UNIVERSIDAD LAICA VICENTE ROCAFUERTE DE GUAYAQUIL

FACULTAD DE CIENCIAS SOCIAL Y DERECHO

CARRERA DE DERECHO

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

ABOGADO

TEMA

MARCO LEGAL DE LA TECNOLOGÍA DIGITAL Y LA PRIVACIDAD DE LOS DATOS.

TUTOR

PhD. MARIO MARTINEZ HERNANDEZ.

AUTORES

RONALDO SNAIDER FARFAN CORNEJO

WIDINSON ARTURO CORNEJO RAMON

GUAYAQUIL

2025

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA		
FICHA DE REGISTRO DE TESIS		
TÍTULO Y SUBTÍTULO: Marco legal de la tecnología digital y la privacidad de los datos.		
AUTOR/ES: Farfan Cornejo Ronaldo Snaider Cornejo Ramon Widinson Arturo	**TUTOR:** PhD. Mario Martínez Hernández	
INSTITUCIÓN: **Universidad Laica Vicente Rocafuerte de Guayaquil**	**Grado obtenido:** Abogado	
FACULTAD: FACULTAD DE CIENCIAS SOCIAL Y DERECHO	**CARRERA:** CARRERA DE DERECHO	
FECHA DE PUBLICACIÓN: 2025	**N. DE PÁGS:** 102	
ÁREAS TEMÁTICAS: Derecho		
PALABRAS CLAVE: Protección de datos, Derecho a la privacidad, Digitalización, Legislación		
RESUMEN: El trabajo tuvo como objetivo analizar la efectividad y los desafíos del marco legal de la tecnología de Ecuador en la protección de la privacidad de los datos frente a los avances tecnológicos en un entorno digital globalizado. La metodología fue mista, tuvo carácter cualitativo debido al análisis de bases teóricas, tuvo aproximación cuantitativa debido a la aplicación de una encuesta escala de Likert a 20 abogados del Colegio de Abogados de Guayas. Los resultados señalan que un 35% consideró que la normativa no es clara en garantizar la privacidad en el entorno digital, el 55% no estaba seguro de la alienación de la ley con estándares internacionales y 40% consideró que las instituciones encargadas de hacer cumplir la normativa no actúan con eficiencia y rigor. El 45% de los encuestados indicó que los mecanismos de denuncia de vulneraciones no son efectivos. Con base en ello, se concluyó que la Ley Orgánica de Protección de Datos Personales y su reglamento establecen principios sólidos, aunque existen desafíos en su aplicación y cumplimiento.		
N. DE REGISTRO (en base de datos):	**N. DE CLASIFICACIÓN:**	
DIRECCIÓN URL (Web):		
ADJUNTO PDF:	**SI** [X]	**NO** [ ]

CONTACTO CON AUTOR/ES: Farfan Cornejo Ronaldo Snaider Cornejo Ramon Widinson Arturo	**Teléfono:**	**E-mail:** rfarfanco@ulvr.edu.ec wcornejor@ulvr.edu.ec
CONTACTO EN LA INSTITUCIÓN:	PhD. Adrián Camacho Domínguez Decano de la facultad de Ciencias Sociales y Derecho **Teléfono:** (04) 2596500 **Ext**. 250 **E-mail:** acamacho@ulvr.edu.ec Mgtr. Carlos Pérez Leyva **Teléfono:** (04) 2596500 **Ext.** 233 **E-mail:** cperezl@ulvr.edu.ec	

CERTIFICADO DE SIMILITUD

TESIS PREGRADO

INFORME DE ORIGINALIDAD

7%	10%	9%	4%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.ucsg.edu.ec Fuente de Internet	1%
2	repositorio.upse.edu.ec Fuente de Internet	1%
3	insolidumabogados.com Fuente de Internet	1%
4	repositorio.ulasalle.edu.pe Fuente de Internet	1%
5	www.risti.xyz Fuente de Internet	1%
6	Dennys Adrian Morales Echeverria, Freddy Patricio Morales Alarcón, Efrén Efraín Cajamarca Altamirano, Francisco Javier Intriago Usca et al. "The protection of personal data in Ecuador: legislative evolution and comparison with regional models in South America", Perspectivas Sociales y Administrativas, 2024 Publicación	1%
7	repositorio.upn.edu.pe Fuente de Internet	1%
8	www.planv.com.ec Fuente de Internet	1%
9	repositorio.ulvr.edu.ec Fuente de Internet	1%

10 Submitted to Universidad Católica de Santa María 1%

Trabajo del estudiante

Excluir citas	Apagado	Excluir coincidencias	< 1%
Excluir bibliografía	Apagado		

Firmado electrónicamente por:
MARIO MARTINEZ HERNANDEZ

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS PATRIMONIALES

Los estudiantes egresados RONALDO SNAIDER FARFÁN CORNEJO Y WIDINSON ARTURO CORNEJO RAMÓN, declaramos bajo juramento, que la autoría del presente Trabajo de Titulación, Marco Legal de la Tecnología Digital y la Privacidad de los Datos, corresponde totalmente a los suscritos y nos responsabilizamos con los criterios y opiniones científicas que en el mismo se declaran, como producto de la investigación realizada.

De la misma forma, cedemos los derechos patrimoniales y de titularidad a la Universidad Laica VICENTE ROCAFUERTE de Guayaquil, según lo establece la normativa vigente.

Autores,

Firma:
RONALDO SNAIDER FARFAN CORNEJO

C.I. 0941127961

Firma:
WIDINSON ARTURO CORNEJO RAMON

C.I.0941128050

CERTIFICACIÓN DE ACEPTACIÓN DEL DOCENTE TUTOR

En mi calidad de docente Tutor del Trabajo de Titulación Marco Legal de la Tecnología Digital y la Privacidad de los Datos, designado(a) por el Consejo Directivo de la Facultad de Ciencias Sociales y Derecho de la Universidad Laica VICENTE ROCAFUERTE de Guayaquil.

CERTIFICO:

Haber dirigido, revisado y aprobado en todas sus partes el Trabajo de Titulación, titulado: Marco Legal de la Tecnología Digital y la Privacidad de los Datos, presentado por los estudiantes RONALDO SNAIDER FARFÁN CORNEJO Y WIDINSON ARTURO CORNEJO RAMÓN como requisito previo, para optar al Título de ABOGADO, encontrándose apto para su sustentación.


Firmado electrónicamente por:
MARIO MARTINEZ HERNANDEZ

Firma:

PhD. Mario Martínez Hernández

C.C. 1755217492

AGRADECIMIENTO

Queremos agradecer, en primer lugar, a nuestras familias, por su apoyo incondicional, su paciencia y por ser nuestro motor en este camino. Sin su confianza y motivación, este logro no sería posible.

A nuestro asesor, por su guía y conocimientos, que fueron fundamentales para la realización de esta tesis. Su orientación nos ayudó a mejorar y a superar los desafíos del proceso.

A nuestros amigos y compañeros, por su compañía, sus palabras de aliento y por hacer más llevadero este recorrido.

Y a todas las personas que, de una u otra manera, contribuyeron a que este proyecto se hiciera realidad. Gracias de corazón.

DEDICATORIA

Dedicamos este trabajo, en primer lugar, a nuestras familias, quienes nos han acompañado en cada paso de este camino con su amor, paciencia y apoyo incondicional. Sin ustedes, este logro no sería posible.

A nuestros amigos y seres queridos, por su compañía, palabras de aliento y por recordarnos que siempre hay tiempo para una sonrisa, incluso en los momentos más desafiantes.

A nuestros docentes y asesor, por compartir su conocimiento y guiarnos en este proceso, ayudándonos a crecer tanto académica como personalmente.

Y, por último, a nosotros mismos, por la dedicación, el esfuerzo y la perseverancia que nos llevaron a culminar este proyecto.

RESUMEN

El trabajo tuvo como objetivo analizar la efectividad y los desafíos del marco legal de la tecnología de Ecuador en la protección de la privacidad de los datos frente a los avances tecnológicos en un entorno digital globalizado. La metodología fue mista, tuvo carácter cualitativo debido al análisis de bases teóricas, tuvo aproximación cuantitativa debido a la aplicación de una encuesta escala de Likert a 20 abogados del Colegio de Abogados de Guayas. Los resultados señalan que un 35% consideró que la normativa no es clara en garantizar la privacidad en el entorno digital, el 55% no estaba seguro de la alienación de la ley con estándares internacionales y 40% consideró que las instituciones encargadas de hacer cumplir la normativa no actúan con eficiencia y rigor. El 45% de los encuestados indicó que los mecanismos de denuncia de vulneraciones no son efectivos. Con base en ello, se concluyó que la Ley Orgánica de Protección de Datos Personales y su reglamento establecen principios sólidos, aunque existen desafíos en su aplicación y cumplimiento.

Palabras Claves: Protección de datos, Derecho a la privacidad, Digitalización, Legislación

ABSTRACT

The study aimed to analyze the effectiveness and challenges of Ecuador's legal framework on technology in protecting data privacy against technological advancements in a globalized digital environment. The methodology was mixed: it had a qualitative approach due to the analysis of theoretical frameworks and a quantitative approach through the application of a Likert-scale survey to 20 lawyers from the Guayas Bar Association. The results indicated that 35% of respondents believed the regulations are unclear in guaranteeing privacy in the digital environment, 55% were unsure whether the law aligns with international standards, and 40% considered that the institutions responsible for enforcing the regulations do not act efficiently and rigorously. Additionally, 45% of respondents stated that the mechanisms for reporting privacy violations are ineffective. Based on these findings, it was concluded that while the Organic Law on Personal Data Protection and its regulations establish solid principles, there are challenges in their implementation and enforcement.

Keywords: Data protection, Right to privacy, Digital technology, Legislation

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

Esta investigación aborda la deficiencia en la implementación y cumplimiento del marco legal de protección de datos personales en Ecuador, esto dentro del contexto digital. Dicho esto, la aplicación de la Constitución de la República y la Ley Orgánica de Protección de Datos Personales se ve dificultada por la falta de recursos y la poca capacitación de las autoridades encargadas de supervisar la privacidad de los datos. De igual forma, el incremento de la digitalización, la inteligencia artificial y el internet de las cosas generan mayor incertidumbre sobre el camino legal a seguir.

En este campo, la implementación de las regulaciones se ve afectada por una falta de concientización en la sociedad y la escasa capacidad de las instituciones públicas. Esto expone a los ciudadanos al robo de identidad, fraudes cibernéticos y otros tipos de violaciones de privacidad. La relevancia de esta investigación viene dada por el hecho de que una gestión deficiente de los datos afecta a los individuos y tiene consecuencias socio-económicas a nivel empresarial; en este último punto, las empresas deben cumplir con regulaciones estrictas para evitar sanciones y proteger su reputación.

El primer capítulo establece el enfoque general de la investigación, se parte del planteamiento del problema y se formula la pregunta general. Luego se definen los objetivos generales y específicos, los cuales buscan analizar la eficacia del marco legal ecuatoriano en la protección de la privacidad de los datos en el contexto digital. Asimismo, se presenta la línea de investigación y la justificación del estudio, detallando su relevancia para el entorno legal y digital del país. De igual forma, se establece la idea a defender y se describe la propuesta dentro del marco académico.

En el segundo capítulo, se aborda el marco teórico que cimenta las bases académicas para el análisis del tema. Se inicia con la definición de tecnología digital y privacidad de los datos, destacando su importancia; a su vez, se explora la relación entre estos conceptos y el impacto social que tiene la protección de la privacidad, además de analizar cómo las políticas públicas en Ecuador han

contemplado la digitalización. También se presentan estudios de casos internacionales y nacionales que evidencian cómo otros países y Ecuador han manejado la protección de datos. Se finaliza la sección con el marco legal que regula la privacidad en el país, haciendo énfasis en la Constitución, la Ley Orgánica de Protección de Datos Personales, y el Código Orgánico Integral Penal.

El tercer capítulo describe la metodología empleada en la investigación, partiendo de la determinación del enfoque y alcance. Posteriormente, se explica la técnica y los instrumentos de recolección de datos, así como la población y muestra. Este trabajo de campo se centró en evaluar la percepción de los alimentantes y expertos sobre el tema.

El cuarto capítulo presenta los resultados obtenidos a partir de la encuestas y entrevistas aplicadas. En función de los resultados, se propone una serie de recomendaciones para mejorar la eficacia del marco legal en la protección de la privacidad de los datos en Ecuador. La propuesta contiene su justificación, los beneficiarios y el desarrollo necesario para su implementación.

CAPÍTULO I
ENFOQUE DE LA PROPUESTA

1.1 Tema:

Marco legal de la tecnología digital y la privacidad de los datos.

1.2 Planteamiento del Problema:

A pesar de la existencia de normativas, se han identificado algunas debilidades en su aplicación y cumplimiento, principalmente relacionadas con la falta de recursos y capacitación de las autoridades encargadas de velar por la protección de los datos personales.

El marco legal que regula la privacidad de los datos en Ecuador se encuentra principalmente en la Constitución de la República, la Ley Orgánica de Protección de Datos Personales y la Ley Orgánica de Comunicación.

En cuanto a la Constitución, se reconoce el derecho a la intimidad y la protección de los datos personales en el artículo 66, el cual establece que toda persona tiene derecho a la intimidad personal y familiar, y a la protección de sus datos personales. Además, se establece que el acceso a la información y la protección de los datos personales son derechos que deben ser garantizados por el Estado.

La Ley Orgánica de Protección de Datos Personales (LOPD, 2021) establece los principios básicos para la protección de los datos personales, tales como la finalidad, proporcionalidad, consentimiento, entre otros. También regula la creación y funcionamiento del Registro Nacional de Datos Públicos, así como las obligaciones de los responsables del tratamiento de datos personales y los derechos de los titulares de los mismos.

Por otro lado, la Ley Orgánica de Comunicación (2013) regula la protección de los datos personales en el ámbito de los medios de comunicación,

estableciendo limitaciones para la obtención y difusión de información personal sin consentimiento previo del titular.

El marco legal que rodea la privacidad de los datos en Ecuador aun no es sólido, aún existen retos en su implementación efectiva y en la concientización de la sociedad sobre la importancia de proteger la información personal.

El marco legal que regula la privacidad de los datos en Ecuador es aún incipiente y se encuentra en desarrollo, lo que plantea varios desafíos y problemas para la protección de los datos personales de los ciudadanos.

Otro problema es la falta de recursos y capacidades en las autoridades encargadas de supervisar el cumplimiento de las normativas de protección de datos. Esto limita su capacidad para investigar y sancionar adecuadamente a las organizaciones que violan la privacidad de los ciudadanos.

Además, en un contexto de creciente digitalización y uso de tecnologías de la información, es necesario actualizar y adaptar el marco legal existente para abordar los nuevos desafíos en materia de protección de datos, como el tratamiento de datos biométricos, la inteligencia artificial y el internet de las cosas.

> Haciendo el ejercicio de comparar las regulaciones europeas y ecuatorianas en materia de protección de datos, se desprende que ambas legislaciones establecen responsabilidades claras para el responsable del tratamiento de datos personales en caso de violación de datos. Si bien existen diferencias en cuanto a los detalles específicos de cada normativa, la premisa básica es similar: el responsable del tratamiento de datos personales debe garantizar la seguridad y privacidad de los datos, así como actuar diligentemente en caso de incidentes.
>
> En conclusión, la ciberseguridad y la protección de datos personales son temas de gran relevancia tanto a nivel nacional como internacional. Las empresas en Ecuador deben prestar atención a las responsabilidades y

> obligaciones establecidas en la LOPD y otros marcos regulatorios, y adoptar medidas efectivas para garantizar la seguridad de los datos personales que manejan. Al hacerlo, estarán protegiendo no solo a sus clientes y empleados, sino también a sus propias operaciones y reputación en el mercado (Ramírez, 2023, p. 1).

Actualmente se está produciendo un aumento en la cantidad de datos personales que son recopilados, procesados. Esta abundancia de datos ha generado preocupaciones sobre la privacidad de los individuos y la protección de sus derechos.

La protección de datos personales es una de las leyes más relevantes en la actualidad, originándose como una estrategia de privacidad en Europa durante la década de 1970. Establecer una constitución que incluya estos derechos no ha sido fácil en los sistemas legales. El derecho fundamental a la autodeterminación informativa surgió a partir de debates que consideraban que el derecho a la privacidad, por sí solo, no era suficiente para proteger completamente al individuo frente a los avances tecnológicos.

La Ley Orgánica de Protección de Datos Personales (LOPDP) ha tenido un impacto significativo a nivel mundial. Aunque es un tema en auge en numerosos países, esta ley es resultado de un desarrollo prolongado en la protección de datos en la Unión Europea, que ha servido de modelo para otras regiones, incluyendo América Latina. En la actualidad, muchos países ya cuentan con leyes de protección de datos vigentes.

En Ecuador, las reformas a la Constitución han incluido el derecho fundamental de proteger la información personal, con el poder de consultar y consentir el uso de esta información, como se establece en la Constitución de 2008. En los últimos años, se ha generado preocupación por el uso indebido de la información personal sin consentimiento, lo que ha impulsado la creación de una ley para regular este aspecto.

Con el avance de la digitalización y la automatización, el procesamiento de datos personales mediante herramientas tecnológicas está en constante crecimiento, lo que subraya la necesidad urgente de leyes para su protección. Existen grandes oportunidades para recopilar, almacenar y analizar datos, pero también es crucial salvaguardarlos. La Ley de Protección de Datos Personales protege a las personas del uso indebido de sus datos, tanto en formato digital como físico, y de amenazas públicas o privadas.

Desde mayo de 2021, Ecuador cuenta con su primera Ley Orgánica de Protección de Datos Personales (LOPDP), destinada a garantizar la implementación del derecho a la protección de datos personales. Esta ley establece principios, derechos, obligaciones y garantías, y define cómo se deben manejar los datos y qué tipos de datos requieren protección específica.

En general, se observa un aumento en los incidentes de violación de datos debido al creciente uso de internet y tecnologías digitales. Esto incluye casos de filtraciones de bases de datos, ataques de phishing, robos de identidad y otros tipos de fraudes cibernéticos.

> En agosto del año pasado Jorge presentó una denuncia por extorsión. Un usuario desconocido se había hecho pasar por él y había contactado a 9 personas de su entorno. Les escribía desde un nuevo número de WhatsApp pidiendo que guarden ese nuevo contacto. ¿Buen día cómo vas? Aquí Jorge para guardes mi nuevo número decían los mensajes. Tras entablar conversación el usuario que se hacía pasar por Jorge les pedía dinero, montos desde los $500 hasta los $2000.
>
> La Fiscalía trabajó en coordinación con la Unidad Nacional de Investigación Antisecuestros y Extorsión (UNASE) a través del rastreo de teléfonos celulares y cuentas bancarias. Se pudo capturar a cuatro personas que están siendo procesadas penalmente confirmó Nelson Vela, coordinador de la Fiscalía de Patrimonio Ciudadano de la Fiscalía Provincial del Guayas. (Novik, 2021, p. 1)

El problema de la privacidad de los datos en Ecuador se manifiesta principalmente en el ámbito digital, donde cada vez se utilizan información personal de los ciudadanos sin su consentimiento. Esto pone en riesgo la privacidad y seguridad de los datos de los ecuatorianos, ya que pueden ser víctimas de robos de identidad, fraudes o estafas.

Por tanto, es fundamental realizar un estudio crítico del marco legal que regula la privacidad de los datos en Ecuador para identificar las brechas existentes y proponer medidas que fortalezcan la protección de la información personal de los ciudadanos. Esta investigación es importante no solo para garantizar el cumplimiento de la legislación vigente, sino también para proteger los derechos fundamentales de privacidad y seguridad de los individuos en la era digital. Además, un marco legal sólido en materia de protección de datos contribuirá a fortalecer la confianza de los ciudadanos en el uso de la tecnología y fomentar un entorno seguro y transparente en el que puedan ejercer sus derechos de forma plena.

1.3 Formulación del Problema:

¿Cuál es la efectividad y los desafíos del marco legal de la tecnología de Ecuador en la protección de la privacidad de los datos frente a los avances tecnológicos en un entorno digital globalizado?

1.4 Objetivo General

Analizar la efectividad y los desafíos del marco legal de la tecnología de Ecuador en la protección de la privacidad de los datos frente a los avances tecnológicos en un entorno digital globalizado.

1.5 Objetivos Específicos

- Identificar los referentes teóricos del marco legal de la tecnología de Ecuador y la privacidad de los datos.

- Evaluar la situación actual de la protección de datos personales en el marco de la normativa de protección y derecho a la privacidad.

- Proponer recomendaciones para mejorar la protección de la privacidad de los datos.

1.6 Idea a Defender

La efectividad y los desafíos del marco legal de la tecnología de Ecuador en la protección de la privacidad de los datos frente a los avances tecnológicos en un entorno digital globalizado.

1.7 Línea de Investigación Institucional / Facultad.

Línea institucional

Sociedad civil, derechos humanos y gestión de la comunicación.

La Línea de la facultad

Derecho procesal con aplicabilidad al género, la identidad cultural y derechos humanos.

CAPÍTULO II
MARCO REFERENCIAL

A nivel internacional, en Colombia, Jiménez (2024) investigó la seguridad y privacidad en la era digital, enfocándose en la información líquida y la vigilancia panóptica. La metodología fue descriptiva por medio de una revisión bibliográfica y normativas legales, analizando diferentes enfoques teóricos y jurídicos. Entre los principales hallazgos, se evidenció que la digitalización ha debilitado la privacidad, convirtiéndola en un elemento fluido y expuesto. Adicionalmente, la acumulación de datos personales en corporaciones gigantes como Google y Facebook ha llevado al capitalismo de la vigilancia. Al no existir mucho control sobre la privacidad, se cometen delitos tales como fraude y robo de identidad. De acuerdo con la conclusión de este estudio, medidas más estrictas y la educación en el ámbito digital son necesarios para asegurar que usar personas se den cuenta del valor de su información privada y su exposición en el digital.

En México, Murrugarra (2024) indagó cómo los sistemas de inteligencia artificial que gestionan datos personales representan una amenaza para la privacidad de los usuarios de internet. El enfoque de su investigación fue cualitativo basado en el análisis documental de cinco artículos científicos, tres informes y tres videos de YouTube sobre la temática. Los principales hallazgos indicaron que la IA puede vulnerar la privacidad de los usuarios debido al desconocimiento sobre el manejo de sus datos y la falta de mecanismos de seguridad adecuados. También señala que muchas organizaciones no toman las medidas necesarias de privacidad desde el diseño, lo que propicia la violación del acceso a la información personal. Asimismo pueden utilizarse sistemas de IA para la vigilancia, la publicidad personalizada y los ciberataques. La conclusión principal del texto es que a pesar del potencial de IA de reproducir la seguridad de los datos, sin mucha más regulación presenta riesgos. Por lo tanto, sugiere fortalecer la ley y la transparencia de la IA en lo que respecta a la información privada.

Sánchez (2023) realizó un estudio del derecho a la protección de datos personal en la era digital enfocándose en los efectos de la tecnología e

inteligencia artificial en la privacidad de la información personal. Este autor realizó un análisis normativo y de doctrina, analizaron casos extraídos de la jurisprudencia y regulaciones. Una de las principales expresiones de este estudio señala que el 90% de los usuarios de internet en México están preocupados por su seguridad en línea, debido al aumento de ciberdelitos y la creciente comercialización de datos personales. Además, se destacó que la inteligencia artificial representa riesgos sin precedentes, ya que podría automatizar hasta el 25% de los empleos en Estados Unidos y Europa. Como conclusión, el estudio subraya la importancia de un enfoque ético y regulatorio en el desarrollo tecnológico, ya que la falta de control sobre los datos personales incrementa la vulnerabilidad de los ciudadanos.

Barahona y Mayorga (2024) investigaron la regulación del derecho a la privacidad en la era digital en Ecuador desde la perspectiva jurídica como social. Los autores realizaron la investigación sobre la base de la metodología cualitativa a través de realizar la revisión bibliográfica de fuentes académicas, normativas legales y documentos internacionales. Entre las publicaciones se tomó en consideración las que estaban hecha desde 2015 hasta 2023, en la que se observa la dinámica del desarrollo de la regulación y de su impacto. Entre los principales hallazgos, se identificó que, aunque Ecuador cuenta con leyes como la Ley Orgánica de Protección de Datos Personales, persisten desafíos en la seguridad de la información y el acceso indiscriminado del Estado a los datos personales. Además, se halló que el 85% de la población ecuatoriana tuvo acceso a internet en 2021, pero existen brechas digitales entre áreas urbanas y rurales. Esto permite inferir que, a pesar de los avances normativos, es necesario fortalecer la educación digital, la transparencia en el manejo de datos y garantizar la privacidad en un entorno cada vez más digitalizado.

En el mismo contexto nacional, Barahona (2024) analizó el derecho a la protección de datos en Ecuador y su relación con el avance de las nuevas tecnologías, abordando implicaciones legales y éticas. El método utilizado fue mixto, consistió en el análisis cualitativo de la normativa y la literatura académica, y cuantitativa por la aplicación de una encuesta. De ella, 384 personas respondieron a las preguntas donde 98% de ellos indicaron que el concepto de

protección de los datos electrónicos es necesario, pero sólo el 69% tiene información sobre este tema. Por otro lado, el 100% de los encuestados cree que las leyes necesitan reformarse para proteger a las personas del abuso. Además, el 78% cree necesaria la creación de nuevas regulaciones específicas. Este estudio permite concluir que Ecuador cuenta con un marco legal en la temática de protección de datos, no obstante, su aplicación tiene desafíos aún por superar, debido a la falta de conciencia social y la rápida evolución tecnológica. Es decir, es esencial fortalecer la educación digital y la supervisión regulatoria para garantizar una protección efectiva.

2.1 Marco Teórico:

2.1.1 Definición de Tecnología Digital

La tecnología digital es un sistema de herramientas y sistemas que emplean datos binarios para el envío, la transmisión y el almacenamiento de información. La idea de la tecnología digital ha progresado desde la noción de tecnologías de la información y comunicación (TIC) hasta simplemente la noción de la tecnología digital, porque está implícito en todos los ámbitos de la existencia humana y profesional (Nava, 2021). La transformación digital, impulsada por tecnologías como la inteligencia artificial, el big data, la computación en la nube y el Internet de las Cosas (IoT), ha revolucionado la manera en que las organizaciones operan y se comunican (Galindo, 2020).

De acuerdo con Mosquera et al. (2022), estas tecnologías posibilitan la automatización de procesos en las organizaciones y tienen un impacto disruptivo en la sociedad y la industria. A través de ellas, se produce la transformación digital que consiste en el proceso de reorientar una organización hacia la aplicación y el uso de tecnologías emergentes. Es decir, no se trata únicamente de la adopción de herramientas digitales, ya que involucra un cambio profundo en la cultura organizacional. Por ello, a este proceso se asocia el concepto de innovación, que impulsa la adopción de esas tecnologías emergentes y la mejora en la dinámica productiva y social.

En el contexto empresarial, la adopción de tecnologías digitales transforma los procesos operativos, también redefine modelos de negocio, creando nuevas oportunidades para el crecimiento y la competitividad. Empresas de todos los tamaños están incorporando herramientas como la automatización, el análisis de datos y la inteligencia artificial para optimizar la toma de decisiones, mejorar la eficiencia y ofrecer productos o servicios más personalizados a sus clientes. De hecho, la integración de tecnologías digitales en los negocios fomenta la innovación disruptiva, permitiendo que las organizaciones se adapten rápidamente a los cambios del mercado, generen valor de manera más ágil y, en muchos casos, transformen completamente su sector de actividad (Schmitt, 2022).

Por otro lado, el impacto de la tecnología digital se evidencia también en la educación, puesto que nuevas soluciones tecnológicas han modificado las metodologías de enseñanza y aprendizaje. En este ámbito, la integración de herramientas digitales ha permitido el diseño de entornos de aprendizaje más dinámicos e interactivos, cuyo beneficio radica en la facilidad para comprender conceptos complejos y promover la participación de los estudiantes en el proceso educativo (León et al., 2024; Punina et al., 2024). A pesar de sus ventajas, la rápida adopción de tecnologías digitales, indistintamente del campo de aplicación, trae consigo desafíos debido a la brecha digital que se crea y la urgencia de establecer un marco ético que oriente su uso de manera responsable (Arriola, 2024).

2.1.2 Privacidad de los Datos

La privacidad de los datos es la facultad de un individuo para decidir qué información personal desea compartir con otros dependientes, la forma en que esta se almacene y divulgue, y cómo los corresponsales pueden manejar o desempeñar el tratamiento de sus datos. Este concepto es relevante en la era digital ya que el uso muy extendido de información personal y su recopilación en plataformas, aplicaciones y servicios es uno de los principales desafíos de la transformación digital (Muzzio, 2023). En ese sentido, la protección de datos personales implica la seguridad de la información, al igual que el respeto por la

dignidad y los derechos de los individuos, por lo tanto, existe la necesidad de marcos legales que regulen el tratamiento de estos datos (Hernández, 2021).

Al respecto, Salazar y Ávila (2024) enfatizan que la protección de datos personales requiere de la implementación de estándares en seguridad informática o ciberseguridad reconocidos internacionalmente como la normas ISO vinculantes a esta materia, ya que la correcta aplicación minimiza riesgos de vulneración de datos. En esa misma línea, Vinueza et al. (2024) señalan que la implementación de leyes específicas para salvaguardar la privacidad de los datos, como la Ley Orgánica de Protección de Datos Personales en Ecuador, permite establecer medidas de seguridad y principios de conservación de datos, obligando a las organizaciones a realizar un análisis de riesgos y a mantener un registro actualizado de los datos que manejan

Cabe señalar que la privacidad de los datos está intrínsecamente relacionada con el concepto de derecho al olvido, que permite a los individuos solicitar la eliminación de su información personal de bases de datos y registros públicos (Garcés et al., 2023). Como derecho, la privacidad de los datos es fundamental para proteger a los individuos de posibles abusos y para asegurar que su información no sea utilizada de manera indebida o sin su consentimiento. Sin embargo, la implementación efectiva de estos derechos es compleja debido a la rápida evolución tecnológica y la nueva tendencia de uso de inteligencia artificial, frecuentemente complica la obtención del consentimiento y el manejo de datos personales (Albornoz, 2021).

El derecho al olvido, como una extensión del derecho a la privacidad, plantea una serie de cuestiones legales en su implementación eficaz. En muchos países, este derecho se ha convertido en un tema de debate dentro de los tribunales, especialmente en lo que respecta a la relación entre la libertad de expresión y la protección de la privacidad. La aplicación del derecho al olvido puede generar conflictos, ya que permite que los individuos soliciten la eliminación de su información personal de Internet, pero, al mismo tiempo, se enfrenta a la dificultad de equilibrar este derecho con el derecho público a la información y la memoria histórica. Además, la ejecución de este derecho

plantea interrogantes sobre cómo deben las plataformas gestionar la eliminación de datos y si las leyes actuales están equipadas para lidiar con las complejidades del entorno digital globalizado (Garcés et al., 2023).

En otro orden de ideas, la ciberseguridad también tiene un rol en la protección de la privacidad de los datos, dado que las organizaciones deben establecer estrategias lo suficientemente seguras para proteger la información personal de amenazas digitales, asegurando que los datos sean accesibles solo para aquellos que tienen autorización (Rojas et al., 2023). La falta de medidas adecuadas puede resultar en pérdidas financieras, daños a la reputación y responsabilidades legales, lo que subraya la importancia de la privacidad de los datos en la confianza del consumidor y la sostenibilidad de las empresas (Muzzio, 2023).

Ciberdelitos

El panorama de los delitos cibernéticos en Ecuador muestra un aumento significativo, exacerbado por la pandemia de COVID-19 debido al mayor uso de tecnologías digitales. Un estudio de Kaspersky Lab encontró que los delitos cibernéticos han aumentado en todo el mundo un 35% durante la crisis sanitaria. En Ecuador, la falta de denuncias y la falta de estadísticas precisas dificultan comprender plenamente la situación. Las estadísticas disponibles muestran una disminución de las denuncias en 2020 en comparación con 2019. Sin embargo, esto no indica una reducción de la delincuencia, sino una subnotificación por restricción de movimiento durante la detención e imposibilidad de comunicarse en persona.

La subnotificación de delitos cibernéticos en Ecuador es un fenómeno que agrava la comprensión y la respuesta efectiva ante este tipo de criminalidad. Varias razones contribuyen a esta subnotificación, como la desconfianza en las autoridades, la falta de conocimiento sobre cómo proceder ante un ciberdelito y la escasa educación en materia de ciberseguridad entre la población. Además, muchas víctimas de delitos cibernéticos, como el fraude en línea o el robo de información personal, con frecuencia no presentan denuncias debido al temor de

que sus casos no sean resueltos o que los procedimientos legales sean demasiado complicados o prolongados. Esto crea una brecha en las estadísticas oficiales y en la capacidad del Estado para desarrollar políticas públicas eficaces, destacando la necesidad de mejorar los mecanismos de denuncia y aumentar la confianza en las autoridades encargadas de la ciberseguridad (Estrada, 2024).

Los ciberdelitos más comunes en el Ecuador son el fraude en línea, la violación de la privacidad, el acceso no autorizado a sistemas informáticos, los ataques a la integridad de los sistemas y las transacciones fraudulentas en términos electrónicos. El phishing es uno de los métodos más comunes mediante el cual los delincuentes engañan a las víctimas para que revelen información personal y financiera. Además, existe una creciente preocupación por el ciberacoso y otros delitos que involucran a menores, como el acoso sexual.

Robo de información personal en línea. Según los resultados obtenidos, el 69% de las personas encuestadas respondieron afirmativamente, indicando que han experimentado el robo de información personal en línea. Por otro lado, el 31% restante respondió negativamente, afirmando que no han sido víctimas de dicho robo. Estos resultados pueden ser relevantes desde el punto de vista jurídico, ya que evidencian la existencia de un problema real y preocupante relacionado con la seguridad de la información personal en línea, el alto porcentaje de personas que afirman haber sufrido el robo de información destaca la necesidad de fortalecer las medidas de protección y seguridad en el ámbito digital. Desde el punto de vista legal, este tipo de encuestas puede proporcionar una base de datos útil para comprender la magnitud del problema y orientar la toma de decisiones por parte de los legisladores y las autoridades competentes, estos resultados pueden respaldar la implementación de leyes y regulaciones más rigurosas en materia de protección de datos personales y ciberseguridad, así como el desarrollo de políticas públicas destinadas a prevenir y sancionar el robo de información personal en línea.

2.1.3 Importancia de la Protección de Datos

De acuerdo con Rivera (2020), la importancia de la protección de datos porque garantiza el derecho de los ciudadanos a decidir sobre su información personal y evita su uso indebido por terceros. El avance tecnológico ha generado un mundo digital paralelo donde los datos se gestionan sin control, exponiendo a las personas a riesgos como la violación de la privacidad, la discriminación y el uso no autorizado de su información. En consecuencia, la implementación de leyes y estándares internacionales es definitivo para regular el uso de datos, fomentar una cultura de respeto a la privacidad y garantizar la seguridad digital.

En la práctica, la protección de datos es un aspecto fundamental en la seguridad digital; en especial, en los ambientes de redes de área local, ya que la vulnerabilidad al acceso virtual de la información y datos que se manipulan es mucho mayor. Es decir, no basta con restringir accesos, se deben tomar medidas físicas y lógicas para prevenir la exposición de información, asegurando integridad, confidencialidad y disponibilidad de los datos y la información contenida en los servidores respectivos. En ese sentido, un factor fundamental para la prevención de riesgos y fuga de información es la configuración de firewalls, el cifrado de datos y la prevención de intrusiones ajenas. Del mismo modo, la expansión en el uso de dispositivos y medios inalámbricos presenta un mayor margen de exposición a amenazas (Ponce, 2024).

En Ecuador, el auge de las tecnologías digitales y la recopilación de información por parte de empresas y entidades gubernamentales ha hecho que la protección de datos personales sea un tema central de debate. La promulgación de la Ley Orgánica de Protección de Datos Personales (LOPDP) en 2021 representó un avance en la regulación del uso y almacenamiento de datos en el país, alineándose con estándares internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea (Morales et al., 2024).

La protección de datos personales no es un concepto reciente. Desde la creación de las primeras leyes de privacidad en Europa hasta la implementación del GDPR por la Unión Europea en 2016, el mundo ha comprendido la importancia de salvaguardar la información personal de las personas. En

América Latina, la tendencia hacia la protección de datos ha cobrado fuerza en las últimas décadas, con varios países adoptando sus propias normativas. En este contexto, Ecuador ha seguido la tendencia global, reconociendo la privacidad de datos como un derecho fundamental y respondiendo a la necesidad de una regulación moderna que enfrente los retos de la era digital.

2.1.4 Impacto Social

La protección de los datos tiene un alcance social en varias dimensiones de la vida, sobre todo en esta era de digitalización, es fundamental para proteger derechos básicos fundamentales de las personas, como la privacidad, la seguridad y la libertad de expresión. En la actualidad, los datos personales están constantemente expuestos debido al crecimiento de la tecnología, las redes sociales y la inteligencia artificial, lo que genera preocupaciones sobre el uso indebido de la información (Madrigal, 2024).

Desde una perspectiva social, la protección de datos influye en la confianza de los ciudadanos en las instituciones públicas y privadas, ya que el mal manejo de la información puede derivar en discriminación, exclusión social y violaciones a los derechos humanos. La falta de protección adecuada de los datos personales pone en riesgo la seguridad y la privacidad de los individuos, también afecta su bienestar psicológico y social. Las personas cuyos datos son mal utilizados pueden enfrentar consecuencias como el robo de identidad, el acoso en línea y la discriminación en diversos ámbitos, como el empleo, la salud y la educación. A nivel colectivo, el uso indebido de la información personal también puede socavar la cohesión social, al crear desconfianza entre los ciudadanos y las instituciones, lo que dificulta el desarrollo de una sociedad digital inclusiva y equitativa. En este contexto, la implementación de políticas y leyes de protección de datos se vuelve primordial para salvaguardar los derechos individuales, y para garantizar la estabilidad social y el respeto a la dignidad humana (Acurio & Romero, 2024).

Además, la falta de regulación o el uso indebido de los datos por parte de empresas y gobiernos puede conducir a la manipulación de la opinión pública,

como ocurrió en el caso de Cambridge Analytica, donde se utilizaron datos personales para influir en procesos electorales (Rivadeneira et al., 2023). Asimismo, la transformación digital ha traído consigo la necesidad de una mayor educación y conciencia sobre la seguridad digital, ya que muchas personas desconocen los riesgos asociados a compartir su información en línea (Galindo, 2020).

Molina (2023) asegura que la inteligencia artificial y el Big Data son responsables de la manera en que en que se gestionan los datos personales, permitiendo la recolección masiva de información a través de distintos dispositivos y plataformas, muchas veces sin el conocimiento o consentimiento del usuario. Esto plantea problemas a estas personas en términos de privacidad, ya que se utilizan muchos datos combinados para crear perfiles predictivos, que luego se utilizan para promocionar y vender cualquier cosa o influir en el comportamiento de la persona subyacente en el perfil, o incluso para discriminarlo en el trabajo o en la sociedad en general. Además, el uso de algoritmos en la toma de decisiones automatizadas puede reforzar desigualdades y vulnerar derechos, al replicar sesgos presentes en los datos con los que fueron entrenados.

2.1.5 Gobernanza de Datos

El gobierno de datos es un marco integral que se centra en la capacidad de una organización para gestionar eficazmente sus datos. Este marco incluye las políticas, procedimientos, estructuras organizativas, funciones, responsabilidades y actividades necesarias para utilizar los datos como un recurso real. La gobernanza de datos eficaz permite a las organizaciones cumplir con las leyes de protección de datos, optimizar las operaciones y tomar decisiones basadas en datos de alta calidad.

Fundamentos de la Gobernanza de Datos

Los principios básicos de la gestión de datos se basan en la idea de que los datos son un recurso valioso que debe gestionarse con cuidado. La calidad

de los datos es importante. Los datos inexactos u obsoletos pueden dar lugar a decisiones comerciales incorrectas y a importantes consecuencias financieras y legales. La confiabilidad de los datos garantiza coherencia y precisión a lo largo del tiempo, lo cual es importante para organizaciones como la presentación de informes financieros y el análisis de las condiciones del mercado. La seguridad de los datos protege contra el acceso no autorizado y evita la exposición a riesgos legales y de reputación. La privacidad es importante en el mundo actual, donde los datos personales están adecuadamente protegidos y se cumplen las expectativas de los clientes.

La clasificación de los datos es un proceso fundamental en la gobernanza de estos, este permite organizar la información según su nivel de sensibilidad y uso dentro de una organización. En términos generales, los datos pueden agruparse en varias categorías. Los datos personales incluyen información identificable de individuos, como nombres, direcciones y números de identificación, esto exige su protección conforme a regulaciones de privacidad. Los datos confidenciales abarcan información interna de la organización, como estrategias comerciales, reportes financieros o propiedad intelectual, cuya divulgación no autorizada podría generar riesgos competitivos. Por otro lado, los datos públicos son aquellos accesibles sin restricciones, como informes gubernamentales o publicaciones en sitios web institucionales. Finalmente, los datos críticos para el negocio permiten la operatividad de una empresa, como bases de clientes, registros de transacciones o infraestructura tecnológica, cuya pérdida o alteración podría afectar la continuidad del negocio (Zhang & Datta, 2023).

Una adecuada clasificación de los datos ayuda a la implementación de medidas de seguridad y del cumplimiento legal acordes con su nivel de sensibilidad. Por ejemplo, los datos personales y confidenciales requieren cifrado, controles de acceso y mecanismos de auditoría para prevenir accesos no autorizados y cumplir con regulaciones como la Ley Orgánica de Protección de Datos Personales en Ecuador o el Reglamento General de Protección de Datos (RGPD) en Europa. Asimismo, la correcta categorización de los datos permite definir estrategias de retención y eliminación, asegurando que la

información se conserve solo durante el tiempo necesario y se elimine de manera segura cuando ya no sea requerida (Ávila, 2023).

La seguridad y privacidad de los datos son parte importante de la gobernanza de la información, ya que buscan proteger los datos contra accesos no autorizados, pérdida, manipulación o filtraciones. Para ello, las organizaciones implementan diversas políticas y controles de seguridad. Entre los mecanismos más utilizados se encuentra el cifrado de datos, que transforma la información en un formato ilegible para cualquier persona que no tenga la clave de acceso. La autenticación multifactor (MFA) agrega una capa adicional de seguridad al requerir múltiples métodos de verificación antes de permitir el acceso a los datos. Por otro lado, la anonimización y seudonimización se aplican para reducir los riesgos asociados con el tratamiento de datos personales, dificultando la identificación de los individuos en caso de una filtración. Además, las auditorías de seguridad permiten evaluar continuamente la eficacia de los controles implementados, identificar vulnerabilidades y fortalecer la protección de la información (Autoridad Nacional de Protección de Datos de Singapur, 2022).

En el ámbito normativo, la seguridad y privacidad de los datos están reguladas por marcos legales como la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador y el RGPD en Europa, los cuales establecen obligaciones para el tratamiento de la información personal. Estas regulaciones exigen a las organizaciones aplicar medidas de seguridad adecuadas, garantizar la transparencia en el uso de los datos y permitir a los titulares ejercer sus derechos sobre su información. El incumplimiento de estas normativas puede derivar en sanciones económicas y daños a la reputación de las empresas.

Otro punto relevante en la gobernanza de datos es la gestión de acceso, esta garantiza que solo las personas autorizadas puedan acceder a la información según su rol dentro de la organización. Para ello, se aplica el principio de privilegio mínimo, que establece que los usuarios deben contar únicamente con los permisos estrictamente necesarios para desempeñar sus funciones, reduciendo así el riesgo de exposición de datos sensibles. Este

enfoque reduce el impacto de posibles amenazas internas y evita que empleados, contratistas o terceros accedan a información que no les corresponde. Además, el uso de controles de identidad, como autenticación multifactor (MFA) y gestión centralizada de credenciales, refuerza la seguridad al exigir métodos adicionales de verificación antes de conceder acceso a los sistemas y datos organizacionales (Basile et al., 2023).

Para garantizar un acceso estructurado y seguro, las organizaciones implementan roles y permisos basados en políticas organizacionales. A través de modelos como el control de acceso basado en roles (RBAC), se asignan permisos según la posición o funciones del usuario, evitando asignaciones manuales que pueden generar errores o accesos indebidos. También se emplea el control de acceso basado en atributos (ABAC), que define permisos según reglas específicas como ubicación, dispositivo o nivel de confidencialidad de los datos (B. Campos et al., 2024).

En la gobernanza de datos, la calidad de estos es un principio primordial dentro del derecho a la información y la protección de datos personales, ya que garantiza que los registros almacenados y utilizados por entidades públicas y privadas sean precisos, consistentes, completos y actualizados. Desde el punto de vista normativo, las leyes exigen que los responsables del tratamiento implementen medidas para asegurar la veracidad y actualización de la información, evitando perjuicios a los titulares de los datos. Un dato inexacto o desactualizado puede derivar en decisiones erróneas por parte de entidades gubernamentales, financieras o sanitarias, afectando derechos fundamentales como el acceso a servicios públicos, la contratación laboral o la reputación de las personas (Instituto Geográfico Agustín Codazzi, 2024).

Para garantizar la calidad de los datos y cumplir con las normativas, se aplican técnicas como la deduplicación, que elimina registros redundantes y evita errores en bases de datos; la validación de datos, que verifica que la información ingresada cumpla con criterios de exactitud y coherencia; y el monitoreo de calidad, que permite detectar y corregir inconsistencias a lo largo del tiempo. Estas prácticas mejoran la toma de decisiones dentro de las organizaciones y

refuerzan la seguridad jurídica al garantizar que los datos utilizados en procesos administrativos y judiciales sean confiables. En este contexto, el derecho a la rectificación de datos personales, reconocido en múltiples marcos normativos, permite a los ciudadanos exigir la corrección de información errónea que pueda afectar su identidad, historial crediticio o cualquier otro aspecto relevante de su vida personal y profesional (Mendoza, 2021).

Por otro lado, la retención y eliminación de datos es un aspecto relevante en la protección de la privacidad y el cumplimiento regulatorio, ya que las organizaciones deben gestionar el ciclo de vida de la información conforme a las disposiciones legales. Las legislaciones establecen que los datos personales no deben conservarse más allá del tiempo necesario para cumplir con la finalidad para la que fueron recopilados. Esto implica definir períodos de retención adecuados según la naturaleza de la información, el tipo de entidad que la maneja y los requisitos específicos de cada sector. Por ejemplo, en el ámbito financiero y sanitario, ciertos reglamentos exigen la conservación de registros durante períodos prolongados para auditorías o responsabilidades legales, mientras que otros datos deben eliminarse inmediatamente tras su uso para reducir riesgos de acceso indebido (Ministerio de Ambiente y Desarrollo Sostenible de Colombia, 2025).

Desde una perspectiva jurídica, la eliminación segura de datos permite evitar vulneraciones al derecho a la privacidad y posibles filtraciones de información sensible. Existen métodos como la sobrescritura de datos, la destrucción física de dispositivos de almacenamiento o la anonimización irreversible que permiten que los datos no puedan ser recuperados ni utilizados de forma indebida. El incumplimiento de las políticas de retención y eliminación puede derivar en sanciones legales y responsabilidades civiles, especialmente si la información es utilizada sin el consentimiento del titular o expuesta en incidentes de seguridad (Ministerio de Ambiente y Desarrollo Sostenible de Colombia, 2025).

La trazabilidad y auditoría de datos son otros elementos utilizados para asegurar la transparencia y el cumplimiento de normas en el manejo de la

información. Desde una perspectiva legal, se establece la obligación de registrar y supervisar las actividades relacionadas con el acceso, modificación y eliminación de datos personales. Los registros de auditoría permiten verificar quién accedió a qué información, en qué momento y con qué propósito, lo que resulta fundamental para determinar responsabilidades en caso de incidentes de seguridad o uso indebido de los datos. Además, esta trazabilidad contribuye a garantizar el principio de responsabilidad proactiva, exigiendo que las organizaciones puedan demostrar la implementación de medidas adecuadas para proteger la privacidad de los titulares de datos (Stitilis & Malinauskaite, 2024).

Los registros de auditoría cumplen una función de seguridad, a su vez, sirven como evidencia en procesos legales y administrativos. En casos de violaciones de datos, la trazabilidad facilita la identificación de brechas de seguridad y permite a las autoridades competentes evaluar si la organización ha actuado conforme a las regulaciones aplicables. Además, en sectores altamente regulados como el financiero y el sanitario, las auditorías periódicas son un requisito obligatorio para prevenir fraudes, proteger la confidencialidad de la información y evitar sanciones. La implementación de mecanismos como la firma digital, los registros inmutables y la supervisión en tiempo real refuerza la integridad del sistema de gobernanza de datos (Stitilis & Malinauskaite, 2024).

La interoperabilidad y la gestión del ciclo de vida de los datos permiten la integración segura de sistemas sin comprometer la privacidad de los titulares. En este punto, la interoperabilidad entre sistemas debe cumplir con principios como la minimización de datos, evitando la exposición innecesaria de información sensible, y el consentimiento informado, asegurando que los titulares sean conscientes de cómo se comparte su información entre plataformas. A su vez, el uso de estándares abiertos y mecanismos de autenticación segura contribuye a reducir riesgos de accesos no autorizados y vulneraciones de seguridad (Coloma, 2023).

La gestión del ciclo de vida de los datos implica establecer reglas claras sobre la recolección, almacenamiento, uso, transferencia y eliminación de la

información conforme a los plazos definidos por la legislación aplicable. En sectores como el financiero o el sanitario, donde la interoperabilidad de los sistemas es fundamental para la eficiencia operativa, la normativa exige que las empresas apliquen controles estrictos sobre la trazabilidad y acceso a los datos. La implementación de principios como la portabilidad de datos permite a los usuarios ejercer sus derechos sobre su información, ayudando en la transferencia segura entre plataformas sin vulnerar la privacidad. De igual manera, la correcta administración del ciclo de vida de los datos evita sanciones por retención indebida de información (Coloma, 2023).

Implementación de la Gobernanza de Datos

La implementación efectiva de la gestión de datos requiere un enfoque sistemático y estructurado. Las políticas deben ser claras y ejecutables, con procedimientos establecidos para garantizar su cumplimiento. La distribución de tareas y responsabilidades es importante. Las personas o grupos son responsables de la calidad de los datos, la seguridad, el cumplimiento y la gestión de la privacidad.

Estas actividades deben estar claramente definidas y contar con la autoridad y los recursos necesarios para ser efectivas. La gestión activa de datos tiene muchos beneficios. Una buena gestión puede conducir a una mejor toma de decisiones basada en la calidad y confiabilidad de los datos. También puede aumentar la eficiencia operativa al eliminar redundancias y errores. La reducción de riesgos es otro beneficio importante, ya que una buena gestión de datos ayuda a prevenir violaciones de seguridad y cumplir con las leyes de protección de datos. Además, puede fortalecer la reputación de la organización al demostrar un compromiso con la protección y gestión adecuada de la información.

Además de los beneficios mencionados, la implementación efectiva de la gobernanza de datos también influye directamente en la cultura organizacional. Para que las políticas y procedimientos sean realmente efectivos, es pertinente fomentar una mentalidad organizacional que valore la importancia de los datos en todos los niveles. La capacitación continua y el fortalecimiento de la

conciencia sobre la importancia de la gestión adecuada de los datos son relevantes para mantener el compromiso de los empleados. Una cultura que promueva el respeto por los datos y la privacidad, además de garantizar la transparencia y la responsabilidad, contribuye significativamente al éxito a largo plazo de las iniciativas de gobernanza (Fattah, 2024).

Implicaciones para el ejercicio del derecho a la privacidad

• **Consentimiento de información:** Es importante que los usuarios comprendan la recopilación, uso y protección de sus datos al utilizar estas tecnologías.

• **Transparencia y control**: los usuarios deben tener derechos de acceso y revisión. y gestionar los datos recopilados sobre ellos, y publicar la recopilación de datos que GDPR en la UE y leyes similares en otras jurisdicciones.

En resumen, si bien la tecnología tiene muchos beneficios, también plantea desafíos importantes para proteger la privacidad de las personas. Una aplicación ética y legal adecuada es esencial para mitigar estos riesgos y garantizar que las personas puedan ejercer su derecho a la privacidad en un entorno digital complejo.

Enfoques futuros

Regulación robusta y global: es esencial implementar y reforzar leyes y regulaciones que garanticen la protección de la privacidad de los datos tanto a nivel nacional como internacional, incluyendo normativas claras sobre el consentimiento informado, el derecho al olvido y la responsabilidad de las empresas en la protección de datos.

Educación y concienciación: mejorar la alfabetización digital y la conciencia pública sobre los riesgos y derechos relacionados con la privacidad puede empoderar a los individuos para tomar decisiones informadas sobre la gestión de sus datos personales.

Tecnología para la privacidad: desarrollar y promover tecnologías que protejan proactivamente la privacidad, como herramientas de anonimización de datos, criptografía robusta y sistemas de gestión de consentimientos, puede ayudar a mitigar los riesgos asociados con la recopilación y el uso de datos personales.

Colaboración entre sectores: fomentar la colaboración entre gobiernos, empresas, organizaciones de la sociedad civil y académicos para abordar los desafíos complejos de la privacidad digital, promoviendo estándares éticos y buenas prácticas en la gestión de datos.

Reforzar la rendición de cuentas: establecer mecanismos sólidos de rendición de cuentas y sanciones efectivas para las violaciones de privacidad puede disuadir conductas irresponsables y fortalecer la confianza del público en la gestión de datos por parte de las organizaciones.

Proteger la privacidad en la era digital es un desafío continuo que requiere un enfoque multidimensional que combine regulación efectiva, innovación tecnológica responsable, educación y colaboración global. El equilibrio entre la innovación y la protección de los derechos individuales será fundamental para un futuro digital más seguro y ético.

2.1.6 Políticas Públicas para la digitalización en el Ecuador

El gobierno ecuatoriano, a través del Plan Nacional de Gobierno Electrónico 2018-2021, ha adoptado un enfoque participativo y accesible para mejorar la relación entre los ciudadanos y el gobierno. Se han establecido centros de información y telecentros en comunidades rurales desfavorecidas como puntos de acceso a Internet con el objetivo de reducir la brecha digital y el analfabetismo tecnológico. Sin embargo, a pesar de los avances, la sostenibilidad de estas iniciativas se ha visto comprometida, en parte porque la pandemia de COVID-19 ha limitado la expansión y el mantenimiento de estos

servicios (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2018).

Antes de la pandemia, las políticas públicas tuvieron un impacto significativo en la lucha contra la exclusión digital, pero, como quedó demostrado durante la crisis sanitaria, no brindaron soluciones duraderas.

En 2022, Ecuador continuó enfrentando desafíos en el desarrollo de las tecnologías de la información y las comunicaciones (TIC), entre ellos: Estos incluyen la mala conectividad en las zonas rurales, los altos costos del servicio, la mala calidad de los proveedores de Internet y los altos impuestos a los dispositivos móviles para garantizar la inclusión digital de las personas con discapacidad.

Con el Plan de Transformación Digital de Ecuador 2022-2025, el país apunta a digitalizar el gobierno para mejorar los servicios públicos y afrontar los desafíos de la digitalización. Sin embargo, se ha considerado importante para la implementación de políticas de tecnologías de la información y las comunicaciones (TIC), la mejora de la infraestructura tecnológica, la reducción de los impuestos a las importaciones de tecnología y la reforma de las leyes. El objetivo es hacer que los teléfonos sean lo más convenientes, de calidad y consistentes posible (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022).

Estos esfuerzos reflejan la comprensión de que, a pesar de los avances, la implementación de políticas públicas no ha sido suficiente para cerrar la brecha digital, especialmente en las zonas rurales y desatendidas. La idea es que antes de proceder con la implementación de estas directrices, se debe crear un marco legal sólido que permita un mejor y más eficiente uso de los recursos técnicos.

2.1.7 Manejo de la privacidad de información personal en las empresas.

Los resultados obtenidos, el 55% de las personas encuestadas respondieron que las empresas siempre respetan su derecho a la privacidad al recopilar información personal. El 37% indicó que las empresas lo hacen a veces, mientras que el 8% afirmó que las empresas nunca respetan su derecho a la privacidad. Estos resultados son relevantes desde el punto de vista jurídico, ya que reflejan la percepción de las personas encuestadas sobre el grado de respeto de las empresas hacia su derecho a la privacidad, el alto porcentaje de personas que creen que las empresas siempre respetan su derecho a la privacidad sugiere que existe confianza en las prácticas de recopilación de información personal por parte de las empresas. Sin embargo, el porcentaje significativo de personas que consideran que las empresas lo hacen solo a veces o nunca indica preocupación y desconfianza en cuanto a la protección de su privacidad por parte de las empresas.

Medidas consideradas necesarias para proteger la privacidad en la era digital

En primer lugar, se resalta la importancia de cuidar nuestras contraseñas y utilizar contraseñas o códigos seguros. Además, se mencionó la necesidad de ser selectivos al proporcionar datos personales y de evitar compartirlos con terceros. Los encuestados sugirieron que las empresas en línea deben tener requisitos más estrictos al recopilar información personal y deben adherirse a políticas de privacidad clara y centrada en el usuario. La encuesta reveló una preocupación generalizada sobre la privacidad en la era digital, los participantes sugirieron implementar leyes de protección de datos y sanciones para la vulneración de la privacidad, también abogaron por contar con agentes especializados en ciberseguridad y mejorar la seguridad de las bases de datos para evitar accesos no autorizados. Se destacó la importancia de fortalecer contraseñas, regulaciones legales y capacitación de usuarios para salvaguardar la privacidad y promover un uso seguro de la tecnología en el entorno digital.

2.1.8 Regulaciones internacionales sobre privacidad y protección de datos

El Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) es la normativa de privacidad y protección de datos más estricta de la Unión Europea, vigente desde mayo de 2018. Su objetivo principal es otorgar a los ciudadanos un mayor control sobre su información personal y unificar la regulación en los Estados miembros. Se aplica a cualquier organización, dentro o fuera de la UE, que procese datos personales de residentes europeos, estableciendo principios fundamentales como la transparencia, la minimización de datos y la responsabilidad en su tratamiento (Guamán et al., 2021).

Entre los aspectos clave del GDPR se encuentra el consentimiento explícito de los usuarios para el tratamiento de sus datos, el derecho a ser olvidado, la portabilidad de la información y la obligación de las empresas de informar sobre violaciones de seguridad en un plazo máximo de 72 horas. Además, introduce sanciones para las organizaciones que incumplan sus disposiciones, con multas que pueden alcanzar hasta el 4% de la facturación global anual o 20 millones de euros, esto ha incentivado a muchas empresas a reforzar sus políticas de seguridad y cumplimiento (Abanlex, 2022).

El impacto del GDPR ha trascendido las fronteras de la UE, influyendo en legislaciones de otros países y promoviendo un estándar más elevado en la protección de datos a nivel global. Muchas empresas han adoptado medidas adicionales para cumplir con la normativa, como la implementación de oficiales de protección de datos (DPO), auditorías constantes y sistemas de anonimización de datos. No obstante, el reglamento también ha generado dificultades, especialmente para pequeñas y medianas empresas que deben destinar recursos adicionales para su cumplimiento (Abanlex, 2022).

En cambio, la Ley de Privacidad del Consumidor de California (CCPA), que entró en vigor en enero de 2020, es una de las regulaciones más importantes en Estados Unidos en cuanto a privacidad de datos. Esta ley otorga a los residentes de California derechos más amplios sobre la recopilación, uso y venta de su información personal. El CCPA permite a los consumidores solicitar a las empresas que divulguen los datos personales que han recopilado sobre ellos, exijan la eliminación de dichos datos y opten por no permitir la venta de su

información a terceros. A su vez, las empresas deben proporcionar una política de privacidad describiendo sus prácticas de manejo de datos (State of California Department of Justice, 2024).

Una de las características distintivas de la CCPA es la facultad de los consumidores para ejercer un derecho a la no discriminación, lo que significa que no pueden ser penalizados si eligen ejercer sus derechos bajo la ley, como la opción de optar por no vender su información. Las empresas también deben verificar la identidad de los solicitantes antes de proporcionar o eliminar datos personales, lo que busca prevenir fraudes. De igual forma, la ley exige que las empresas informen sobre las categorías de datos que recopilan, el propósito para el cual se usan y los posibles destinatarios de esos datos (State of California Department of Justice, 2024).

Aunque la CCPA ha sido un avance importante en la protección de datos en Estados Unidos, también ha generado varios problemas para las empresas. La falta de una legislación federal uniforme sobre privacidad de datos ha provocado una variedad de interpretaciones y enfoques, esto genera incertidumbre en las empresas que operan en varios estados. Como respuesta, se han propuesto enmiendas y nuevas leyes, como la California Privacy Rights Act (CPRA), que amplía y refuerza el CCPA, dándole aún más poder a los consumidores y creando una Agencia de Privacidad de California dedicada a supervisar el cumplimiento de la ley (California Privacy Rights Act, 2020).

En América Latina, varios países han adoptado leyes y regulaciones relacionadas con la protección de datos personales, inspirados por modelos como el GDPR de la Unión Europea. Un ejemplo destacado es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de México, que establece principios y obligaciones para el tratamiento de datos personales en el sector público y privado. Esta ley se enfoca en la transparencia, el consentimiento de los individuos y la protección de sus derechos, permitiendo a los ciudadanos acceder, rectificar y eliminar sus datos. También se contemplan sanciones para las empresas que incumplen sus disposiciones, al igual que el GDPR (Cámara de Diputados de México, 2017).

En Brasil, la Lei Geral de Proteção de Dados Pessoais (LGPD), promulgada en 2018 y vigente desde 2020, es otra de las legislaciones más relevantes en América Latina. Similar al GDPR, la LGPD establece un marco regulatorio integral para la protección de los datos personales de los ciudadanos brasileños, con un enfoque en el consentimiento, la transparencia y la seguridad de los datos. La ley aplica tanto a empresas locales como a aquellas extranjeras que procesan datos de residentes brasileños, y se espera que impulse a las organizaciones a mejorar sus políticas de privacidad y seguridad. La creación de una Autoridad Nacional de Protección de Datos (ANPD) supervisa el cumplimiento de la ley y sanciona a las empresas que violen sus disposiciones (Congreso Nacional de Brasil, 2019).

A nivel mundial, otras jurisdicciones también han establecido regulaciones estrictas sobre la privacidad y protección de datos. Un ejemplo notable es Australia, que implementó la Privacy Act 1988, modificada en los últimos años para adaptarse a las nuevas realidades digitales. La ley establece principios de privacidad y regulaciones para el manejo de datos personales, con un enfoque en el derecho de los individuos a acceder a sus datos y corregirlos (Australian Government, 2025). En Asia, países como Japón y Corea del Sur también han adoptado legislaciones estrictas, como la Act on the Protection of Personal Information (APPI) en Japón, que fue reformada en 2020 para alinearse con los estándares internacionales de privacidad (Personal Information Protection Commission, 2025).

2.1.9 Estudios de casos internacionales

Hemos visto ejemplos de casos legales y violaciones de la privacidad que han impactado las discusiones legislativas o judiciales internacionales.

- Facebook y Cambridge Analytica En 2018, la consultora política Cambridge Analytica recopiló datos personales de millones de usuarios de Facebook sin su consentimiento para influir en las campañas políticas. El caso desató una gran controversia sobre la privacidad en línea y llevó a Facebook a

enfrentar investigaciones regulatorias en varios países y cambios importantes en sus políticas de privacidad.

- Schrems II contra Facebook El activista de privacidad Maximilian Schrems ha lanzado un desafío legal a la transferencia de datos personales de la UE a los EE. UU., argumentando que los estándares de protección de datos estadounidenses son insuficientes. En 2020, el Tribunal de Justicia de la Unión Europea invalidó el acuerdo de Puerto Seguro que facilitaba las transferencias transatlánticas de datos y posteriormente impugnó el Escudo de Privacidad. Estos casos resaltan la importancia de garantizar la protección efectiva de los datos personales durante las transferencias internacionales.

- Reglamento GDPR y multas para grandes empresas. Desde la implementación del Reglamento General de Protección de Datos , varias empresas se han enfrentado a enormes multas debido a violaciones de datos. Por ejemplo, Google fue multada con 50 millones de euros por no obtener un consentimiento válido para la personalización de anuncios, y otras empresas fueron multadas por violar los derechos de acceso y eliminación de datos de los usuarios.

- Controversia sobre WhatsApp y cambios en la política de privacidad A principios de 2021, WhatsApp, propiedad de Facebook, anunció cambios en su política de privacidad para permitir el intercambio de datos con Facebook para mejorar la orientación de los anuncios. Esto ha generado preocupación y críticas en varios países, lo que ha llevado a usuarios y reguladores a cuestionar cómo se manejan los datos personales en las grandes plataformas de mensajería y redes sociales.

2.1.10 Estudios de caso en Ecuador

Aquí tenemos algunas sentencias relevantes de la Corte Constitucional de Ecuador sobre privacidad y protección de datos en el contexto digital.

Sentencia 59-19-IN/24

La sentencia 59-19-IN/24 fue dictada el 11 de julio de 2024, cuyo emisor fue el Pleno de la Corte Constitucional del Ecuador. La sentención se debió a la presentación de una acción de inconstitucionalidad contra el Acuerdo Ministerial 0341-2019, que aprobaba y autorizaba la aplicación del instructivo denominado Aplicación de la Historia Clínica Ocupacional, el cual establecía la obligatoriedad de formularios médicos ocupacionales en el ámbito laboral. Las demandantes alegaban que esta normativa violaba los derechos a la intimidad y a la protección de datos personales establecidos en los artículos 66.19 y 66.20 de la Constitución. El problema jurídico se centró en determinar si el Acuerdo Ministerial 0341-2019 y sus formularios vulneran los derechos a la intimidad y a la protección de datos personales de los trabajadores; así como si es constitucional que el Ministerio de Salud Pública exija datos personales sensibles sin el consentimiento explícito de los trabajadores.

Al respecto, la Corte Constitucional reconoció la importancia de la salud ocupacional y la planificación de políticas públicas, pero enfatizó que esto no puede vulnerar derechos fundamentales. Por ello, aplicó un test de proporcionalidad para analizar si la limitación a los derechos de los trabajadores era legítima y necesaria. En dicho análisis, la Corte determinó que la recopilación obligatoria de ciertos datos sensibles (orientación sexual, identidad de género, religión) no era esencial para cumplir el objetivo del MSP. En ese sentido, se concluyó que la afectación a la intimidad y autodeterminación informativa de los trabajadores era desproporcionada frente a los beneficios perseguidos. Por lo tanto, se declaró la inconstitucionalidad del Acuerdo Ministerial 0341-2019 con efectos diferidos, es decir, su aplicación quedaría sin efecto, aunque con un período de transición para que el MSP reformule los formularios de historia clínica ocupacional, eliminando la solicitud de información innecesaria y garantizando un tratamiento adecuado de los datos personales.

Sentencia No. 2064-14-EP/21

La Sentencia No. 2064-14-EP/21 de la Corte Constitucional del Ecuador tuvo como fecha de emisión el 27 de enero de 2021. Esta sentencio tuvo lugar

debido a una acción extraordinaria de protección contra una sentencia de segundo nivel que revocó la decisión de primera instancia en una acción de hábeas data. La actora presentó una acción contra una persona natural (la demandada), con el objetivo de conocer cómo esta llegó a poseer fotografías íntimas y personales de la demandante. También solicitó su eliminación inmediata y una reparación integral por la vulneración de sus derechos. El problema jurídico implicó juzgar si se vulneraron los derechos constitucionales de la actora al revocar la sentencia de primera instancia. De igual manera, si el tratamiento de las fotografías por parte de la demandada constituyó una violación al derecho a la protección de datos personales y a la autodeterminación informativa.

Frente a los hechos, la Corte Constitucional consideró que la demandante tenía derecho a que su apelación fuera analizada solo en relación con la reparación integral y que la Corte Provincial no podía fallar en su contra en aspectos que ella no impugnó; y se confirmó que la decisión de segunda instancia vulneró el principio de *non reformatio in pejus*. De igual forma, la Corte señaló que la demandada no demostró tener el consentimiento explícito de la actora para poseer y almacenar dichas imágenes, lo que configuró una vulneración a la protección de datos personales. En ese sentido, ordenó la eliminación de las fotografías y presentar una declaración juramentada certificando su eliminación. Esta sentencia marca un precedente en la protección de datos personales, debido a que refuerza la idea de que la posesión no consentida de imágenes personales constituye un tratamiento indebido de estos.

Sentencia No. 29-21-JI

La Corte Constitucional del Ecuador emitió la Sentencia No. 29-21-JI el 1 de diciembre de 2021, como respuesta al caso de acciones de acceso a la información pública presentadas por la Defensoría del Pueblo contra el Ministerio de Salud Pública (MSP) respecto al acceso a datos sobre el proceso de vacunación contra la COVID-19. El problema jurídico radica en si el MSP vulneró el derecho de acceso a la información pública al no entregar datos completos sobre el proceso de vacunación; asimismo, si la entrega del listado de vacunados

con sus datos personales (nombre, cédula, edad, grupo prioritario) afecta derechos de privacidad y confidencialidad; de igual manera, cómo debe ponderarse el derecho de acceso a la información pública con la protección de datos personales en el contexto de una pandemia. La parte demandante argumentó que el derecho de acceso a la información es fundamental en el control ciudadano de políticas públicas. Por su lado, el demandado sostuvo que los nombres y cédulas de los vacunados son información confidencial protegida por la normativa de datos personales.

Al respecto, la Corte Constitucional determinó que la información sobre las vacunas y su distribución es de carácter público y debe ser accesible a la ciudadanía, ya que implican el uso de recursos públicos. No obstante, reconoció que los nombres, apellidos y cédulas son datos personales protegidos por el derecho a la privacidad. En línea con ese fundamento, la Corte decidió que se podían entregar ciertos datos (como grupos prioritarios y cantidad de dosis aplicadas), sin divulgar información que pudiera vulnerar la privacidad de las personas vacunadas. En esta sentencia, se prohibió la entrega de nombres y cédulas de personas vacunadas, reafirmando la protección de datos personales.

2.1.11 Dificultades y tendencias en la protección de datos en la era digital

Las amenazas cibernéticas han evolucionado rápidamente en los últimos años, y los ataques de ransomware, el phishing avanzado y el fraude en línea son algunas de las formas más sofisticadas y peligrosas que enfrentan las organizaciones y los individuos en la era digital. El ransomware ha ganado notoriedad por su capacidad de bloquear el acceso a sistemas críticos y exigir un rescate a cambio de la liberación de los datos, lo que pone en riesgo tanto la operatividad como la seguridad de la información. El phishing avanzado se ha vuelto más engañoso, utilizando técnicas como el spoofing o la suplantación de identidad para engañar a los usuarios y obtener acceso a información sensible. El fraude en línea, por su parte, incluye desde transacciones falsas hasta la manipulación de sistemas de pago electrónicos, lo que afecta tanto a los consumidores como a las empresas (Marais et al., 2022).

Desde una perspectiva legal, estos delitos cibernéticos presentan retos significativos en cuanto a la protección de datos personales y la responsabilidad de las empresas. Las organizaciones se enfrentan a un entorno normativo cada vez más estricto, con reglamentos que exigen que se tomen medidas preventivas y reactivas frente a estas amenazas. Las empresas tienen la obligación de implementar medidas de seguridad robustas para proteger la información personal de sus clientes, y en caso de un ataque, deben notificarlo de manera oportuna a las autoridades y a los afectados. El incumplimiento de estas normativas pone en riesgo la privacidad de los datos, puede generar sanciones económicas y daños reputacionales que afectan la confianza del consumidor y la integridad de la empresa (Campos, 2025).

Para combatir estas amenazas, las organizaciones están adoptando diversas medidas de seguridad para proteger los datos personales de los usuarios. Entre las principales estrategias se encuentran el cifrado de datos, que asegura que la información esté protegida incluso si es interceptada, y el uso de autenticación multifactor para reforzar la seguridad de las cuentas de usuario. Además, las empresas están invirtiendo en sistemas de detección de intrusiones y monitoreo continuo para identificar comportamientos sospechosos y prevenir ataques antes de que se materialicen. También se está promoviendo la educación de los usuarios sobre las mejores prácticas de seguridad digital, como el reconocimiento de correos electrónicos de phishing y la creación de contraseñas fuertes. A nivel normativo, las regulaciones están impulsando la adopción de estándares más rigurosos para la protección de datos, lo que obliga a las empresas a establecer medidas más estrictas para salvaguardar la privacidad de los datos personales (Oña et al., 2025).

La inteligencia artificial (IA) está revolucionando las estrategias de seguridad de datos mediante el uso de técnicas avanzadas para detectar patrones anómalos y realizar análisis predictivos de riesgos. A través de algoritmos de aprendizaje automático y minería de datos, la IA es capaz de analizar grandes volúmenes de información y reconocer comportamientos inusuales que podrían indicar una violación de seguridad. Esto permite a las organizaciones detectar ataques como intrusiones, fraudes y otros incidentes de

seguridad antes de que se materialicen. El análisis predictivo, por su parte, permite prever posibles vulnerabilidades en los sistemas y adoptar medidas preventivas para mitigar riesgos, mejorando significativamente la capacidad de respuesta ante amenazas cibernéticas en tiempo real (Schmitt, 2023).

En términos legales, el uso de la IA en la seguridad de datos, especialmente en sistemas de autenticación biométrica como el reconocimiento facial y las huellas dactilares, plantea importantes consideraciones sobre la privacidad y el consentimiento. Las regulaciones como el GDPR en Europa y la CCPA en California exigen que las empresas obtengan el consentimiento explícito de los usuarios antes de recolectar y procesar datos biométricos, considerados como información sensible. Además, deben garantizar que estos datos se almacenen de manera segura y que no sean utilizados para fines no autorizados. Las organizaciones deben ser transparentes sobre cómo se emplean estas tecnologías y asegurarse de que los usuarios tengan acceso a sus datos y puedan solicitarlos o eliminarlos, de acuerdo con sus derechos legales (Abanlex, 2022; State of California Department of Justice, 2024).

Sin embargo, el uso de la IA en la protección de datos también enfrenta problemas relacionados con la transparencia y la explicabilidad de los algoritmos utilizados. Los algoritmos de aprendizaje automático pueden ser complejos y operar como cajas negras, lo que dificulta entender cómo se toman las decisiones sobre la seguridad de los datos. Esta falta de transparencia plantea preocupaciones sobre la posible discriminación o sesgo en los sistemas de autenticación, así como la necesidad de que los usuarios comprendan cómo sus datos son procesados (Campos, 2025). Desde una perspectiva legal, esto puede generar dificultades en términos de cumplimiento normativo, ya que las leyes de protección de datos exigen que las empresas proporcionen explicaciones claras sobre el funcionamiento de los sistemas que procesan datos personales.

El uso de la tecnología blockchain en la protección de datos personales ha emergido como una herramienta poderosa para garantizar la integridad y la inmutabilidad de la información. Blockchain, al ser una cadena de bloques descentralizada, permite que los datos se registren de manera segura y que una

vez ingresados no puedan ser modificados ni eliminados sin el consenso de todos los participantes en la red. Esta característica es especialmente valiosa en el contexto de la protección de datos, ya que asegura que los datos personales almacenados en la blockchain sean inalterables, proporcionando una capa adicional de seguridad frente a intentos de manipulación o acceso no autorizado. Además, la transparencia inherente a la tecnología permite a los usuarios monitorear quién accede a sus datos y cómo se utilizan, lo que refuerza la confianza en el sistema de protección (Basile et al., 2023).

La adopción de blockchain en la gestión de datos personales tiene el potencial de transformar significativamente la manera en que las organizaciones manejan la privacidad. En lugar de depender de bases de datos centralizadas, que son vulnerables a ataques y violaciones de seguridad, blockchain ofrece un enfoque descentralizado que distribuye la información a través de múltiples nodos, minimizando los riesgos de acceso no autorizado. Las ventajas legales de esta adopción son claras: se puede demostrar de manera eficaz que los datos no han sido alterados desde su entrada en la cadena, lo cual es un elemento relevante para el cumplimiento de normativas de protección de datos. Además, el uso de blockchain podría facilitar el ejercicio de derechos de los usuarios, como el derecho a la portabilidad de los datos, ya que la información se encuentra registrada en un formato que es fácilmente accesible y verificable por los usuarios, sin la necesidad de intermediarios (Basile et al., 2023).

Sin embargo, la implementación de blockchain en la protección de datos personales enfrenta varios problemas técnicos y regulatorios. Uno de los principales obstáculos es la escalabilidad de la tecnología, ya que las blockchains públicas pueden volverse lentas y costosas cuando se procesan grandes volúmenes de datos. Además, la adopción generalizada de blockchain por parte de las organizaciones puede verse limitada por la falta de conocimiento técnico y la resistencia al cambio, especialmente en sectores tradicionales o conservadores que aún dependen de sistemas centralizados. Desde una perspectiva legal, el reto también radica en la integración de blockchain con las normativas existentes, ya que la descentralización y la immutabilidad de la tecnología pueden entrar en conflicto con principios como el derecho al olvido

bajo el GDPR, que exige la eliminación de datos personales en determinadas circunstancias. Este conflicto plantea interrogantes sobre cómo reconciliar las características de blockchain con los derechos de privacidad y protección de datos que las leyes buscan salvaguardar.

La recopilación masiva de datos personales ha generado una serie de dilemas éticos que requieren una reflexión profunda, especialmente en cuanto a la violación de la privacidad y el uso de datos sin el consentimiento explícito de los usuarios. En muchas ocasiones, las empresas y otras entidades obtienen acceso a datos sensibles sin proporcionar a los individuos una comprensión clara de cómo se utilizarán estos datos ni obtener su consentimiento informado, lo que pone en cuestión los principios fundamentales de la autonomía y la privacidad. La falta de transparencia en estos procesos, combinada con la creciente capacidad de las tecnologías para almacenar y analizar grandes cantidades de información, plantea la preocupación de que los individuos puedan estar siendo explotados sin su conocimiento o acuerdo, especialmente cuando estos datos son utilizados para fines comerciales, políticos o sociales sin su explícita autorización.

En este contexto, la vigilancia masiva se ha convertido en uno de los principales problemas éticos asociados con la recopilación de datos. La capacidad de los gobiernos y empresas para monitorear a gran escala las actividades de los individuos plantea serias implicaciones sobre el derecho a la privacidad y las libertades civiles. El uso de tecnologías como el reconocimiento facial, la geolocalización y el seguimiento en línea permite una vigilancia detallada y continua de las personas, lo que puede llevar a abusos, como la represión política, la discriminación o el control social excesivo. Este tipo de prácticas también puede derivar en una normalización de la intrusión en la vida privada, debilitando los mecanismos de protección de derechos fundamentales y favoreciendo una cultura de vigilancia sin un marco legal adecuado que limite su alcance y uso.

El debate ético sobre la protección de datos personales versus el desarrollo de nuevas tecnologías como la IA y el análisis de grandes datos (big

data) se encuentra en el centro de la discusión sobre la privacidad. Estas tecnologías ofrecen avances significativos en áreas como la salud, el transporte y la educación, sin embargo, también presentan riesgos importantes para la seguridad de los datos y los derechos de los individuos. La recopilación masiva de datos es fundamental para el funcionamiento de la IA y el big data, pero esta recopilación debe equilibrarse cuidadosamente con la necesidad de proteger la privacidad de los individuos. Este debate exige una regulación clara que permita el desarrollo tecnológico sin comprometer los derechos fundamentales de los ciudadanos (Erdélyi et al., 2023).

Una de las principales dificultades regulatorias en la protección de datos personales es la falta de armonización global en las normativas de privacidad. A pesar de los esfuerzos de regulación, existe una notable diversidad en las legislaciones nacionales sobre privacidad de datos, lo que genera un entorno complejo para las organizaciones que operan a nivel global. Cada país tiene diferentes enfoques y estándares para la recopilación, el procesamiento y la transferencia de datos personales, lo que dificulta la creación de políticas de protección de datos coherentes y uniformes. Esta disparidad genera dificultades para las empresas que deben cumplir con múltiples marcos legales, a su vez, plantea problemas para los individuos, quienes pueden enfrentar la dificultad de entender sus derechos y cómo se protegen en diversas jurisdicciones. Por lo tanto, se hace evidente la necesidad de una regulación global armonizada que pueda facilitar el cumplimiento y mejorar la protección de los datos personales a nivel internacional.

Las pequeñas y medianas empresas (PYMEs) enfrentan problemas adicionales al intentar implementar políticas de protección de datos que cumplan con los requisitos legales. A menudo, estas empresas carecen de los recursos financieros y humanos necesarios para adoptar tecnologías avanzadas de protección de datos o para contratar personal especializado en cumplimiento normativo. A pesar de que muchas legislaciones, como el GDPR, establecen obligaciones para todas las organizaciones, independientemente de su tamaño, las PYMEs se ven particularmente afectadas por los costos asociados con la adaptación tecnológica, la formación del personal y la gestión de la privacidad.

Además, la complejidad de las normativas, junto con la falta de claridad en la interpretación y aplicación de los requisitos, puede generar incertidumbre y riesgos de incumplimiento, lo que podría resultar en sanciones significativas (Lucio & Campaña, 2024). Por tanto, se necesita proporcionar apoyo técnico y asesoría jurídica para las PYMEs, permitiendo que puedan cumplir con las normativas sin comprometer su sostenibilidad económica.

2.1.12 Definiciones

1. Protección de Datos Personales

La protección de datos personales se refiere a las normativas y prácticas diseñadas para proteger la información identificable de las personas y garantizar que se maneje de manera ética y segura. Las leyes de protección de datos buscan regular cómo las organizaciones recopilan, almacenan y procesan los datos personales.

2. Regulaciones Internacionales y Regionales

Las regulaciones como el GDPR en la Unión Europea y la CCPA en California establecen estándares globales para la privacidad de los datos. Estas leyes influencian no solo las prácticas dentro de sus jurisdicciones, sino también globalmente debido a la naturaleza transnacional del internet.

3. Derechos Digitales

Los derechos digitales incluyen el derecho a la privacidad, la protección de datos y la seguridad en el entorno digital. Estos derechos están consagrados en diversos marcos legales y tratados internacionales, y están destinados a proteger a los individuos de abusos y violaciones de su privacidad.

4. Tecnologías Emergentes y Desafíos

La rápida evolución de las tecnologías, como la inteligencia artificial y el análisis de big data, presenta nuevos desafíos para la privacidad de los datos. Las leyes deben adaptarse para abordar estos desafíos, equilibrando la innovación con la protección de los derechos individuales.

5. Cumplimiento y Aplicación

La eficacia del marco legal depende no solo de la existencia de regulaciones, sino también de su implementación efectiva y del cumplimiento por parte de las organizaciones. Esto incluye la capacidad de las autoridades para hacer cumplir las leyes y de las empresas para adherirse a ellas.

2.2 Marco Legal:

2.2.1 Constitución de la República del Ecuador

Ecuador se constituye como un Estado constitucional de derechos y justicia, en el que todas las personas se convierten en amparadas, bajo la protección de la carta magna. De hecho, si bien es cierto, el país cuenta con una de las constituciones consideradas at the time modernas en América Latina, no solo por ser inclusivo, sino también por estar comprometido con la era digital e irse por la tendencia informativa en la línea de las nuevas tecnologías. Desde este punto, la protección de datos personales se constituye como un mecanismo jurídico cuya finalidad general es la de hacer efectivo el derecho de las personas a tener una vida privada en torno a la información que se puede derramar en diferentes lugares físicos como en varios savants digitales. A eso se le llama la privacidad de la información personal.

El Artículo 66 de la Constitución del Ecuador establece los derechos de las personas, dentro de los cuales los numerales 11 y 19 son esenciales para la protección de la privacidad y los datos personales en entornos digitales. El Numeral 11 garantiza el derecho a la reserva de las convicciones personales, lo que refuerza el principio de confidencialidad en el ámbito digital, asegurando que los datos relacionados con ideologías, creencias o cualquier tipo de información

sensible no sean divulgados sin consentimiento. Por su parte, el Numeral 19 reconoce el derecho a la protección de datos personales, incluyendo el acceso, control y resguardo de la información, lo cual es fundamental en la regulación de la privacidad digital y la gestión de datos en plataformas tecnológicas (Constitución de la Republica del Ecuador, 2008).

En el contexto de esta investigación, los numerales 11 y 19 de la Constitución del Ecuador proporcionan un marco legal clave para comprender cómo se deben garantizar y proteger los derechos de privacidad y datos personales en la era digital. Estos artículos establecen los derechos fundamentales de las personas, y proporcionan una base para la implementación de medidas que aseguren la confidencialidad y la integridad de la información personal. El principio del consentimiento informado, que es central para el tratamiento de datos en plataformas digitales, se encuentra respaldado por estos numerales, lo que permite analizar la importancia de que los ciudadanos tengan control sobre sus propios datos.

A su vez, la constitución reconoce la necesidad de que los datos sean tratados con seguridad, esto plantea la obligación de crear mecanismos robustos para prevenir el acceso no autorizado, la divulgación o el uso indebido de la información personal. También se resalta el derecho de los ciudadanos a acceder, corregir y eliminar la información que les concierne, lo que se alinea con los principios de autodeterminación informativa y el derecho a la rectificación. Este análisis refuerza la importancia de contar con una regulación coherente y eficaz que proteja la privacidad en un contexto donde el uso de tecnologías digitales sigue creciendo.

2.2.2 Ley Orgánica de Protección de Datos Personales

El marco teórico en el estudio del marco legal de la tecnología digital y la privacidad de los datos se basa en la intersección de la protección de datos personales, la regulación de tecnologías emergentes y los derechos fundamentales de los individuos en un entorno digital. Este marco explora cómo las normativas intentan equilibrar la innovación tecnológica con la protección de

la privacidad, garantizando derechos individuales mientras se promueve el desarrollo tecnológico.

La aprobación de la Ley Orgánica de Protección de Datos Personales en Ecuador en 2021 no ocurre de manera aislada, sino que forma parte de un contexto global donde la conciencia sobre la importancia de la privacidad de los datos ha ido en aumento. Durante la última década, han tenido lugar una serie de acontecimientos que han transformado radicalmente la percepción pública sobre la seguridad y el control de la información personal. Escándalos de gran repercusión, como las revelaciones de Edward Snowden en 2013 sobre programas de vigilancia masiva, y violaciones de seguridad que han afectado a millones de personas, como el caso de Cambridge Analytica en 2018, han evidenciado las debilidades en la protección de los datos personales y han generado una demanda global por una regulación más estricta.

Estos eventos han demostrado no solo lo fácil que es comprometer la información personal en la era digital, sino también las posibles consecuencias devastadoras de tales violaciones para la privacidad individual y la estabilidad de las democracias. La respuesta a estos desafíos ha sido variada, incluyendo desde la implementación de políticas de privacidad más estrictas por parte de las empresas tecnológicas hasta la creación de leyes nacionales y acuerdos internacionales más rigurosos.

En este marco, la LOPDP de Ecuador se alinea con iniciativas internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, considerado un referente en la protección de datos. La ley ecuatoriana muestra un entendimiento de que la protección de datos personales supera las fronteras nacionales y requiere tanto cooperación global como mecanismos internos de control que aseguren la autonomía y los derechos de las personas sobre su información personal.

Por lo tanto, la LOPDP es un reconocimiento de la interdependencia global y la necesidad de armonizar las prácticas de protección de datos con los estándares internacionales. Al mismo tiempo, refleja un compromiso con los

ciudadanos ecuatorianos para proteger su información personal frente al uso indebido, el acceso no autorizado y las filtraciones. Esta ley establece un marco legal que busca no solo prevenir violaciones de datos, sino también proporcionar los medios para perseguir y sancionar eficazmente a quienes incumplan las normativas de privacidad.

Objeto y aplicación:

La LOPDP se extiende a entidades públicas y privadas que traten datos personales dentro de Ecuador, así como a aquellos responsables fuera del país cuyas actividades impacten a ciudadanos residentes en Ecuador. La ley cubre datos procesados de manera automatizada o manual, incluyendo la recopilación, registro, organización, almacenamiento, modificación, recuperación, consulta, uso, divulgación a través de transmisión, difusión u otros métodos de acceso, alineación o combinación, además de la restricción, eliminación o destrucción de datos personales.

Principios Rectores:

Los principios de la LOPDP incluyen la legalidad del tratamiento, que exige el cumplimiento de la legislación aplicable; la lealtad y transparencia, que obliga a informar al titular sobre el uso de sus datos; la limitación de la finalidad, que impide utilizar los datos para fines diferentes a aquellos para los cuales fueron recopilados; la minimización de datos, que recomienda limitar el tratamiento a lo estrictamente necesario; la exactitud, que exige mantener los datos actualizados y precisos; la limitación del plazo de conservación, que establece restricciones temporales para el almacenamiento de datos; la integridad y confidencialidad, que requiere proteger los datos contra tratamientos no autorizados o ilícitos y contra su pérdida, destrucción o daño accidental; y la responsabilidad proactiva, que demanda a los responsables y encargados del tratamiento demostrar su cumplimiento con estos principios.

Derecho del Propietario:

La ley garantiza y reconoce los derechos ARCO (acceso, rectificación, cancelación y oposición) así como el derecho a la portabilidad y a no tomar decisiones basadas únicamente en el tratamiento automatizado de datos. Estos derechos permiten a las personas ejercer un control efectivo sobre sus datos personales y requieren que los controladores de datos respeten su privacidad.

Personas responsables:

Los controladores de datos deben cumplir con obligaciones específicas, incluida la implementación de políticas y procedimientos de privacidad que garanticen la protección de datos, la realización de evaluaciones de impacto sobre la protección de datos personales y la notificación de cualquier violación de seguridad a las autoridades competentes y a los interesados afectados dentro de un período de tiempo específico.

Seguridad de datos:

La Ley Orgánica de Protección de Datos Personales de Ecuador estipula que las entidades públicas y privadas deben implementar medidas de seguridad técnicas y organizativas para proteger los datos personales. Estas medidas deben ser proporcionales al nivel de riesgo de las operaciones de procesamiento de datos y tener en cuenta la probabilidad y la gravedad del impacto sobre los derechos y libertades de las personas. La ley reconoce que la seguridad de los datos es un proceso dinámico, por lo que las medidas deben revisarse y actualizarse periódicamente para adaptarse a los avances tecnológicos y los nuevos desafíos de seguridad. Estos incluyen el cifrado de datos, la seguridad física y lógica del sistema y la capacitación continua del personal involucrado en el procesamiento de datos.

Autoridad de Control:

La LOPDP establece la Autoridad de Protección de Datos Personales, que actúa como organismo independiente responsable de supervisar la aplicación de la ley. La agencia tiene amplios poderes, incluida la capacidad de

realizar investigaciones, revisar procedimientos y prácticas de manejo de datos y emitir recomendaciones y orientación. Además, tiene la facultad de imponer sanciones por incumplimiento de la ley. Su autonomía administrativa y técnica son cruciales para su labor regulatoria, lo que le permite actuar sin interferencias externas y basándose enteramente en estándares técnicos y legales.

Sanción:

La Ley Orgánica de Protección de Datos Personales de Ecuador establece un sistema de sanciones para violaciones relacionadas con la protección de datos. Las sanciones van desde censuras hasta multas y pueden llegar hasta el 4% de los ingresos brutos anuales globales de la empresa (según el año fiscal anterior a la infracción). En casos graves, además de multas, empresas y particulares pueden enfrentarse a medidas preventivas o incluso al cierre temporal o definitivo de sus actividades. Estas sanciones están diseñadas para ser proporcionales a la naturaleza, gravedad y duración de la infracción, teniendo en cuenta las intenciones y acciones tomadas para mitigar el daño causado.

Derechos de los Titulares de Datos

Los derechos de los titulares de datos bajo la LOPDP incluyen:

- **Derecho a la Información**: Acceder a información sobre el tratamiento de sus datos personales.

- **Derecho de Acceso:** Consultar sus datos personales que se encuentran en poder de las organizaciones.

- **Derecho a la Rectificación**: Solicitar la corrección de datos inexactos o incompletos.

- **Derecho a la Cancelación y Desistimiento**: Solicitar la eliminación de datos personales cuando ya no sean necesarios para el propósito

para el cual fueron recolectados. El derecho de cancelación y desistimiento de un modo y objetivo pueden considerarse como la misma materia. El Diccionario Panespañol de Español Jurídico establece que las personas tienen derecho a detener o terminar el uso o tratamiento de sus datos personales por parte de la entidad, institución o persona que controle sus datos personales. Expulsión o supresión física, en particular con las materias que cada ley considere apropiadas en su marco legal. Pero en general, la supresión de datos personales indica que incluye la protección de datos como un derecho independiente, además de que existe un procedimiento legal o judicial para hacer valer este derecho, el cual está previsto por la protección de datos.

Se justifica la supresión cuando sea absolutamente necesaria para una persona, porque afecta al interesado o titular de los datos personales. Por otro lado, la información sobre cancelación se puede organizar, de modo que se puedan eliminar todos los datos personales o un dato específico. Suponiendo que la persona es responsable o responsable del tratamiento de los datos, y la obligación de proteger, procesar y proteger los datos personales, independientemente del interés individual del titular de los datos bajo autorización pasada.

Acotado a lo anterior, el derecho de cancelación se vuelve relevante ante su finalidad y el efecto que contrae la cancelación, que puede tener varios puntos distintivos en cada legislación.

Primero, desde su enfoque, a nivel latinoamericano este poder ha estado reservado al sector privado, siendo en muchos casos polémico y controversial el criterio de unidad. En segundo lugar, el significado básico, bajo la interpretación simple, de la palabra “suprimir” va allí donde el marco legal considera la supresión de datos en el sentido literal, antes de la sustracción, la supresión, la supresión y la destrucción física y material de los datos. Pero otro marco legal considera que la supresión de datos es nula, inválida o inválida. En los casos en que se determine que se considera inválido o no válido, pero no se elimine físicamente, dichos datos se considerarán eliminados.

Ahora bien, en ambos casos, la finalidad de suprimir los datos es independiente de su eliminación y tratamiento físico o material. Pero al mismo tiempo, es útil distinguir entre rechazo y prevención, por un lado, y rechazo y rechazo, por el otro.

En Ecuador, la ley orgánica de protección de datos personales señala en su artículo 15 el derecho de cancelación, el cual distingue el derecho a cancelar, retirar o eliminar los elementos filtrados. El marco legal nacional se llama que, copiando las leyes españolas que son pioneras en materia de derecho y protección de datos personales, será útil el mismo principio mencionado anteriormente sobre la supresión y adición a la lista de este derecho, afirma. "El derecho a perdonar El titular tiene derecho a retirar sus datos personales del encargado del tratamiento cuando:

1. • La conducta no se ajuste a los principios establecidos en esta Ley.

2. El tratamiento no es necesario o necesario para cumplir la finalidad.

3. • La información personal cumple con el propósito para el cual fue recopilada o procesada.

4. • Ha expirado el plazo de conservación de los datos personales.

5. • Esta práctica afecta a derechos fundamentales y libertades individuales.

6. • Retirar el consentimiento prestado o indicar que no ha sido otorgado para un fin o finalidad particular, sin motivo válido. O,

7. • Un requisito constitucional…" .

• **Derecho de Oposición:** Oponerse al tratamiento de sus datos personales en ciertas circunstancias.

- **Derecho al Olvido:** Solicitar la eliminación de datos personales cuando se haya revocado el consentimiento. La naturaleza jurídica de este derecho proviene del desarrollo, progreso tecnológico del mundo digital y electrónico en el que se produce, almacena y procesa información personal en el verdadero sentido de dato personal. Quienes tienen acceso a Internet en diversas formas de búsqueda, donde la información fluye y se almacena en esta nube digital, pueden no tener parámetros de seguridad o no tener derecho a revelar, no más de lo que la ley establece como más fuerte. violar la privacidad y reputación de una persona. Con la flexibilidad que proporciona la red para romper los filtros de seguridad. El derecho a la privacidad se considera un derecho fundamental de las personas a controlar y decidir qué cantidad de sus datos se divulgan o se ponen a disposición del público. De ahí la importancia del derecho al olvido en este mundo cada vez más globalizado, que requiere un marco regulatorio.

Las nuevas tecnologías son una amplia ventana de progreso y es fácil para las personas desconectarse de un dispositivo esté donde esté, acceder a Internet y tener un mundo de información al alcance de la mano, adquirir nuevos conocimientos, y las dudas se aclaran, se hacen trámites, pero el . Es una manera fácil para que las personas accedan a información personal, uso indebido de la información, divulgación de información personal sin el consentimiento del titular, violación a la privacidad, el honor y el buen nombre (Bernal, 2022).

2.2.3 Reglamento General de la Ley Orgánica de Protección de Datos Personales

El Artículo 5 del Reglamento General de la Ley Orgánica de Protección de Datos Personales (2023) establece la necesidad de obtener el consentimiento expreso e informado del titular para el tratamiento de sus datos, garantizando así la transparencia y el respeto a la privacidad. Además, enfatiza que el consentimiento debe ser inequívoco y no puede presumirse por silencio o inacción. En el contexto del presente trabajo de investigación, este artículo es fundamental porque define los principios clave para la protección de la

información personal en entornos digitales. Su análisis permite comprender los límites legales del uso de tecnologías que procesan datos y la importancia de mecanismos de consentimiento explícito en plataformas digitales, lo que contribuye a un desarrollo normativo que equilibre innovación y derechos fundamentales.

El Artículo 6 del Reglamento instaura el derecho del titular a revocar su consentimiento en cualquier momento, obligando al responsable del tratamiento a suspender el uso de los datos una vez recibida la notificación. Además, garantiza que la revocatoria no afecte la licitud de los tratamientos previos. Para la presente investigación, este artículo es clave para analizar cómo las plataformas digitales deben implementar mecanismos efectivos y accesibles para que los usuarios puedan retirar su consentimiento. Su estudio permite evaluar el cumplimiento de principios de autodeterminación informativa y control sobre los datos en entornos digitales, asegurando la protección de la privacidad en un ecosistema tecnológico en constante evolución.

El Capítulo V de este Reglamento General regula la transferencia y comunicación de datos a terceros, estableciendo que, en principio, se requiere el consentimiento del titular, salvo en casos en los que los datos sean anonimizados o existan razones legítimas para la transferencia (Art. 21 y 22). Además, el Art. 23 garantiza que el titular pueda ejercer sus derechos de rectificación, actualización, oposición y eliminación de sus datos incluso cuando estos han sido transferidos. En el contexto de presente trabajo, este capítulo es permite analizar cómo se gestionan y protegen los datos en un entorno digital interconectado, permite evaluar las obligaciones de las empresas tecnológicas respecto a la privacidad, el uso de técnicas de anonimización y el derecho del usuario a mantener el control sobre su información, aspectos clave en el desarrollo de regulaciones sobre protección de datos en la era digital.

A partir de los artículos y disposiciones del Reglamento General de la Ley Orgánica de Protección de Datos Personales, se observa un enfoque integral hacia la protección de la privacidad y el fortalecimiento del control de los individuos sobre sus datos personales en entornos digitales. El consentimiento

expreso e informado, estipulado en el Artículo 5, establece una base fundamental para garantizar la transparencia y el respeto por los derechos de los titulares, permitiendo que el tratamiento de datos se realice de manera ética y conforme a los principios de autodeterminación informativa. La posibilidad de revocar dicho consentimiento en cualquier momento, contemplada en el Artículo 6, refuerza la autonomía del titular sobre su información personal, asegurando que su privacidad no sea comprometida por decisiones previas. Por otro lado, los artículos 21 y 22, relacionados con la transferencia de datos, demuestran el compromiso del reglamento con la protección de la información, limitando la comunicación de datos a terceros y estableciendo condiciones claras para garantizar la seguridad y los derechos de los titulares.

2.2.4 Código Orgánico Integral Penal

En el artículo 178 del Código Orgánico Integral Penal (COIP, 2014) regula el delito de acceso ilícito a sistemas informáticos. Según este artículo, se considera delito el acceso no autorizado a un sistema informático o la interceptación de datos transmitidos por redes de telecomunicaciones. El artículo 179 del COIP, por su parte, aborda el delito de interceptación de datos informáticos. Este delito se configura cuando una persona intercepta datos informáticos transmitidos por redes de telecomunicaciones, sin la debida autorización, con el fin de obtener información protegida o modificarla.

Ambos artículos son fundamentales para combatir el robo de información personal en línea, ya que ofrecen un marco legal claro para la protección de datos personales y la privacidad de los ciudadanos. Al regular el acceso no autorizado a los sistemas informáticos y la interceptación ilegal de datos, estos artículos refuerzan la seguridad de la información tanto en almacenamiento como en transmisión a través de redes de telecomunicaciones. De esta manera, se busca proteger la integridad y confidencialidad de los datos, además evitar el uso malintencionado de la información personal con fines fraudulentos o delictivos. En este sentido, la aplicación de estas disposiciones legales es relevante en un contexto digital cada vez más vulnerable a ciberataques, donde la protección de la privacidad se ha convertido en un derecho fundamental.

Asimismo, el cumplimiento de estas leyes puede disuadir a potenciales infractores y contribuir a una cultura de respeto por la privacidad y seguridad en línea, promoviendo un entorno digital más seguro y confiable para los usuarios.

2.2.5 Habeas data vs derecho al olvido

Luego de la idea del derecho al olvido, en diferentes leyes, se llega al punto que el derecho al olvido en el marco jurídico del Ecuador no ha sido discutido como tal concepto. Pero en la ley ambiental para la protección de datos personales, considero los derechos básicos que otorgan derechos especiales al derecho a la protección de datos, incluida la privacidad y la dignidad. A pesar de que el programa presentado a los legisladores fue presentado, rechazado y mejorado el argumento, hubo más libertad para participar, defender, oponerse y llevar adelante. Antes de la aprobación de la Ley de Datos Personales, el Habeas Data era el método actual de protección de datos personales, proporcionada por el Tribunal de Justicia como garantía de protección de datos.

El Habeas Data es una garantía legal, cuya finalidad se basa en la protección de datos personales, que asegura su protección y el respeto de los derechos fundamentales en caso de que estos sean vulnerados. Reproducir, reproducir, utilizar de cualquier forma, sin el derecho o permiso del propietario. En este contexto, se crea la Ley de Habeas Data como un mecanismo mediante el cual los individuos tienen el primer derecho de acceso a la información y datos personales en poder de entidades públicas y privadas, pudiendo determinar el uso y finalidad de la información. y su destino (Shevar, 2011; Zamora, 2016).

A pesar de que tanto el Habeas Data como el Derecho al Olvido buscan garantizar la protección de la privacidad y el respeto de los derechos fundamentales, existe una distinción clave en su enfoque y aplicación. El Habeas Data se enfoca principalmente en el acceso, rectificación, actualización y supresión de los datos personales en poder de las entidades, tanto públicas como privadas, y busca asegurar que los datos personales no sean utilizados de manera indebida o sin el consentimiento del titular. En cambio, el Derecho al Olvido, aunque relacionado, se extiende a la eliminación de la información de los

motores de búsqueda o de los registros públicos cuando dicha información ya no es relevante, actual o adecuada para el contexto. En este sentido, el Derecho al Olvido se presenta como un derecho más integral y profundo, ya que implica un cambio en la disponibilidad pública de los datos personales, mientras que el Habeas Data solo regula el tratamiento de los mismos dentro de las entidades o registros.

En resumen, parece que el mejor método de protección de datos es una característica importante, entre las que destaca, una práctica que puede aplicarse a personas físicas y jurídicas sin limitación y de forma gratuita. La Corte Constitucional en sentencia 2064-13-EP. Se hará un análisis en profundidad que se refiere al habeas data correspondiente y es un proceso legal que garantiza los derechos de las personas. (Corte de Justicia del Ecuador, 2021). Pero hay errores en muchos casos, incluyendo castigos que violan la justicia, las personas jurídicas tienen derecho a presentar demandas y, finalmente, la falta de información sobre cuándo las personas pueden registrarse mientras los derechos estén disponibles. Es necesario para el desarrollo, por ejemplo, el derecho al olvido.

Es por esto que el derecho al olvido es hoy una parte importante de la protección de datos personales, porque cuando lo ponderamos, el derecho al olvido es más grave que la acción de habeas data y viceversa. Poniendo fin a la garantía y convirtiéndose en una autoridad independiente. No es un trabajo, sino un derecho permanente.

CAPÍTULO III
MARCO METODOLÓGICO

3.1 Enfoque de la investigación

En la investigación se ha aplicado un enfoque de carácter cuantitativo, se han construido las bases teóricas a partir de las variables de investigación presentadas en la idea a defender del Capítulo 1, la tecnología digital y la privacidad de los datos.

Igualmente se ha aplicado una encuesta escala Likert, dirigida a profesionales del derecho sobre preguntas relacionadas con la problemática de la investigación, sobre la ley y la eficiencia ante los casos de vulneración de derechos a la privacidad de datos personales.

3.2 Alcance de la investigación:

Descriptiva: El alcance de la investigación ha sido descriptivo, se ha descrito las características, fundamentos y elementos tanto de la variable tecnología digital como de la variable privacidad de datos.

Exploratoria: También se ha aplicado un diseño específico dentro del alcance exploratorio como ha sido el estudio de caso, en concreto las Sentencias de la Corte Constitucional: Sentencia No. 59-19-IN/24; Sentencia No. 2064-14-EP/21; Sentencia No.1068-19-JP/25

3.3 Técnica e instrumentos para obtener los datos

En la presente investigación se aplicó la técnica de la encuesta, cuyo instrumento para recoger la obtención de datos fue el cuestionario, por medio de escala de Likert. El cuestionario está compuesto por 12 ítems divididos en tres dimensiones; la primera sobre el Marco legal y regulación, que abarca cuatro preguntas (ítems 1-4); la segunda dimensión refiere a la Aplicación y

cumplimiento, consta de cuatro preguntas (ítems 5-8); y la terca dimensión que engloba los Desafíos en la Protección de Datos a través de cuatro preguntas (ítems 9-12). La escala de Likert fue de cinco puntos según el nivel de acuerdo con las afirmaciones presentadas, donde podía utilizar Totalmente en desacuerdo (1), En desacuerdo (2), Neutral (3), De acuerdo (4) y Totalmente de acuerdo (5).

3.4 Población y muestra

La Población de la investigación son los Abogados del Colegio de Abogados de Guayas, cuyo registro indica que hay 20,189 afiliados. La Muestra ha sido aleatoria intencional no probabilística conformada por 20 abogados.

CAPÍTULO IV
PROPUESTA O INFORME

4.1 Presentación y análisis de resultados

En el presente apartado se presentan los resultados de la investigación, tanto de su fase descriptiva con la tabulación de los resultados y las gráficas respectivas. En esta misma sección se presenta un análisis de los hallazgos en relación con la Ley Orgánica de Protección de Datos Personales y las recomendaciones formuladas para mejorar la protección de la privacidad de los datos.

4.1.1 Resultados descriptivos

Marco legal y regulación

1. La normativa ecuatoriana sobre protección de datos personales es clara para garantizar la privacidad en el entorno digital.

Tabla 1

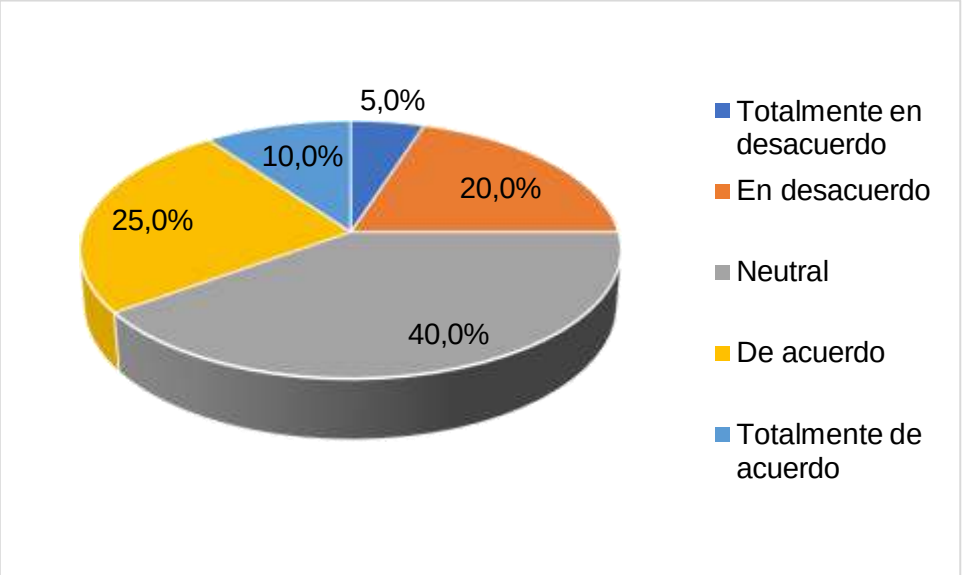
Claridad de la normativa para garantizar la privacidad

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	1	5.0%
En desacuerdo	4	20.0%
Neutral	8	40.0%
De acuerdo	5	25.0%
Totalmente de acuerdo	2	10.0%
Total	**20**	**100.0%**

Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Figura 1

Claridad de la normativa para garantizar la privacidad



Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

De acuerdo con la figura 1, el 40% de los encuestados se mantuvo en una posición neutral, debido a que no tienen certeza sobre si la normativa es clara en la garantía de la privacidad. Adicionalmente, un 35% consideró que la normativa no es clara en absoluto, al estar en desacuerdo o totalmente en desacuerdo. Los resultados muestran que existe una percepción de incertidumbre sobre la claridad de la normativa ecuatoriana de protección de datos personales, por lo cual, podría no estar cumpliendo su función de garantizar la privacidad en el entorno digital de manera efectiva.

2. La Ley Orgánica de Protección de Datos Personales en Ecuador se encuentra alineada con estándares internacionales de protección de datos.

Tabla 2

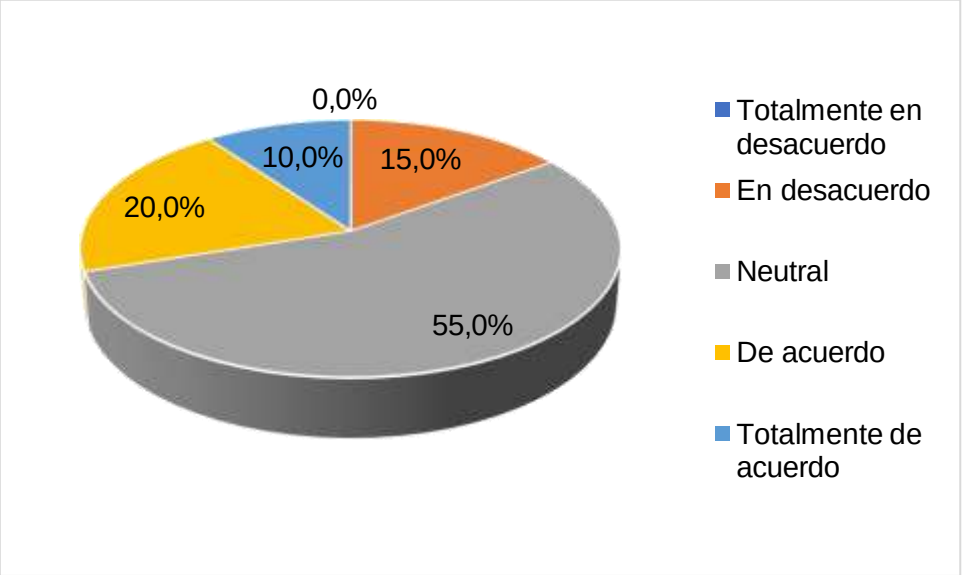
Alineación de la LOPD con estándares internacionales

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	0	0.0%
En desacuerdo	3	15.0%
Neutral	11	55.0%
De acuerdo	4	20.0%
Totalmente de acuerdo	2	10.0%
Total	**20**	**100.0%**

Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Figura 2

Alineación de la LOPD con estándares internacionales



Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

La figura 2 ilustra que el 55% de los encuestados mantiene en una postura neutral por la falta de conocimiento o claridad sobre el tema. Sin embargo, un 15% considera que la normativa no está alineada con los estándares internacionales, por ende, existe preocupación en este aspecto. En ese sentido, la alta proporción de respuestas neutras demuestra que el nivel de confianza en la adecuación de la normativa es bajo.

3. Las instituciones encargadas de hacer cumplir la normativa de privacidad de datos en Ecuador actúan con eficiencia y rigor.

Tabla 3

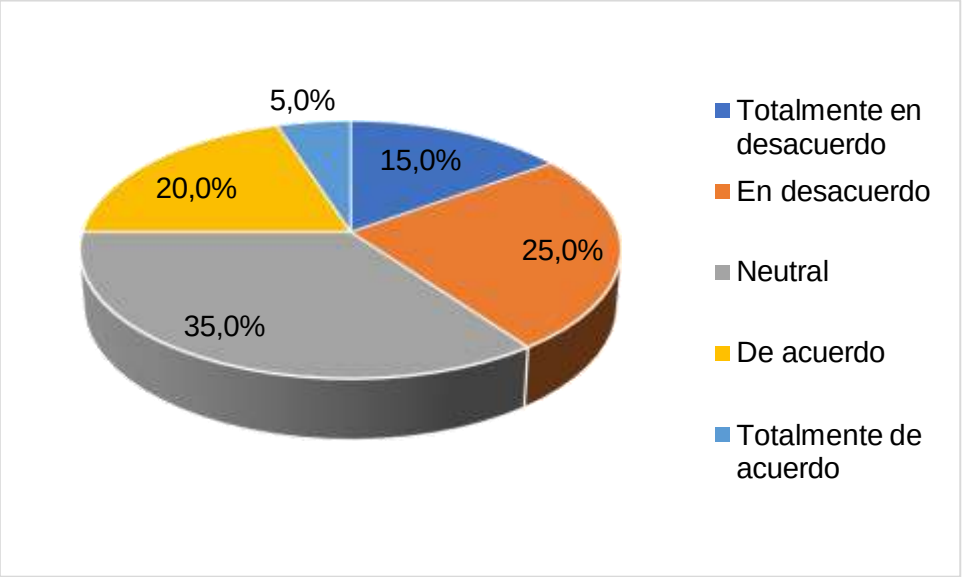
Eficiencia y rigor de las instituciones encargadas

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	3	15.0%
En desacuerdo	5	25.0%
Neutral	7	35.0%
De acuerdo	4	20.0%
Totalmente de acuerdo	1	5.0%
Total	**20**	**100.0%**

Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Figura 3

Eficiencia y rigor de las instituciones encargadas



Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

En la figura 3 se aprecia que los encuestados manifestaron estar 15% en desacuerdo y 25% totalmente en desacuerdo respecto a la eficiencia y el rigor de las autoridades de protección de datos, situación que indica una falta de confianza en la gestión de estas instituciones. Por otra parte, el 35% se mantuvo en una posición neutral, lo cual apunta a la incertidumbre o desconocimiento sobre su desempeño. Los resultados evidencian una percepción de deficiencia para hacer cumplir la normativa de privacidad de datos en Ecuador.

4. La regulación actual se adapta adecuadamente a los avances tecnológicos y a las nuevas amenazas a la privacidad digital.

Tabla 4

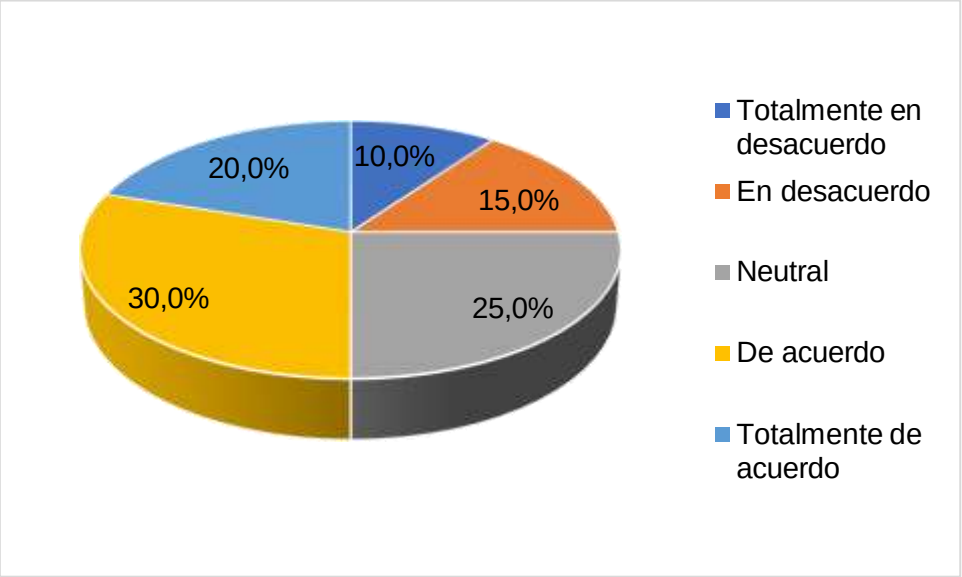
Adaptación de la regulación a nuevas amenazas a la privacidad digital

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	2	10.0%
En desacuerdo	3	15.0%
Neutral	5	25.0%
De acuerdo	6	30.0%
Totalmente de acuerdo	4	20.0%
Total	**20**	**100.0%**

Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Figura 4

Adaptación de la regulación a nuevas amenazas a la privacidad digital



Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

En la figura 4 se puede observar que un 25% optó por ser neutral denotando su incertidumbre sobre la efectividad de la normativa en la protección de datos. En cambio, el 15% señaló desacuerdo y el 10% total desacuerdo, es decir, un sector de los abogados considera que la regulación no responde adecuadamente a los desafíos tecnológicos emergentes, y esa presencia de dudas y desacuerdos señala que el tema sigue siendo motivo de preocupación.

Aplicación y cumplimiento

5. Las empresas y entidades públicas en Ecuador cumplen con las regulaciones de protección de datos personales de manera efectiva.

Tabla 5

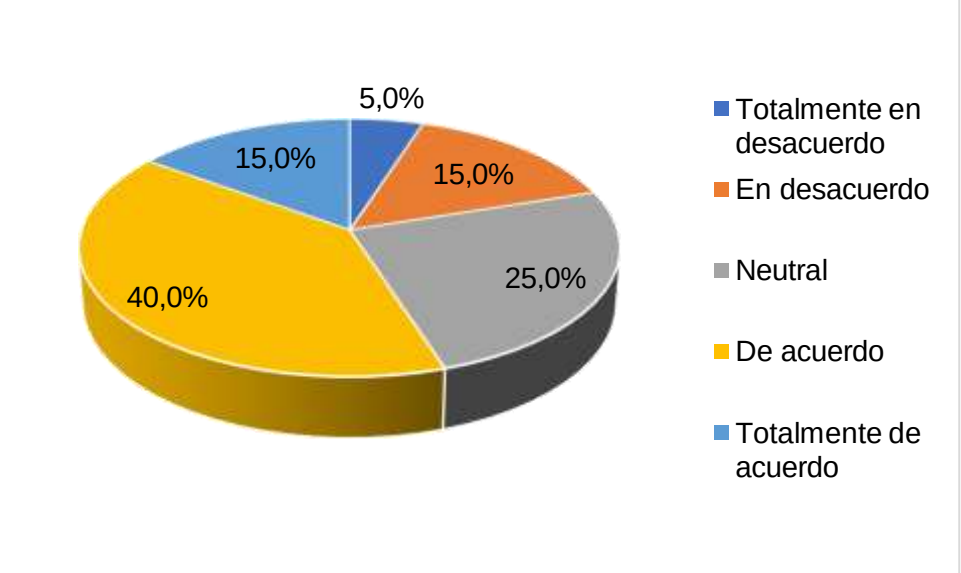
Cumplimiento de regulaciones de protección de datos

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	1	5.0%
En desacuerdo	3	15.0%
Neutral	5	25.0%
De acuerdo	8	40.0%
Totalmente de acuerdo	3	15.0%
Total	**20**	**100.0%**

Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Figura 5

Cumplimiento de regulaciones de protección de datos



Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Los resultados de la figura 5 exponen que el 40% está de acuerdo y considera que las empresas y entidades públicas cumplen con las regulaciones de protección de datos personales. Sin embargo, el 25% demuestra que todavía hay indicios de duda y escepticismo al mantener una postura neutral. Este

resultado señala que existe una percepción de incumplimiento o debilidades en la aplicación de las regulaciones por las empresas.

6. Existen mecanismos adecuados para denunciar vulneraciones a la privacidad de los datos en Ecuador.

Tabla 6

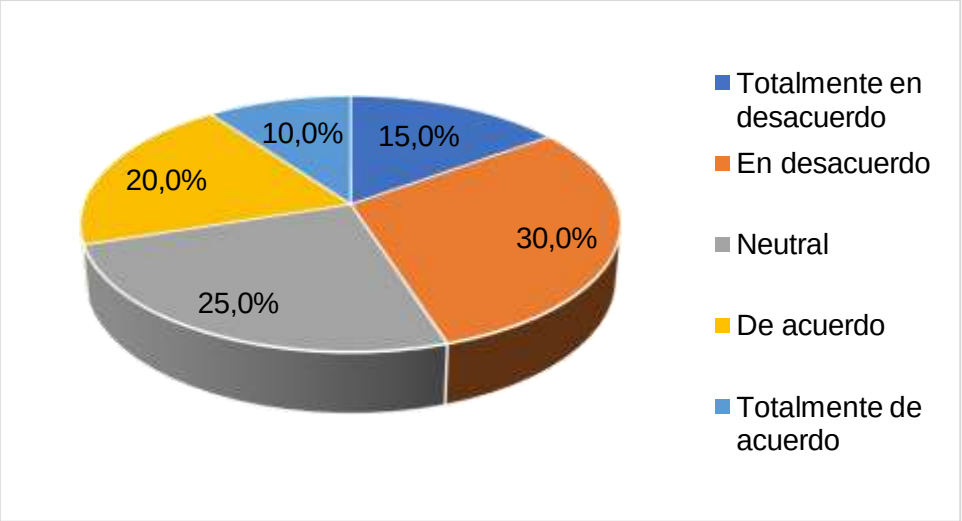
Mecanismos para denunciar vulneraciones

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	3	15.0%
En desacuerdo	6	30.0%
Neutral	5	25.0%
De acuerdo	4	20.0%
Totalmente de acuerdo	2	10.0%
Total	**20**	**100.0%**

Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Figura 6

Mecanismos para denunciar vulneraciones



Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Los resultados de la figura 6 muestran una percepción de insuficiencia en los mecanismos para denunciar vulneraciones a la privacidad de los datos en Ecuador, dado que el 30% de los encuestados está en desacuerdo y el 15% totalmente en desacuerdo con la afirmación. Esto denota falta de confianza en la accesibilidad o efectividad de estos mecanismos. Además, un 25% se

mantiene en una postura neutral, sinónimo de incertidumbre del funcionamiento y refleja preocupación sobre la capacidad del sistema para garantizar una protección efectiva de los datos personales.

7. Las sanciones establecidas por la normativa ecuatoriana son efectivas para prevenir vulneraciones a la privacidad de los datos

Tabla 7

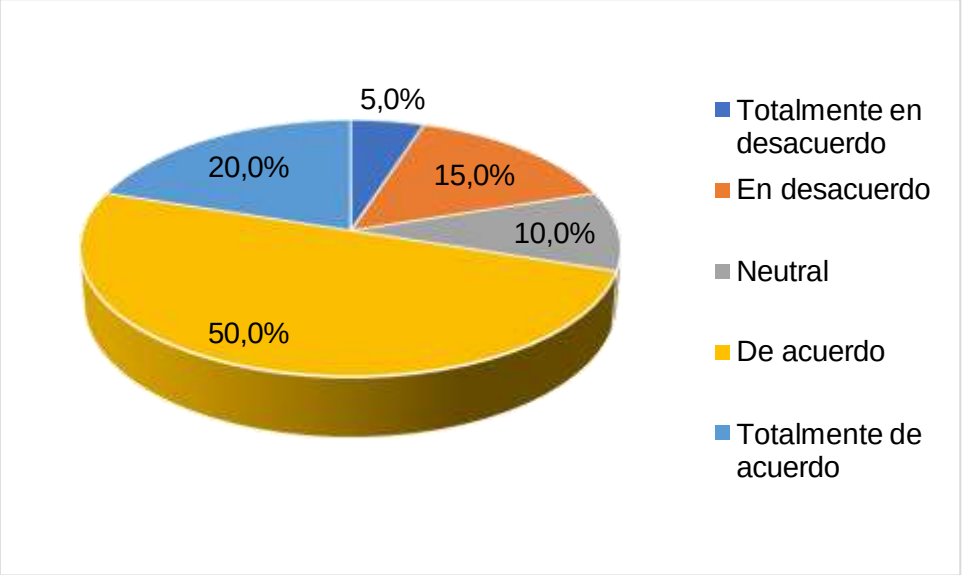
Efectividad de las sanciones para prevenir vulneraciones

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	1	5.0%
En desacuerdo	3	15.0%
Neutral	2	10.0%
De acuerdo	10	50.0%
Totalmente de acuerdo	4	20.0%
Total	**20**	**100.0%**

Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Figura 7

Efectividad de las sanciones para prevenir vulneraciones



Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Los resultados de la figura 7 señalan que el 50% de los participantes considera que las sanciones establecidas por la normativa ecuatoriana son efectivas para prevenir vulneraciones a la privacidad de los datos. No obstante,

persisten preocupaciones sobre su aplicación o impacto real, dado que el 15% no percibe que sean efectivas y el 10% se mantiene en una postura neutral, que denota incertidumbre o falta de información sobre la eficacia de estas medidas.

8. La ciudadanía ecuatoriana está suficientemente informada sobre sus derechos en cuanto a la protección de datos personales.

Tabla 8

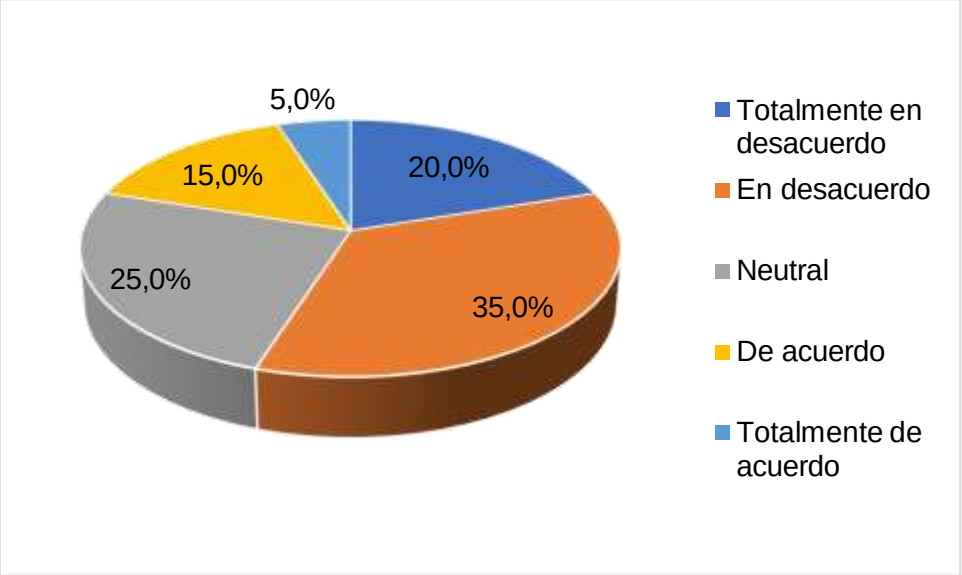
Información de la ciudadanía sobre derechos de protección de datos

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	4	20.0%
En desacuerdo	7	35.0%
Neutral	5	25.0%
De acuerdo	3	15.0%
Totalmente de acuerdo	1	5.0%
Total	**20**	**100.0%**

Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Figura 8

Información de la ciudadanía sobre derechos de protección de datos



Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

La figura 8 muestra que los participantes creen que la ciudadanía no está informada sobre sus derechos de protección de datos, dado que un 35% estuvo en desacuerdo y un 20% totalmente en desacuerdo; es decir, existe una

percepción generalizada de desinformación en la población. Al mismo tiempo, un 25% expresó estar neutral, demostrando indecisión respecto al grado de conocimiento ciudadano en este tema, situación que reafirma una brecha en la concienciación y educación referente a la protección de datos personales.

Desafíos en la Protección de Datos

9. La cooperación internacional es clave para fortalecer la protección de datos personales en el país.

Tabla 9

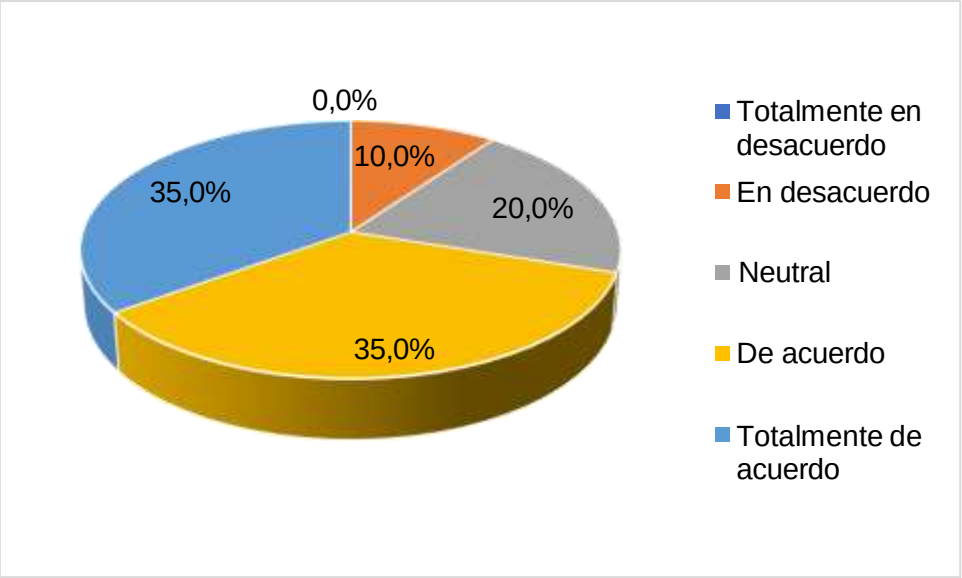
Cooperación internacional para fortalecer la protección de datos

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	0	0.0%
En desacuerdo	2	10.0%
Neutral	4	20.0%
De acuerdo	7	35.0%
Totalmente de acuerdo	7	35.0%
Total	**20**	**100.0%**

Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Figura 9

Cooperación internacional para fortalecer la protección de datos



Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Según la figura 9, el 70% entre de acuerdo y totalmente de acuerdo demuestran que los abogados reconocen la importancia de la cooperación internacional para fortalecer la protección de datos personales en el país. Aun así, el 10% de los participantes está en desacuerdo y no percibe la cooperación internacional como un factor esencial en esta materia.

10. Existen deficiencias en la infraestructura tecnológica y jurídica que afectan la efectiva aplicación de las leyes de protección de datos.

Tabla 10

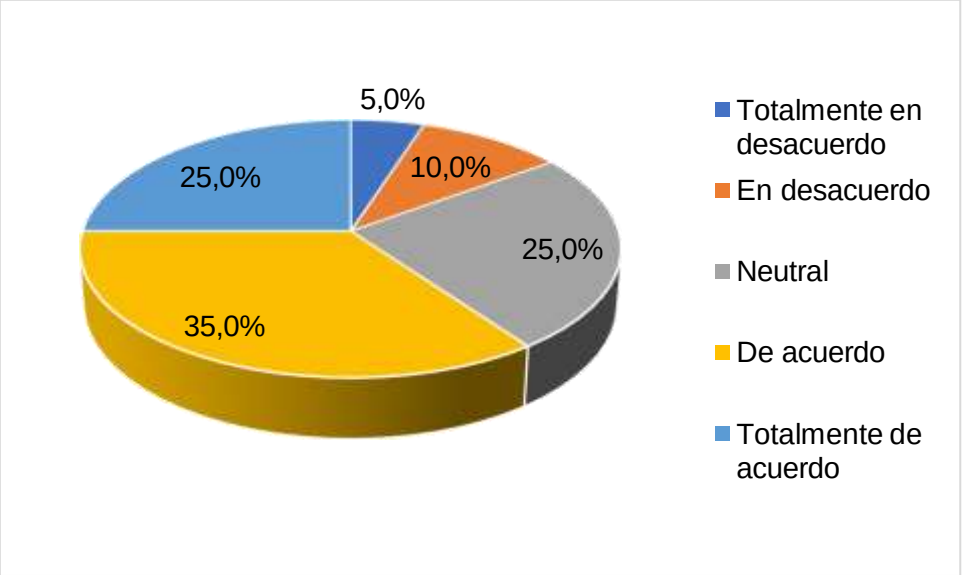
Deficiencias en la infraestructura tecnológica y jurídica

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	1	5.0%
En desacuerdo	2	10.0%
Neutral	5	25.0%
De acuerdo	7	35.0%
Totalmente de acuerdo	5	25.0%
Total	**20**	**100.0%**

Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Figura 10

Deficiencias en la infraestructura tecnológica y jurídica



Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Los datos ilustrados en la figura 10 ilustran que el 60% está de acuerdo o totalmente de acuerdo en que la infraestructura tecnológica y jurídica, por tanto, representan un obstáculo en la implementación de la normativa de protección de datos. Igualmente, un 25% se optó por una postura neutral, que exterioriza la falta de certeza o información sobre el impacto de estas deficiencias, y refuerza la existencia de problemas estructurales en este ámbito.

11. Es necesario un mayor esfuerzo en la capacitación de jueces, fiscales y abogados en materia de protección de datos personales.

Tabla 11

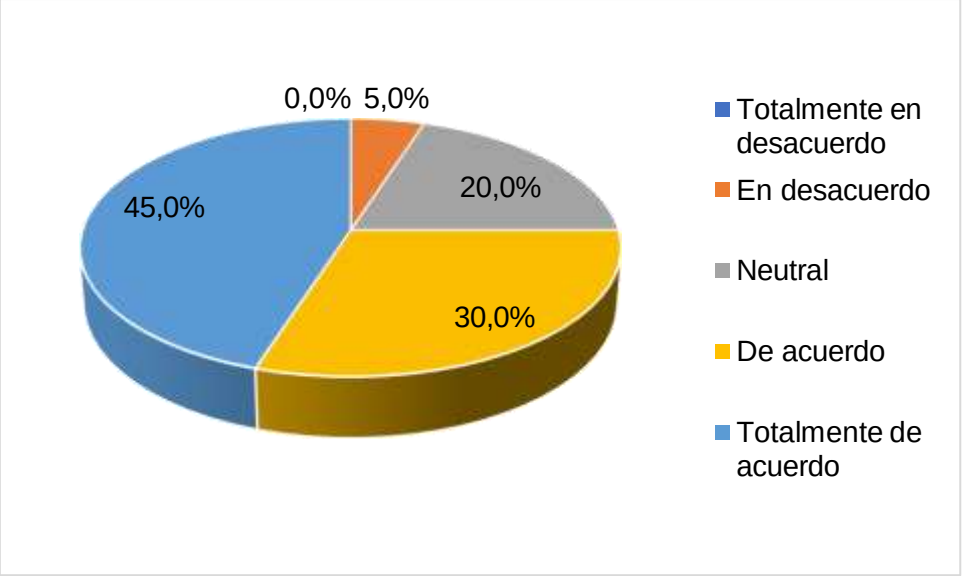
Necesidad de capacitación en materia de protección de datos

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	0	0.0%
En desacuerdo	1	5.0%
Neutral	4	20.0%
De acuerdo	6	30.0%
Totalmente de acuerdo	9	45.0%
Total	**20**	**100.0%**

Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Figura 11

Necesidad de capacitación en materia de protección de datos



Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

En la figura 11 se demuestra que se debe fortalecer la capacitación sobre protección de datos personales para jueces, fiscales y abogados, debido al 45% de encuestados totalmente de acuerdo y 30% de acuerdo; además, un 20% se mantiene en una posición neutral. Estos resultados señalan que actualmente la formación en este ámbito es considerada insuficiente y requiere mayor atención en el sistema jurídico.

12. Considera que el marco legal actual en Ecuador ofrece suficientes garantías para proteger la privacidad de los datos personales frente a entidades extranjeras.

Tabla 12

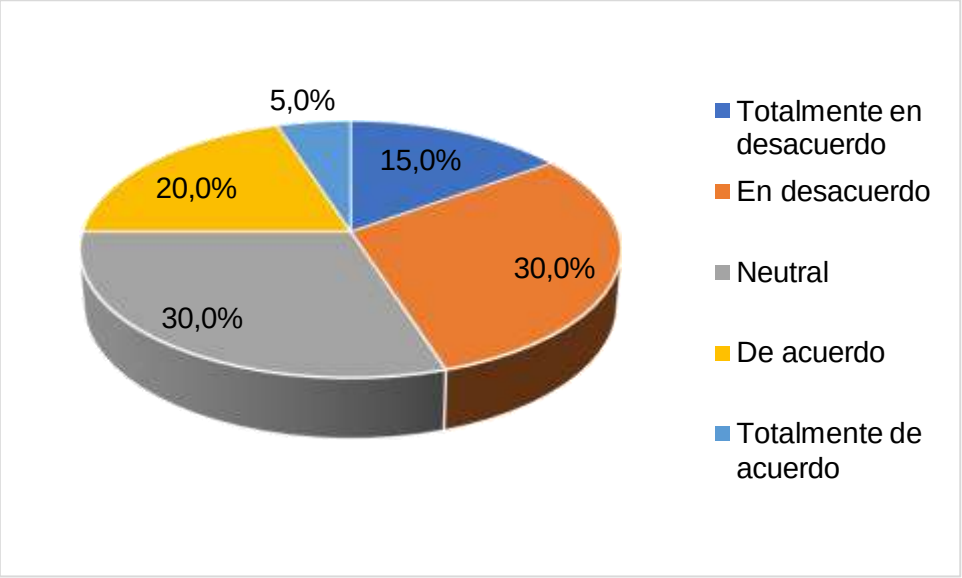
Garantías para proteger la privacidad frente a entidades extranjeras

Descripción	Frecuencia	Porcentaje
Totalmente en desacuerdo	3	15.0%
En desacuerdo	6	30.0%
Neutral	6	30.0%
De acuerdo	4	20.0%
Totalmente de acuerdo	1	5.0%
Total	**20**	**100.0%**

Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Figura 12

Garantías para proteger la privacidad frente a entidades extranjeras



Fuente: Encuesta a abogados del Colegio de Abogados de Guayas.
Elaborado por: Farfán y Cornejo (2025)

Los datos de la figura 12 exponen falta de confianza en la capacidad del marco legal ecuatoriano, ya que un 45% de los encuestados está en desacuerdo o totalmente en desacuerdo en que puedan proteger la privacidad de los datos personales frente a entidades extranjeras. En adición, el 30% tomó una postura neutral, que indica indecisión sobre la efectividad de las garantías legales existentes, y evidencia una percepción de vulnerabilidad en la protección de datos frente a actores internacionales.

4.1.2 Análisis general de los resultados

La era digital en al que se envuelve el mundo en la actualidad constituye un momento convergente para asegurar tanto el acceso global a la información y tecnología digital, así como la protección de datos personales, garantizando la privacidad de los ciudadanos frente a amenazas derivadas del uso inadecuado de la información personal. En Ecuador, la Ley Orgánica de Protección de Datos Personales y su Reglamento General, además de los derechos reconocidos por la Constitución de 2008, constituyen el marco normativo que regula esta materia. Sin embargo, la aplicación efectiva de estas disposiciones es objeto de evaluación crítica, considerando que la ley se promulgó en 2021 y el reglamento se expidió años más tarde en 2023.

Como punto inicial, los resultados de la investigación reflejan percepciones mixtas respecto a la claridad de la normativa ecuatoriana, mayoritariamente con profesionales del derecho en una postura neutral, que consideró que la normativa no es lo suficientemente clara en garantizar la privacidad en el entorno digital, por ende, existe un problema de interpretación o aplicación efectiva, que puede derivar en falta de seguridad jurídica para los ciudadanos y las empresas.

Uno de los objetivos de la LOPDP es armonizarse con estándares globales, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea; no obstante, los profesionales del derecho consultados manifiestan incertidumbre al respecto, considerando que la normativa no está

alineada con estos estándares. Esto refleja la necesidad de mejorar la divulgación de la normativa y explicación de los fundamentos o bases que permitieron su elaboración, dado que, según Morales et al. (2024) la LOPDP está influenciada por GDPR de la Unión Europea al establecer principios para garantizar un tratamiento seguro de la información personal. En consonancia, Razza (2023) señaló que esta ley adoptó principios fundamentales como el consentimiento, la finalidad, la seguridad y la confidencialidad que acogía el instrumento europeo.

En otro orden de ideas, los hallazgos de la presente investigación exponen que las instituciones encargadas de hacer cumplir la normativa no actúan con eficiencia y rigor, situación que presenta una percepción de debilidad institucional que podría afectar la confianza en la aplicación efectiva de la ley. Cabe destacar que, sin mecanismos de supervisión sólidos, el cumplimiento normativo podría verse comprometido. Estos resultados concuerdan con las conclusiones de Arellano (2020) quien afirma que la existencia de una ley no implica seguridad debido a la desconfianza de su aplicación desde el sector público debido a las amenazas informáticas, puesto que los intereses económicos favorecen la intromisión en la privacidad. Por ello, señala que se deben desarrollar propuestas para mejorar su aplicación en el sector público.

Por otro lado, los encuestados consideran que las empresas y entidades cumplen con las regulaciones de protección de datos, se indicó que los mecanismos de denuncia de vulneraciones no son efectivos, lo cual podría desalentar a los ciudadanos a ejercer sus derechos en caso de afectaciones. Esto se puede deber a que, la LOPD establece como mecanismo de denuncia un reclamo ante la Autoridad de Protección de Datos Personales; hasta el momento existen dos mecanismos para presentar una denuncia o solicitud. La primera es de forma escrita ante la Superintendencia de Protección de Datos Personales en sus ventanillas habilitadas. El segundo mecanismo es a través del sitio web de la Superintendencia, para lo cual, la ciudadanía debe descargar el formulario y enviarlo al correo electrónico (Superintendencia de Protección de Datos Personales, 2025).

En cuanto a sanciones, se consideró que las que están establecidas en la normativa son efectivas, existe desacuerdo, incluso una postura neutral, que sugiere que si bien las sanciones existen y pueden tener un impacto disuasorio, su aplicación efectiva podría requerir mejoras en la fiscalización y el proceso sancionador. En este sentido, la LOPDP establece multas y otras medidas correctivas dependiendo de la gravedad de la infracción. Entre ellas, una infracción leve sanciona con 1 a 10 salarios básicos unificados para funcionarios públicos, mientras que para las entidades privadas y empresas públicas pagarían una multa del 0.1% al 0.7% del volumen de negocio del ejercicio económico anterior. Cabe señalar que estas sanciones se aplican sin perjuicio de la responsabilidad civil o penal que pueda derivarse del incumplimiento de la normativa.

4.2 Propuesta

4.2.1 Título de la propuesta

Recomendaciones para el fortalecimiento de la protección de la privacidad de los datos en Ecuador.

4.2.2 Objetivos

Objetivo general

Establecer recomendaciones para mejorar la protección de la privacidad de los datos en Ecuador.

Objetivos específicos

1. Formular recomendaciones para la protección de la privacidad de los datos en Ecuador.

2. Elaborar recomendaciones para la mejora de los mecanismos de denuncia y sanción.

3. Formular recomendaciones para la educación y sensibilización ciudadana.

4. Elaborar recomendaciones para la adaptabilidad de la Normativa a los avances tecnológicos.

4.2.3 Justificación

La justificación de esta propuesta yace en los resultados de la investigación, los mismo que describen deficiencias en la claridad de la normativa, la supervisión institucional y la concienciación ciudadana sobre la protección de datos personales. Esta propuesta toma importancia en la actualidad debido a que la Ley Orgánica de Protección de Datos Personales y el Reglamento a Ley Orgánica de Protección de Datos Personales don de reciente publicación, por lo cual, las estrategias que se tomen para reforzar la divulgación, conocimiento, sensibilización, y aprehensión permitirán que su alcance e implementación sea efectivo, garantizando así una mayor protección de los datos personales. En ese sentido, la implementación de estas recomendaciones ayudará a la mejora del marco regulatorio y a su efectiva aplicación, promoviendo un ecosistema digital más seguro y confiable.

Además, el fortalecimiento de la protección de la privacidad de los datos en Ecuador mejora la seguridad digital, y también fomenta la confianza de los ciudadanos en las plataformas y servicios digitales. Esta confianza es fundamental para el desarrollo de la economía digital, ya que incentiva la participación de las personas en entornos online, promoviendo el comercio electrónico, la innovación tecnológica y la transformación digital en diversos sectores. Asimismo, al garantizar que las instituciones públicas y privadas respeten los derechos fundamentales de los ciudadanos, se contribuye a la construcción de una sociedad más equitativa y justa, en la que la protección de la privacidad sea un derecho protegido y respetado.

4.2.4 Beneficiarios

Los beneficiarios, una vez implementadas las recomendaciones propuestas, serán los ciudadanos ecuatorianos, quienes verán fortalecidos sus derechos a la privacidad y protección de datos personales. Además, se beneficiarán las empresas y entidades públicas, al contar con directrices claras y mecanismos eficientes para el cumplimiento normativo.

Asimismo, se considera como beneficiarios a los operadores jurídicos, incluyendo jueces, fiscales y abogados, ya que mediante capacitaciones pueden mejorar su desempeño en la aplicación de la normativa. En última instancia, la Autoridad de Protección de Datos Personales se beneficiará debido al fortalecimiento de su capacidad de supervisión y sanción.

4.2.5 Desarrollo de la propuesta

En la presente sección, se establecen y formulas las recomendaciones para mejorar la protección de la privacidad de los datos en Ecuador. La tabla 13 presenta las sugerencias elaboradas por los autores de esta investigación para garantizar la efectiva aplicación de la normativa de protección de datos, a través del fortalecimiento de la supervisión y fiscalización.

Tabla 13

Recomendaciones para el reforzamiento de la supervisión y cumplimiento normativo

Recomendación	¿Cómo se implementa?	¿Cuándo aplicarla?	Recursos necesarios
Dotar a la Autoridad de Protección de Datos Personales de mayores recursos financieros y tecnológicos	A través de una reforma presupuestaria o asignación específica en el Presupuesto General del Estado. Incorporar software especializado para auditorías y monitoreo de cumplimiento.	A corto plazo, con la actualización anual del presupuesto estatal.	Financiamiento estatal, adquisición de software de seguridad, capacitación de personal técnico.

Crear un sistema de certificación obligatoria para empresas que manejen datos personales	Desarrollo de un esquema de certificación similar al ISO 27001, con requisitos de cumplimiento claros y sanciones para quienes no certifiquen.	Aplicación progresiva en un período de 2 años, iniciando con grandes empresas y extendiéndose a PYMES.	Regulación específica, alianzas con organismos certificadores, capacitación empresarial en cumplimiento normativo.

Elaborado por: Farfán y Cornejo (2025)

La tabla 14 recoge las recomendaciones de que buscan digitalizar y agilizar las denuncias, establecer plazos de respuesta claros y asegurar que las sanciones sean efectivas y disuasorias.

Tabla 14

Recomendaciones para la mejora de los mecanismos de denuncia y sanción

Recomendación	¿Cómo se implementa?	¿Cuándo aplicarla?	Recursos necesarios
Implementar una opción de seguimiento de los procedimientos de denuncia de vulneraciones a la privacidad de datos en el sitio web de la Superintendencia.	En el portal web se deben agregar opciones de seguimiento de las denuncias según el número de trámite, así como una opción de asistencia legal. Esta recomendación se debe coordinar con la Autoridad de Protección de Datos Personales.	A corto plazo, en un período de 6 meses a 1 año, priorizando una fase piloto con mejoras progresivas.	Equipo de desarrollo web, infraestructura tecnológica, presupuesto para soporte técnico y campañas de difusión.
Establecer plazos máximos de respuesta.	Modificación de la normativa para incluir plazos claros (por ejemplo, 30 días hábiles para la resolución de una denuncia). Complementación con la opción seguimiento digital con alertas automatizadas.	Aplicación inmediata tras la reforma normativa, con evaluación periódica de cumplimiento.	Marco legal actualizado, capacitación del personal administrativo, herramientas de gestión de casos.
Asegurar que las sanciones sean proporcionales al daño causado y se	Creación de un sistema de cobro automatizado para multas y sanciones. Implementación de	Aplicación en un plazo de 1 año con revisión anual	Análisis jurídico, sistemas de cobro digital, capacitación de jueces y

hagan efectivas con rapidez	mecanismos de apelación claros.	de su efectividad.	funcionarios en protección de datos.

Elaborado por: Farfán y Cornejo (2025)

En la tabla 15 se puede observar las recomendaciones de educación y sensibilización ciudadana, partiendo de la premisa que la protección de datos personales no puede ser efectiva sin un conocimiento adecuado por parte de la ciudadanía. Estas acciones están dirigidas a crear campañas de concienciación, integrar la educación sobre privacidad en los programas escolares y desarrollar plataformas con recursos accesibles para la población.

Tabla 15

Recomendaciones para educación y sensibilización ciudadana

Recomendación	¿Cómo se implementa?	¿Cuándo aplicarla?	Recursos necesarios
Desarrollar campañas de información masiva sobre el derecho a la privacidad y los riesgos de la exposición de datos personales.	Uso de redes sociales, medios de comunicación, charlas en comunidades y material audiovisual para educar a la población. Se debe trabajar con organismos estatales y privados.	A corto plazo, con campañas iniciales dentro de los primeros 6 meses y evaluación de impacto anual.	Presupuesto estatal y privado, agencias de comunicación, materiales digitales e impresos, alianzas con influencers y medios.
Introducir contenidos sobre privacidad digital y derechos de protección de datos en los programas de educación básica, media y superior.	Reformar los planes de estudio con el Ministerio de Educación y universidades. Capacitación a docentes en temas de privacidad y seguridad digital.	A mediano plazo, con implementación gradual en 1 a 2 años.	Desarrollo de material educativo, formación docente, coordinación con instituciones educativas.
Crear plataformas en línea con recursos educativos accesibles sobre buenas prácticas en privacidad digital	Desarrollo de una plataforma web gestionada por la Autoridad de Protección de Datos, con recursos descargables y tutoriales. Integración con	A corto plazo, con lanzamiento en 6 meses y actualización continua.	Equipo de desarrollo web, diseñadores de contenido, presupuesto para mantenimiento y actualización periódica.

	redes sociales y otras instituciones.

Elaborado por: Farfán y Cornejo (2025)

En la tabla 16 se presentan las recomendaciones para la adaptabilidad de la normativa a los avances tecnológicos, un aspecto pertinente dado el constante y acelerado desarrollo de nuevas tecnologías. La normativa de protección de datos debe estar en constante evolución para responder de manera eficaz a las nuevas realidades y dificultades que surgen con las tecnologías emergentes. En particular, tecnologías como la inteligencia artificial y el Big Data representan una amenaza y, a su vez, una oportunidad para la protección de la privacidad, por lo que es necesario que las leyes y regulaciones se adapten rápidamente a estas tendencias. La falta de actualización de la normativa frente a estos avances puede crear vacíos legales que permitan el uso indebido de los datos personales, lo que hace aún más urgente la necesidad de revisar y actualizar los marcos regulatorios. Esta adaptabilidad permitirá proteger mejor los datos personales, y fomentar la innovación tecnológica en un entorno seguro y confiable para los ciudadanos.

Tabla 16

Recomendaciones para la adaptabilidad de la normativa a los avances tecnológicos

Recomendación	¿Cómo se implementa?	¿Cuándo aplicarla?	Recursos necesarios
Implementar estándares de seguridad obligatorios para el almacenamiento y tratamiento de datos en plataformas digitales. Pueden ser cifrado de datos, autenticación multifactor y auditorías de seguridad.	Desarrollo de normativas que regulen las medidas de seguridad en el almacenamiento y procesamiento de datos. Creación de certificaciones obligatorias para proveedores tecnológicos.	Aplicación gradual en un período de 1 a 2 años, iniciando con sectores críticos como el financiero y de salud.	Normativa actualizada, capacitación empresarial, auditorías de cumplimiento y herramientas de certificación.
Fomentar el uso de técnicas avanzadas para proteger la identidad y privacidad de los ciudadanos en entornos digitales.	Incentivos fiscales y certificaciones para empresas que implementen cifrado robusto y anonimización de datos sensibles.	A mediano plazo, en un período de 2 años, con campañas de adopción y	Apoyo gubernamental, colaboración con empresas tecnológicas, formación de

	Creación de guías y normativas sobre su uso adecuado.	supervisión de cumplimiento.	especialistas en seguridad digital.
Regular el uso de la inteligencia artificial en el tratamiento de datos personales y establecer principios y normas para el uso responsable.	Desarrollo de una normativa específica sobre IA y privacidad. Creación de protocolos de supervisión para verificar el uso ético de la IA en entidades públicas y privadas.	A mediano plazo, con aplicación progresiva en los próximos 2 a 3 años, iniciando con sectores estratégicos como banca, salud y gobierno.	Regulación específica, auditorías tecnológicas, capacitación en ética de IA, certificaciones de cumplimiento para desarrolladores de IA.

Elaborado por: Farfán y Cornejo (2025)

CONCLUSIONES

El análisis del marco legal ecuatoriano en materia de tecnología y privacidad de datos permitió identificar que la Ley Orgánica de Protección de Datos Personales y su reglamento establecen principios sólidos, aunque existen desafíos en su aplicación y cumplimiento. No obstante, estos cuerpos legales cumplen con establecer el objeto de la ley, su ámbito de aplicación, sanciones y mecanismos para ejercer el derecho a la protección de datos.

La evaluación de la situación actual evidenció que las instituciones encargadas de la protección de datos personales requieren mayores recursos y estrategias efectivas de fiscalización. Además, se identificó una brecha en el conocimiento de la ciudadanía sobre sus derechos, lo que limita el ejercicio pleno de la normativa vigente. Asimismo, la adaptabilidad del marco legal frente a las nuevas amenazas tecnológicas, especialmente en el uso de inteligencia artificial y almacenamiento digital, debe ser una prioridad.

En respuesta a estos hallazgos, se propusieron recomendaciones enfocadas en fortalecer la supervisión, optimizar los mecanismos de denuncia y sanción, promover la educación sobre privacidad digital y actualizar la normativa conforme a los avances tecnológicos. La implementación de estas medidas garantizará una protección más efectiva de los datos personales en Ecuador y favorecerá la consolidación de un entorno digital seguro y confiable para la sociedad.

RECOMENDACIONES

En función de las recomendaciones, se expresa que es necesario establecer auditorías periódicas en el sector público y privado para asegurar la correcta aplicación de los estándares de privacidad y seguridad de datos.

Asimismo, se sugiere la creación de un comité de evaluación y actualización de la normativa, conformado por expertos en derecho digital y ciberseguridad, que garantice la alineación de la legislación ecuatoriana con estándares internacionales y su adecuación a los avances tecnológicos, incluyendo el uso de inteligencia artificial y almacenamiento en la nube en el tratamiento de datos personales.

Por otro lado, se considera fundamental implementar un programa nacional de formación en protección de datos personales, dirigido tanto a la ciudadanía como a jueces, fiscales y operadores jurídicos, promoviendo así una cultura de protección de datos en la institución jurídica nacional.

REFERENCIAS BIBLIOGRÁFICAS

Abanlex. (2022). *Guía del Reglamento General de Protección de Datos*. https://compliance360.pe/wp-content/uploads/2022/05/Guia_sobre_el_reglamento_general_de_proteccion_de_datos_GDPR-1.pdf

Acurio, A., & Romero, A. (2024). Divulgación de información personal con efectos nocivos a la intimidad. *Polo del Conocimiento*, *9*(12), 23-49. https://doi.org/10.23857/pc.v9i12.8450

Albornoz, M. M. (2021). El titular de datos personales, parte débil en tiempos de auge de la Inteligencia Artificial. ¿Cómo fortalecer su posición? *REVISTA IUS*, *15*(48), Article 48. https://doi.org/10.35487/rius.v15i48.2021.715

Arellano, C. A. (2020). El derecho de protección de datos personales. *Biolex*, *12*(23), 163-174. https://doi.org/10.36796/biolex.v0i23.194

Arriola, C. R. (2024). La ética en la era digital. *Revista Científica Internacional*, *7*(1), 135-153. https://doi.org/10.46734/revcientifica.v7i1.81

Australian Government. (2025). *The Privacy Act*. https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act

Autoridad Nacional de Protección de Datos de Singapur. (2022). *Guía básica de anonimización*. https://www.aepd.es/documento/guia-basica-anonimizacion.pdf

Ávila, E. (2023). La gobernanza de los datos de investigación en el contexto de su organización y sistematización. *Investigación bibliotecológica*, *37*(96). https://doi.org/10.22201/iibi.24488321xe.2023.96.58763

Barahona, F., & Mayorga, E. (2024). La regulación del derecho a la privacidad en la era de la tecnología y la digitalización en Ecuador. *593 Digital Publisher CEIT*, *9*(Extra 3-1), 19-30.

Barahona-Martinez, G. E., Barzola, Y. G., & Peñafiel, L. V. (2024). El Derecho a la Protección de Datos y el Avance de las Nuevas Tecnologías en Ecuador: Implicaciones Legales y Éticas. *Journal of Economic and Social Science Research*, *4*(3), Article 3. https://doi.org/10.55813/gaea/jessr/v4/n3/113

Basile, D., Ciccio, C. D., Goretti, V., & Kirrane, S. (2023). Blockchain based Resource Governance for Decentralized Web Environments. *Frontiers in Blockchain*, *6*, 1141909. https://doi.org/10.3389/fbloc.2023.1141909

California Privacy Rights Act. (2020). *California Privacy Rights Act, 2020 (CPRA)*. https://www.consumerprivacyact.com/california-privacy-act-2020-cpra/

Cámara de Diputados de México. (2017). *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*. https://www.diputados.gob.mx/LeyesBiblio/ref/lgpdppso.htm

Campos, B., Rodríguez, C., & Mendoza, A. (2024). Modelos de control de acceso más utilizados en la seguridad de datos médicos. *Revista Tecnología en Marcha*, *37*(1), 114-127. https://doi.org/10.18845/tm.v37i1.6558

Campos, C. (2025). *Ciber riesgos, una nueva era de riesgos para las empresas* [Tesis de grado, Universidad Pontificia Comillas]. https://repositorio.comillas.edu/rest/bitstreams/599675/retrieve

Código Orgánico Integral Penal, Registro Oficial Suplemento 180 de 10-feb.-2014 (2014). https://www.aduana.gob.ec/gacnorm/data/CODIGO-ORGANICO-DE-LA-PRODUCCION-COMERCIO-E-INVERSIONES.pdf

Coloma, A. (2023). Implicaciones en materia de protección de datos personales en la creación y entrenamiento de modelos algorítmicos. *Revista de privacidad y derecho digital*, *8*(30), 60-90.

Congreso Nacional de Brasil. (2019). *General Personal Data Protection Act (LGPD)*. https://lgpd-brazil.info/

Constitución de la Republica del Ecuador, Registro Oficial 449 de 20-oct-2008 (2008). https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Erdélyi, G., Erdélyi, O. J., & Kempa-Liehr, A. W. (2023). *Data Fusion Challenges Privacy: What Can Privacy Regulation Do?* (arXiv:2111.13304). arXiv. https://doi.org/10.48550/arXiv.2111.13304

Estrada, C. (2024). La impunidad en los delitos informáticos. Una problemática de poco interés por los legisladores, jueces y fiscales. *Ius vocatio*, *7*(9), Article 9. https://doi.org/10.35292/iusVocatio.v7i9.928

Fattah, I. A. (2024). The mediating effect of data literacy competence in the relationship between data governance and data-driven culture. *Industrial Management & Data Systems*, *124*(5), 1823-1845. https://doi.org/10.1108/IMDS-11-2023-0812

Galindo, O. A. (2020). Transformación digital: Una agenda de oportunidades para la investigación y la práctica. *Revista Perspectiva Empresarial*, *7*(2), Article 2. https://doi.org/10.16967/23898186.646

Garcés, F. A., Diaz, I. J. D., & Moreno, P. M. (2023). Evaluación del derecho al olvido en la salvaguarda de datos personales en Ecuador. *Dilemas contemporáneos: Educación, Política y Valores*. https://doi.org/10.46377/dilemas.v11iEspecial.3949

Garcés, F., Díaz, I., & Moreno, P. (2023). Evaluación del derecho al olvido en la salvaguarda de datos personales en Ecuador. *Dilemas contemporáneos: Educación, Política y Valores*, *XI*. https://doi.org/10.46377/dilemas.v11iEspecial.3949

Guamán, D. S., Ferrer, X., Alamo, J. M. del, & Such, J. (2021). *Automating the GDPR Compliance Assessment for Cross-border Personal Data Transfers in Android Applications* (arXiv:2103.07297). arXiv. https://doi.org/10.48550/arXiv.2103.07297

Hernández, A. S. (2021). Alternativa de investigación en los estudios de la comunicación: El acceso a la información pública y su privacidad como derecho humano en México. *Dilemas contemporáneos: educación, política y valores*, *9*(SPE1). https://doi.org/10.46377/dilemas.v9i.2966

Instituto Geográfico Agustín Codazzi. (2024). *Manual para la Gobernanza de los Datos y la Información*. https://www.igac.gov.co/sites/default/files/listadomaestro/MN-GET-01%20Manual%20para%20la%20Gobernanza%20de%20los%20Datos%20y%20la%20Informaci%C3%B3n.pdf

Jiménez, J. M. (2024). Seguridad y Privacidad en el Tiempo Digital, la Era de la Información Liquida. *Ciencia Latina Revista Científica Multidisciplinar*, *8*(2), Article 2. https://doi.org/10.37811/cl_rcm.v8i2.11136

León, W. A., Giler, K. L. M., & Vera, J. C. V. (2024). Evolución de la Tecnología Educativa de la Física y su Impacto en las Estrategias de Enseñanza Activa en el Aprendizaje de la Física en el Instituto Tecnológico Ismael

Pérez Pazmiño. *Ciencia Latina Revista Científica Multidisciplinar*, *8*(4), Article 4. https://doi.org/10.37811/cl_rcm.v8i4.12480

Ley Orgánica de Comunicación, Registro Oficial Suplemento 22 de 25-jun.-2013. Ultima modificación: 20-feb.-2019 (2013). https://www.gob.ec/sites/default/files/regulations/2018-09/Documento_ley-org%C3%A1nica-comunicaci%C3%B3n.pdf

Ley Orgánica de Protección de Datos Personales, Pub. L. No. S/N, Quinto Suplemento del Registro Oficial No.459 (2021).

Lucio, E., & Campaña, E. (2024). Desafíos y estrategias de ciberseguridad para pequeñas empresas. *ResearchGate*, *6*(11), 18-36. http://dx.doi.org/10.35381/gep.v6i11.151

Madrigal, M. (2024). La protección de datos personales de los costarricenses y la relación con los derechos humanos en un contexto de transformación digital. *Rhombus*, *4*(1), Article 1. https://doi.org/10.63058/rhombus.v4i1.168

Marais, B., Quertier, T., & Morucci, S. (2022). *AI-based Malware and Ransomware Detection Models* (arXiv:2207.02108). arXiv. https://doi.org/10.48550/arXiv.2207.02108

Mendoza, O. A. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista IUS*, *15*(48), 179-207. https://doi.org/10.35487/rius.v15i48.2021.743

Ministerio de Ambiente y Desarrollo Sostenible de Colombia. (2025). *Protección de Datos Personales*. https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2018). *Plan Nacional de Gobierno Electrónico 2018-2021*. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/09/PNGE_2018_2021sv2.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). *Agenda de Transformación Digital de Ecuador 2022-2025*. https://www.arcotel.gob.ec/wp-content/uploads/2022/08/Agenda-transformacion-digital-2022-2025.pdf

Molina, O. (2023). Inteligencia artificial, Bigdata y Derecho a la protección de datos de las personas trabajadoras. *Revista de Estudios Jurídico*

Laborales y de Seguridad Social (REJLSS), *6*, Article 6. https://doi.org/10.24310/rejlss.vi6.16225

Morales, D. A. M., Morales, F. P., Cajamarca, E. E., & Intriago, F. J. (2024). La protección de datos personales en Ecuador: Evolución legislativa y comparación con modelos regionales en Sudamérica. *Perspectivas Sociales y Administrativas*, *2*(2), Article 2. https://doi.org/10.61347/psa.v2i2.70

Mosquera, G. G., Espinoza, L. R., & Chancay, J. D. (2022). Transformación digital e innovación. *RECIAMUC*, *6*(3), Article 3. https://doi.org/10.26820/reciamuc/6.(3).julio.2022.736-744

Murrugarra, B. I. (2024). Inteligencia artificial y privacidad en internet: Amenazas para los datos personales de los usuarios. *Revista Científica Multidisciplinaria Ogma*, *3*(2), Article 2. https://doi.org/10.69516/9dp8ap45

Muzzio, J. M. (2023). Competencia de la ley de protección de datos en las compañías de la provincia de Santa Elena. *Perfiles de Ingeniería*, *19*(20), Article 20. https://doi.org/10.31381/perfilesingenieria.v19i20.6029

Nava, E. (2021). Resignificaciones de las tecnologías digitales en la Sierra Norte de Oaxaca: El Colectivo Multimedios Jënmë'ëny. *Redes. Revista de Estudios Sociales de la Ciencia y la Tecnología*, *27*(53), Article 53. https://doi.org/10.48160/18517072re53.135

Novik, M. (2021, diciembre 7). *Fraudes digitales: Cuenteros y estafadores operan con redes sociales*. Plan V. https://planv.com.ec/historias/fraudes-digitales-cuenteros-y-estafadores-operan-con-redes-sociales/

Oña, O. O. O., Reyes, L. P., Celi, M. V., & López, F. Z. (2025). La protección de datos personales en la era digital—Retos y oportunidades. *Revistalexenlace*, *2*(1), Article 1.

Personal Information Protection Commission. (2025). *Act on the Protection of Personal Information*. https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en

Ponce, J. L. (2024). Seguridad en redes LAN: La protección de datos hasta la prevención de intrusiones. *Journal TechInnovation*, *3*(1), Article 1. https://doi.org/10.47230/Journal.TechInnovation.v3.n1.2024.4-14

Punina, M. C., Paguay, J. M., Yacelga, E. L., Camuendo, L. M., & Gualli, P. B. (2024). El Papel de las TIC en la Implementación de Metodologías Activas en el Campo de la Educación. *Ciencia Latina Revista Científica Multidisciplinar*, *8*(2), Article 2. https://doi.org/10.37811/cl_rcm.v8i2.10566

Ramírez, J. (2023, mayo 4). Violación de Datos Personales y Responsabilidad en el Ámbito Jurídico Ecuatoriano. *In Solidum Abogados*. https://insolidumabogados.com/violacion-de-datos-personales-y-responsabilidad-en-ambito-juridico-ecuatoriano/

Razza, C. (2023). Transferencia internacional de datos personales en Latinoamérica. *Revista Cálamo*, *13*, Article 13. https://doi.org/10.61243/calamo.13.158

Reglamento General a la Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 435 (2023). https://www.gob.ec/sites/default/files/regulations/2025-01/02%20Reglamento%20General%20a%20la%20Ley%20Org%C3%A1nica%20de%20Protecci%C3%B3n%20de%20Datos%20Personales_0.pdf

Rivadeneira, C. C., Cuellar, D. R., & Riomaña, K. (2023). ¿Por qué nuestros datos importan? Conceptos claves sobre los impactos de la inteligencia artificial en la protección de los datos personales y sus marcos de regulación. *Revista Lecciones Vitales*, lv0104-lv0104. https://doi.org/10.18046/rlv.2023.6122

Rivera, B. (2020). La importancia de la protección de datos y la situación actual del Ecuador. *Revista Cálamo*, *13*, Article 13. https://doi.org/10.61243/calamo.13.166

Rojas, M. J., Castillo, J. M. H., & Mendoza, A. C. (2023). Seguridad de la información en la prevención de perdida de datos: Una revisión sistemática. *Innovation and Software*, *4*(2), Article 2. https://doi.org/10.48168/innosoft.s12.a92

Salazar, C., & Avila, B. (2024). Estándares de Ciberseguridad Aplicables a los Sistemas Informáticos Sanitarios para Proteger los Datos Personales. *593 Digital Publisher CEIT*, *9*(1), Article 1. https://doi.org/10.33386/593dp.2024.1.2156

Sánchez, M. F. (2023). El derecho a la protección de datos personales en la era digital. *Revista Eurolatinoamericana de Derecho Administrativo*, *10*(1). https://doi.org/10.14409/redoeda.v10i1.12626

Schmitt, M. (2022). *Automated machine learning: AI-driven decision making in business analytics* (arXiv:2205.10538). arXiv. https://doi.org/10.48550/arXiv.2205.10538

Schmitt, M. (2023). Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration*, *36*, 100520. https://doi.org/10.1016/j.jii.2023.100520

State of California Department of Justice. (2024). *California Consumer Privacy Act (CCPA)*. https://www.oag.ca.gov/privacy/ccpa

Stitilis, D., & Malinauskaite, I. (2024). Compliance with basic principles of data protection in cloud computing: The aspect of contractual relations with end-users. *European Journal of Law and Technology*, *5*(1). https://ejlt.org/index.php/ejlt/article/view/231

Superintendencia de Protección de Datos Personales. (2025). *Recepción de denuncias*. https://spdp.gob.ec/

Vinueza, N. V., Macías, M. Á., & Maldonado, R. L. (2024). Implementación de medidas de seguridad y principio de conservación de datos según la ley orgánica de protección de datos personales en instituciones públicas de Babahoyo, Ecuador. *Dilemas contemporáneos: Educación, Política y Valores*. https://doi.org/10.46377/dilemas.v11i2.4080

Zhang, J., & Datta, A. (2023). *Blockchain-enabled Data Governance for Privacy-Preserved Sharing of Confidential Data* (arXiv:2309.04125). arXiv. https://doi.org/10.48550/arXiv.2309.04125

ANEXOS

Anexo 1. Encuesta

Encuesta sobre el marco legal de la tecnología digital y la privacidad de los datos en Ecuador

Lea cada afirmación y seleccione la opción que mejor refleje su grado de acuerdo, donde:

1 = Totalmente en desacuerdo
2 = En desacuerdo
3 = Neutral
4 = De acuerdo
5 = Totalmente de acuerdo

Preguntas	**1**	**2**	**3**	**4**	**5**
Marco legal y regulación					
1. La normativa ecuatoriana sobre protección de datos personales es clara para garantizar la privacidad en el entorno digital.					
2. La Ley Orgánica de Protección de Datos Personales en Ecuador se encuentra alineada con estándares internacionales de protección de datos.					
3. Las instituciones encargadas de hacer cumplir la normativa de privacidad de datos en Ecuador actúan con eficiencia y rigor.					
4. La regulación actual se adapta adecuadamente a los avances tecnológicos y a las nuevas amenazas a la privacidad digital.					
Aplicación y cumplimiento					
5. Las empresas y entidades públicas en Ecuador cumplen con las regulaciones de protección de datos personales de manera efectiva.					
6. Existen mecanismos adecuados para denunciar vulneraciones a la privacidad de los datos en Ecuador.					
7. Las sanciones establecidas por la normativa ecuatoriana son efectivas para prevenir vulneraciones a la privacidad de los datos.					
8. La ciudadanía ecuatoriana está suficientemente informada sobre sus derechos en cuanto a la protección de datos personales.					
Desafíos en la Protección de Datos					
9. La cooperación internacional es clave para fortalecer la protección de datos personales en el país.					
10. Existen deficiencias en la infraestructura tecnológica y jurídica que afectan la efectiva aplicación de las leyes de protección de datos.					
11. Es necesario un mayor esfuerzo en la capacitación de jueces, fiscales y abogados en materia de protección de datos personales.					
12. Considera que el marco legal actual en Ecuador ofrece suficientes garantías para proteger la privacidad de los datos personales frente a entidades extranjeras (por ejemplo, empresas internacionales que operan en Ecuador)					