyberwar threat. *Beta News*. https://betanews.com/2008/12/08/mr-obama-don-t-forget-the-cyberwar-threat/

Hernandez, N. (2018). *Clasificación de los datos personales e implicaciones legales*. repository.upb.edu.co. https://repository.upb.edu.co/bitstream/handle/20.500.11912/3595/Clasificaci%c3%b3n%20de%20los%20datos%20personales%20e%20implicaciones%20legales.pdf?sequence=1&isAllowed=y

IBM. (2024). *¿Qué es un ataque cibernético?* https://www.ibm.com/mx-es/topics/cyber-attack

Kong (2022) *El derecho al olvido y su reconocimiento jurisprudencial. Comentarios a la STC 03041-2021-PHD/TC*. Revista Peruana de Derecho Constitucional, (14), 717–729

Letona, P. A. M. (2025). *Protección de datos e inteligencia artificial (IA). Ius Inkarri. Revista de la Facultad de Derecho y Ciencia Política de la Universidad Ricardo Palma.* https://revistas.urp.edu.pe/index.php/Inkarri/article/view/7566/12173

Lopez de Mantaras, R. (n.d.). *¿Qué es la inteligencia artificial?* Dialnet. Retrieved mayo 11, 2025, from https://dialnet.unirioja.es/servlet/articulo?codigo=9287111

Lopez, H. (2023). *Medidas de seguridad bancarias para mitigar la vulneración de derechos de los usuarios frente al phishing en el sistema financiero*. Chiclayo, Chiclayo, Perú. oemmndcbldboiebfnladdacbdfmadadm/https://tesis.usat.edu.pe/bitstream/20.500.12423/6891/1/TL_LopezOcampoHuillari.pdf

Lopez (2024) ¿para qué olvidar? Análisis comparado de los contornos del derecho al olvido en la jurisprudencia chilena y peruana. https://www.scielo.cl/pdf/rchilder/v51n3/0718-3437-rchilder-51-03-93.pdf#:~:text=comparado%20de%20la%20ju%02risprudencia%20de,a%20informaci%C3%B3n%20que%20se%20encontraba

Mansilla Pizarro, D. (2020). *Implementación de programas de cumplimiento en ciberseguridad como una práctica de buen gobierno corporativo en las entidades que forman parte del sistema financiero peruano* [Tesis de maestría, Pontificia Universidad Católica del Perú]. https://tesis.pucp.edu.pe/server/api/core/bitstreams/5692c4db-ee4b-424f-9263-b51e095ccdf7/content

Mendoza, O. (2022). *El derecho de protección de datos personales en los sistemas de inteligencia artificial*. SciElo. https://www.scielo.org.mx/scielo.php?pid=S1870-21472021000200179&script=sci_arttext

Montes Sanchez, D. V. (2024). *La vulneración del derecho a la intimidad y a la privacidad en el entorno digital en el Perú* [Tesis para optar el título profesional de Abogada, Universidad ESAN]. https://repositorio.esan.edu.pe/server/api/core/bitstreams/57cd1aa5-17a0-4250-8fe0-4ae567302d4a/content

Morales, A. (2021). *El impacto de la inteligencia artificial en el Derecho*. Advocatus. https://revistas.ulima.edu.pe/index.php/Advocatus/article/view/5117

Lund, B. D., Brown, N., Roeschley, A., & Hossain, G. (2026). *PDPL metric: Validating a scale to measure personal data privacy literacy among university students*. arXiv. https://arxiv.org/abs/2601.00715

Olivos, M. (2019, 07 09). La protección de la privacidad como objeto de tutela en el ordenamiento jurídico peruano. *IUS: Revista Investigación de la Facultad de Derecho*, *8*(1), 47-67. https://revistas.usat.edu.pe/index.php/ius/article/view/38

Ortega Candel, J. M. (2021). *Ciberseguridad. Manual práctico*. Ediciones Paraninfo, S.A. https://books.google.com.pe/books?hl=es&lr=&id=QsROEAAAQBAJ&oi=fnd&pg=PR5&dq=ciberseguridad&ots=3temh5uiSa&sig=NCXwuB1NdNrJ7opZaS6w66VBdRc&redir_esc=y#v=onepage&q=ciberseguridad&f=false

Pacheco, R. (2019). *El tratamiento de los datos personales dentro de las empresas vinculadas al sistema financiero peruano*. Universidad Católica Santo Toribio de Mogrovejo. https://tesis.usat.edu.pe/bitstream/20.500.12423/2332/1/TL_PachecoBancayanRonaldo.pdf

Parlamento Europeo. (2016). *Reglamento General de Protección de Datos*. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Paucar, L. (2024). *Robo de datos en Interbank al descubierto: así operó el hacker para sustraer información de los clientes del banco*. Infobae. https://www.infobae.com/peru/2024/11/11/robo-de-datos-en-interbank-al-descubierto-asi-opero-el-hacker-para-sustraer-informacion-de-clientes-del-banco/

Pattanayak, M., Shankar, A. U., Sahay, E. B., Kamalaveni, M. S., & Jayapriya, K. (2025). *Consumer protection laws in the digital era: Challenges & future trends*. *Lex Localis – Journal of Local Self-Government, 23*(S5). https://lex-localis.org/index.php/LexLocalis/article/view/801722/2405

Presidencia del Consejo de Ministros. (2024). Politica Nacional de Transformacion Digital.

Productos y soluciones de seguridad de Cisco. (n.d.). Cisco. Retrieved July 15, 2025, from https://www.cisco.com/site/mx/es/products/security/index.html

Pinto, S. L. (2018). *Privacy and data protection: A study on awareness and attitudes of millennial consumers on the internet – An Irish perspective* [Tesis de maestría, National College of Ireland]. https://norma.ncirl.ie/3386/1/salonilerisapinto.pdf

Quezada Santana, J. (2019). *Análisis de uso de datos personales por instituciones bancarias y financieras*. Universidad de Chile. https://repositorio.uchile.cl/bitstream/handle/2250/170341/Analisis-de-uso-de-datos-personales-por-instituciones-bancarias-y-financieras.pdf?sequence=1

Quiroz, R. (2016). *El Hábeas Data, protección al derecho a la información y a la autodeterminación informativa*. http://www.scielo.org.pe/scielo.php?pid=S2071-50722016000200002&script=sci_arttext

Reglamento Europeo y del Consejo (Ed.). (2016, abril 27). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016*. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Riega Viru, Y., Huamani Chirinos, H., & Machuca Vilchez, J. (2021). Contratación electrónica y los delitos informáticos. En protección al consumidor en el Perú. *evista Lex de la Facultad de Derecho y Ciencias Políticas de la Universidad Alas Peruanas*, *19*(28), 197-236. https://biblat.unam.mx/es/revista/lex-lima/articulo/contratacion-electronica-y-los-delitos-informaticos-en-proteccion-al-consumidor-en-el-peru. chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://revistas.uap.edu.pe/ojs/index.php/LEX/article/download/2318/2372

Romeo Ruiz, A. (2020). la resPonsabilidad Proactiva de las administraciones Públicas en la Protección de datos Personales. *Análisis y Debate Jurídico*. chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://www.ivap.euskadi.eus/contenidos/informacion/18_revgp/eu_def/Romeo_138_153.pdf

Rouhiainen, L. (2023). *Inteligencia artificial: 101 cosas que debes saber hoy sobre nuestro futuro*. Alienta Editorial.

Sagasti Hochhausler, F. R. (2021, Julio 25). *Decreto Supremo, N° 005-2021-de, poder ejecutivo, defensa* [Decreto Supremo que aprueba la 'Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030']. https://app-vlex-com.ezproxy.ucsm.edu.pe/vid/873318961

Solar Silva, David. "En 2025 aumentarán ciberataques en Perú: ¿cómo impactará en las empresas?" *INFOBAE*, INFOBAE, 04 enero 2025, https://www.infobae.com/peru/2025/01/04/en-2025-aumentaran-ciberataques-en-peru-como-impactara-en-las-empresas/. Accessed 11 05 2025.

Superintendencia de Banca y Seguros. (2021, Febrero 19). *Resolución nº 504-2021*.

Superintendencia de Banca, Seguros y AFP. (2017). *Programa finanzas en el cole* [programa de asesoría a docentes sobre el rol y funcionamiento del sistema financiero, de seguros, afp y unidades de inteligencia financiera]. https://www.sbs.gob.pe/portals/3/educacion-financiera-pdf/Guia%20del%20docente%202017.pdf

Tribunal Constitucional del Perú. (2006). *Sentencia del Tribunal Constitucional*. https://tc.gob.pe/jurisprudencia/2008/01535-2006-AA.pdf

Tribunal Constitucional Pleno. (2018, Diciembre 20). *Sentencia Nº 142/2018*. España. https://app-vlex-com.ezproxy.ucsm.edu.pe/search/inPlanOnly:1+fulltext_in_plan:1+content_type:2/ciberseguridad/vid/751869537

Tribunal Constitucional. (2021). *Sentencia del Tribunal constitucional Exp N° 02140-2020-PDH/TC*. https://tc.gob.pe/jurisprudencia/2021/02140-2020-HD.pdf

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI). (2022). *Resolución N.° 0286-2022/PS2 (Expediente N.° 0028-2022/PS2)*

Unión Internacional de Telecomunicaciones. (2008, April 18). *UIT-T Rec. X.1205 (04/2008) Aspectos generales de la ciberseguridad*. ITU. Retrieved July 14, 2025, from https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-S&type=items

Vesga Guedes, P. E. (2024). Delitos informáticos y la vulneración al derecho a la intimidad personal en la Provincia de Barranca, 2023. *Universidad Nacional José Faustino Sánchez Carrión*. https://repositorio.unjfsc.edu.pe/bitstream/handle/20.500.14067/8991/TESIS.pdf?sequence=1&isAllowed=

Zumaita Gilvonio,J. A., Millán Vargas, J. E., & Santivañez Villavicencio, Z. N. (2025) https://derechoglobal.cucsh.udg.mx/index.php/DG/article/view/798

AI Now Institute. (2023, April 11). *Algorithmic Accountability: Moving Beyond Audits*. AI Now Institute. Recuperado Noviembre 11, 2025, from https://ainowinstitute.org/publications/algorithmic-accountability

Brand, D., Hoffman, M., & Van Der Merve, J. (2025, Abril 16). Development of effective methods and tools for the auditing of AI algorithms by the Supreme Audit Institutions. *JeDEM*, 106-141. 10.29379

Engler, A. (2021, Marzo 12). *Auditing emplyment algorithms for discrimination*. Brookings. https://docs.google.com/document/d/1RAkBVILOweg6ZQVr3hUutT9mNypTdKsC/edit

Eticas Foundation Tech. (2023). *Adversarial Algorithmic Auditing Guide*. https://eticasfoundation.org/wp-content/uploads/2024/12/ETICAS-Adversarial-Algorithmic-Auditing-Guide-2023.pdf

Groves, L., Metcalf, J., Kennedy, A., Vecchione, B., & Strait, A. (2024, Julio 03). Auditing Work: Exploring the New York City algorithmic bias audit regime. *Creative Commons*. 979-8-4007-0450-5/24/06

Laime, J., Minkkinen, M., & Mäntymäki, M. (2024, Julio). Ethics-based AI auditing: A systematic literature review on conceptualizations of ethical principles and knowledge contributions to stakeholders. *ELSEVIER*, *61*. https://doi.org/10.1016/j.im.2024.103969

Metaxa, D., & Hancock, J. (2022, Octubre). *Using Algorithm Audits to Understand AI*. chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://hai.stanford.edu/assets/files/2022-10/HAI%20Policy%20Brief%20-%20Using%20Algorithm%20Audits%20to%20Understand%20AI.pdf

Mökander, J. (2023, Noviembre 08). *Auditing of AI: Legal, Ethical and Technical Approaches. DISO 2, 49*. https://link.springer.com/article/10.1007/s44206-023-00074-y

OECD. (2023, Febrero 23). Advancing accountability in AI Governing and managing risks throughout the lifecycle for trustworthy AI. https://www.oecd.org/en/publications/advancing-accountability-in-ai_2448f04b-en.html

Sampath, N. (2022, Octubre). Opening Black Boxes: Addressing Legal Barriers to Public interest Algorithmic Auditing. En *Consumer Reports*. chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://innovation.consumerreports.org/wp-content/uploads/2022/10/CR_Algorithmic_Auditing_Final_10_2022VF2.pdf