

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

TEMA:

“Parámetros Jurídicos de la Ley de Protección de Datos Personales en el entorno universitario”

Proyecto de investigación previo a la obtención de título de abogado

AUTOR:

Merino Lara Peter Andres

TUTOR:

Ab. Mg. José Luis Romo Santana

Ambato-Ecuador

2026

A. PÁGINAS PRELIMINARES

TEMA: "PARAMETROS JURÍDICOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO UNIVERSITARIO".

APROBACIÓN DEL TUTOR

Yo, el suscrito Ab. Mg. José Luis Romo Santana, en mi calidad de tutor del trabajo de investigación titulado "**PARAMETROS JURÍDICOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO UNIVERSITARIO**", certifico que dicho trabajo fue elaborado por el Sr. Peter Andres Merino Lara, egresado de la carrera de Derecho de la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad Técnica de Ambato, como requisito previo para la obtención del título de Abogado. Asimismo, dejo constancia de que el trabajo de investigación cumple con todos los requisitos técnicos, metodológicos, científicos, jurídicos y reglamentarios establecidos, por lo cual autorizo su presentación ante el organismo pertinente, a fin de que sea evaluado por la Comisión Calificadora designada por el Honorable Consejo Directivo.

Ambato 08 de diciembre del 2025

Ab. Mg. José Luis Romo Santana

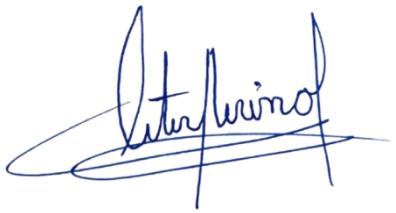
TUTOR

AUTORIA

Los criterios emitidos en el trabajo de investigación "**PARAMETROS JURÍDICOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO UNIVERSITARIO** ". Es un trabajo de investigación es un trabajo de mi propia autoría, el mismo que se realizó a base de una revisión bibliográfica exhaustiva, así como doctrinales y legales. Este trabajo expone ideas, criterios, opiniones, conclusiones y recomendaciones cuya responsabilidad recaen sobre mi autoría.

Ambato, 08 de diciembre del 2025

EL AUTOR



Peter Andres Merino Lara

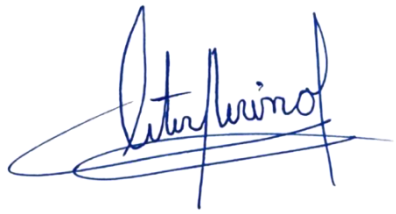
C.I.1804761425

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato a disponer de la presente tesis, en su totalidad o en parte, como documento de consulta, lectura y referencia para fines académicos e investigativos, conforme a las normativas institucionales vigentes.

Asimismo, cedo los derechos patrimoniales en línea de esta obra con fines de divulgación pública, y autorizo su reproducción dentro del marco regulatorio de la Universidad, siempre que dicha reproducción no tenga fines lucrativos y se respete íntegramente mi autoría y los derechos que me corresponden como titular.

Ambato, 08 de diciembre del 2025



Peter Andres Merino Lara

C.I.1804761425

APROBACIÓN DEL TRIBUNAL DE GRADO

Los Miembros del Tribunal de Grado APRUEBAN el Trabajo de Investigación sobre el tema " **PARAMETROS JURÍDICOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO UNIVERSITARIO** ". Presentado por el Sr. Peter Andres Merino Lara, de conformidad con el Reglamento de Graduación para obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato

Ambato, …….. 2026

Para constancia firma:

……

Presidente

…… ……

Miembro Miembro

DEDICATORIA

A Dios, por iluminar cada una de mis decisiones, por sostenerme en los días inciertos y abrirme caminos incluso cuando yo no lograba verlos, a él, que nunca llega tarde y que, incluso en mis dudas, me recuerda que fui creado para avanzar con dignidad, con fe y con un corazón que no se rinde.

A mi madre, Zulema Lara, que desde la distancia tejió para mí un puente de fortaleza e inspiración, a esa mujer que luchó incluso cuando nadie la veía, que calló dolores para que yo aprendiera a volar, que soñó por mí cuando yo aún no comprendía la forma ni el peso de mis propios sueños, cada logro que hoy pronuncio lleva tu nombre escondido entre las letras.

A mi padre, Pedro Merino, mi mejor amigo, quien con acciones más que palabras me enseñó que el coraje no se hereda, se aprende, se practica y se defiende, gracias por guiarme sin imponer, por sostenerme sin empujar, por enseñarme que el verdadero triunfo es mantener la humildad en cualquier circunstancia en la que me encuentre.

A mis hermanos, Lorena Abril y Christian Merino, que fueron abrigo cuando la vida se hizo fría y fueron refugio cuando mis fuerzas flaquearon, gracias por su compañía que cura, por su silencio que entiende, por su presencia que nunca fue duda sino un hogar ya que en ustedes encontré el eco de mi nombre y la certeza de que no camino solo.

A todos ustedes, porque llevo un pedacito de su historia en mi piel y un fragmento de su amor en mi alma. Lo que soy, lo he construido con mis manos, pero con la fuerza que me dieron ustedes.

Gracias con el corazón abierto por ser el origen de todo lo que hoy celebro.

AGRADECIMIENTO

A mis mentores, quienes se convirtieron en pilares esenciales de mi formación, empezando con el Dr. Jorge Arcos, por abrirme la primera puerta en su despacho y permitirme demostrar lo que podía lograr, su confianza en mí se convirtió en un impulso constante para seguir creyendo en mis capacidades.

Al Dr. Pablo Vaca y a la Dra. Daisy López, por confiar en mí, por abrirme un espacio en su vida profesional y personal, y por enseñarme que la justicia se ejerce con firmeza, pero también con humanidad, por sus consejos que llegaron siempre en el momento justo, demostrándome que el conocimiento es más valioso cuando se comparte.

A quienes guiaron mis primeros pasos en el Derecho tanto a SoulLex como al Centro de Mediación Ambato, espacios en donde entendí que el valor del trabajo y la dedicación radica en servir con ética, responsabilidad y respeto.

A mis docentes formadores el Dr. Juan Pablo Montero, el Dr. José Luis Romo, la Dra. Gabriela Acosta, el Dr. Melinton Saca, y a todos los demás docentes que marcaron mi trayectoria, gracias por compartir sus conocimientos con pasión y por mostrarnos que el Derecho es, ante todo, un compromiso con la sociedad.

A mis amigos Luis y David Díaz, con quienes aprendí que un amigo siempre es leal y el hermano nace en la adversidad, porque su amistad fue refugio en mis pruebas y alegría en mis logros. A mis compañeros de clase, Joao y Nayeli, por su presencia constante, su complicidad y su amistad. A la memoria de Edisson Gavilanez, cuya vida dejó huellas profundas en quienes tuvimos la fortuna de conocerlo.

A todas las amistades que formé dentro y fuera de la Universidad, a quienes compartieron conmigo su tiempo, su experiencia, sus consejos, afectos y silencios necesarios.

A cada persona que me ayudó a crecer, que me acompañó emocionalmente y que aportó a mi formación tanto profesional como humana, gracias a todos ustedes porque en cada logro que celebro hay una parte de lo que cada uno sembró en mí.

Peter Merino

INDICE GENERAL

A. PÁGINAS PRELIMINARES ii

TEMA ii

APROBACIÓN DEL TUTOR iii

AUTORIA iv

DERECHOS DE AUTOR v

APROBACIÓN DEL TRIBUNAL DE GRADO vi

DEDICATORIA vii

AGRADECIMIENTO viii

RESUMEN EJECUTIVO xiii

ABSTRACT xiv

B. CONTENIDO 1

CAPITULO I 1

MARCO TEÓRICO 1

1.1.- Estado del Arte 1

1.1.1 Antecedentes Investigativos 1

1.2.- Antecedentes Históricos 6

1.2.1 La Protección de Datos y su origen en la Intimidad como derecho fundamental 6

1.2.2 Origen del Derecho a la Intimidad 6

1.2.3 ¿Qué es el derecho a la intimidad? 8

1.2.4 Aspectos que conforman el Derecho a la Intimidad 9

1.2.5 Titulares del Derecho a la Intimidad 12

1.3.- Antecedentes Conceptuales 15

1.3.1 Conceptualización de Datos Personales 15

1.3.2 Conceptualización de Protección de Datos Personales 16

1.4.- Antecedentes Legales 18
1.4.1 Ley Orgánica de Protección de Datos Personales en el Ecuador 18
1.4.2 Tipos de Datos según la LOPDP y la doctrina jurídica 21
1.4.3 Principios de la LOPDP 23
1.4.4 Parámetros Jurídicos de la LOPDP 26
1.4.5 Derechos que reconoce la LOPDP a sus titulares 28
1.4.6 Parámetros de delegación de protección de datos personales 34
1.4.7 Autoridad de Protección de Datos Personales 36
1.4.8 La Autonomía Universitaria y la aplicación de la LOPDP 38
1.5.- OBJETIVOS 41
1.5.1 Objetivo General 41
1.5.2 Objetivos Específicos 41
1.5.3 Pregunta de Investigación 41
CAPÍTULO II 41
METODOLOGÍA 41
2.1 Tipo de Investigación 41
2.1.1 Diseño 42
2.1.2 Alcance 42
2.2 Métodos de investigación 42
2.2.2 Método Documental 42
2.2.3. Método Analítico y Descriptivo 42
2.2.4. Técnicas e Instrumentos 43
CAPÍTULO III 45
3.1 Resultados y Discusión 45
3.1.1 Análisis y discusión de los resultados 45
CAPÍTULO IV 53
CONCLUSIONES Y RECOMENDACIONES 53

4.1 Conclusiones 53
4.2 Recomendaciones 54
MATERIALES DE REFERENCIA 56
ANEXOS 65
ANEXO 1. GUÍA DE ENTREVISTA CON CONSENTIMIENTO 65
ANEXO 2. FOTOGRAFÍAS CON LOS ENTREVISTADOS 70
ANEXO 3. EVIDENCIA DE LAS ENTREVISTAS 71

INDICE DE TABLAS

Tabla 1. Intimidad vs Protección de datos personales 17
Tabla 2 Entrevista Pregunta 1 45
Tabla 3 Entrevista pregunta 2 46
Tabla 4 Entrevista pregunta 3 48
Tabla 5 Entrevista pregunta 4 49
Tabla 6 Entrevista pregunta 5 50
Tabla 7 Entrevista pregunta 6 50
Tabla 8 Entrevista pregunta 7 51
Tabla 9 Entrevista pregunta 8 52

RESUMEN EJECUTIVO

La investigación titulada *"Parámetros Jurídicos de la Ley de Protección de Datos en el entorno universitario"* desarrolló un análisis jurídico sobre la aplicación de la Ley Orgánica de Protección de Datos Personales en el entorno universitario, con el objetivo de determinar cómo los parámetros legales establecidos en la norma incidieron en los procesos de gestión institucional de datos personales dentro de la Universidad Técnica de Ambato y Universidades Privadas. El estudio se sustentó en una metodología de enfoque cualitativo con diseño documental y alcance descriptivo, basada en la revisión exhaustiva de doctrina, normativa nacional e internacional, así como en entrevistas dirigidas a expertos en materia jurídica y académica. Los resultados evidenciaron que la protección de datos en el ámbito universitario operó de forma limitada, pues, aunque las instituciones contaban con obligaciones normativas claras, persistieron vacíos relacionados con la falta de protocolos específicos, escasa cultura de privacidad, deficiente gestión del consentimiento y ausencia de mecanismos sistemáticos de capacitación para estudiantes, docentes y personal administrativo. Se identificó además que en algunos establecimientos universitarios se trató datos sensibles sin delimitar adecuadamente finalidades, tiempos de conservación y medidas de seguridad, lo que generó riesgos jurídicos y vulneraciones potenciales frente al derecho fundamental a la autodeterminación informativa. Se concluyó que la LOPDP exigió una adaptación estructural que no se encontraba plenamente implementada en la institución, por lo que resultó necesario fortalecer políticas internas, garantizar transparencia en el tratamiento de datos y consolidar una cultura institucional orientada a la protección efectiva de la información personal en el ámbito académico.

Palabras Clave: Protección de datos personales, parámetros jurídicos, entorno universitario, tratamiento de datos, normativa de privacidad, seguridad de la información, derechos del titular, transparencia institucional, autodeterminación informativa, sector académico.

ABSTRACT

The research titled *"Legal Parameters of the Data Protection Law in the University Environment"* conducted a legal analysis of the application of the Organic Law on Personal Data Protection within higher education institutions, aiming to determine how the legal parameters established in the regulation influenced the institutional processes for managing personal data at the Technical University of Ambato and various private universities. The study was based on a qualitative methodology with a documentary and descriptive design, supported by an extensive review of doctrine, national and international regulations, as well as interviews with experts in legal and academic fields. The findings revealed that data protection within the university environment operated in a limited manner; although institutions had clear regulatory obligations, gaps persisted due to the absence of specific protocols, a weak privacy culture, inadequate management of consent, and a lack of systematic training for students, faculty, and administrative staff. Additionally, it was identified that some universities processed sensitive data without properly defining purposes, retention periods, or security measures, resulting in legal risks and potential violations of the fundamental right to informational self-determination. The study concluded that the Organic Law required structural adjustments that were not yet fully implemented within the institutions, making it necessary to strengthen internal policies, ensure transparency in data processing, and promote an institutional culture committed to the effective protection of personal information in the academic environment.

Key words: Personal data protection, legal parameters, university environment, data processing, privacy regulation, information security, data subject rights, institutional transparency, informational self-determination, academic sector.

B. CONTENIDO

CAPITULO I

MARCO TEÓRICO

1.1.- Estado del Arte

1.1.1 Antecedentes Investigativos

El contexto mundial que envuelve la protección de datos y su privacidad reflejan un continuo proceso de optimización bajo una constante actualización de ingenios legales que se encarguen de regular procesos de manejo y tratamiento de datos en entes o contextos institucionales donde la tecnología es sumamente necesaria y útil para generar información de carácter público y privado constantemente (Oña et al., 2025).

En este sentido, los investigadores en su trabajo de investigación "La protección de datos personales en la era digital - Retos y oportunidades" puntualizan que todo ser humano genera datos, motivo por el cual existe intriga respecto a lo que pasa cuando estos datos se almacenan en instituciones que no manejan una cultura de protección y tratamiento apegado a estándares legales esenciales para plasmar fundamentos teóricos y dogmáticos que permitan una comprensión íntegra y un desarrollo metodológico sólido de la LOPDP en Ecuador.

Estudios como la "Transparencia y protección de datos personales en el ámbito universitario en la ciudad de Lima, Perú: hacia una universidad abierta" expone que las universidades, dada su condición de generadoras y tratantes de voluminosos datos personales identificativos, académicos, de salud, creencias, entre otros, deben conciliar su responsabilidad de transparencia con el respeto a la privacidad individual, aun cuando la digitalización y el uso de tecnologías de información ofrecen oportunidades para la gestión institucional y facilitación administrativa.

En este estudio se advierte que una universidad verdaderamente comprometida debe integrar políticas de protección de datos que aseguren consentimiento informado, finalidad legítima, medidas de seguridad y control efectivo del tratamiento de información, evitando vulneraciones de derechos fundamentales, dado este antecedente resulta relevante para el

contexto de educación superior y resalta los desafíos estructurales que enfrentan las instituciones al tratar datos personales en entornos digitalizados (Arenas, 2020).

Otro estudio como es el de Álvarez & Hernández (2024), analizó la protección de datos personales en plataformas digitales utilizadas en instituciones de educación superior en Ecuador, en esta investigación evidenció múltiples vulneraciones derivadas de fallos técnicos, deficiencias en la gestión del consentimiento, ausencia de protocolos claros y una débil cultura institucional de privacidad, pese a la existencia de la Ley Orgánica de Protección de Datos Personales (LOPDP), las universidades aún no logran materializar su cumplimiento de forma efectiva, lo que genera un desfase entre la normativa y su aplicación real, este estudio demuestra que el ámbito universitario enfrenta desafíos estructurales y operativos similares a los identificados en el presente estudio, reforzando la necesidad de examinar la incidencia de la LOPDP en la gestión institucional de los datos personales en el entorno académico ecuatoriano (Álvarez & Hernández, 2024).

Así mismo otra publicación de datos de profesores y alumnos y la privacidad personal en las universidades analiza el manejo y divulgación de datos personales de estudiantes y docentes en instituciones universitarias y advierte que la publicación indiscriminada de información académica vulnera derechos fundamentales de intimidad y protección de datos, esto demuestra que a pesar de la existencia de normativas de protección, muchas universidades no adoptan criterios adecuados para asegurar la confidencialidad, consentimiento informado y finalidad legítima del tratamiento de datos. Este estudio ejemplifica cómo la falta de políticas internas eficaces y la práctica de difusión automática de datos socavan la garantía real de privacidad en el ámbito académico, constituyendo un antecedente relevante que evidencia las dificultades prácticas de aplicar estándares normativos de protección de datos en universidades (Troncoso, 2006).

En estudios como el de Astudillo et al. (2025), se discute la aplicación de la LOPDP en el sistema privado, puesto que las instituciones afrontan grandes dificultades para incorporar a su funcionamiento las disposiciones de la norma, entre los retos que afrontan se presenta la ciberdelincuencia y el acceso no autorizado a los datos personales debido a que no cuentan con políticas claras las cuales conciban los parámetros que indica la ley, la investigación concluye resaltando la urgencia de que las políticas de seguridad y capacitación del personal sean adecuadas a lo necesario para superar los retos que pueden afrontar en conjunto con las posibles sanciones al no velar adecuadamente por los derechos de quienes conforman su institución.

Mientras que el estudio titulado “Protección de datos personales en la universidad: hábitos, actitudes y conocimiento del profesorado” analiza cómo el personal docente comprende y aplica las normas de protección de datos en el contexto universitario, identificando que, aunque existe una actitud favorable hacia la protección de datos, hay un grado significativo de desconocimiento normativo y deficiencias en hábitos concretos que pueden exponer información sensible a vulneraciones.

Los resultados señalan que la protección de datos no está suficientemente integrada en la cultura institucional docente, lo que pone en evidencia la necesidad de acciones educativas y normativas más contundente, esta investigación aporta un referente empírico útil para demostrar que, incluso en contextos con marco normativo, la carencia de conocimiento y prácticas concretas representa un obstáculo real a la efectiva protección de datos en las universidades (Casal Otero et al., 2022).

Es asi que Díaz (2023), en su investigación titulada “Transparencia y protección de datos personales en el ámbito universitario: ¿avance o retroceso?”, critica y analiza la ejecución que las instituciones de educación superior les dan a los cuerpos normativos en aplicación de sus principios básicos, como transparencia y protección de datos, donde se evidencia la utopía que la norma plantea, a pesar del avance tecnológico e institucional que se ha dado continuamente.

Estudios cercanos como el de Constante (2024), titulado “Medidas de seguridad para la protección de datos sensibles de estudiantes y ex estudiantes de UNIANDES”, planteó la identificación de factores que vulneran el tratamiento de datos personales en el entorno universitario y sugirió estrategias de seguridad aplicables para su protección, el estudio destaca que el entorno universitario estudiado carecía de reglamentos, protocolos y capacitación adecuada del personal encargado.

Así mismo Rosas & Pila (2023), en el artículo “La protección de datos personales en Ecuador: una revisión histórica-normativa de este derecho fundamental en el país suramericano”, identificaron los eventos normativos más significativos y principales que respaldan el derecho a la protección de datos personales en Ecuador, destacando el progreso trabado que se ha tenido desde la promulgación de los derechos constitucionales en su carta magna del 2008 hasta el origen y establecimiento de la Ley Orgánica de Protección de Datos Personales en 2021, determinando la persistencia de vacíos normativos que regulen y tutelen efectivamente los derechos que son materia de estudio continuamente.

Entre las observaciones realizadas por los investigadores señalaron que la institución encargada de gestionar el tratamiento de datos personales requiere ser fortalecida y armonizada con mecanismos de estandarización internacional y aplicación efectiva de control, llegando a remarcar que los marcos normativos ecuatorianos demandan la actualización y tratamiento adecuado el cual promueva la confianza de los ciudadanos en las tecnologías de la información con las que el país cuenta y vela por el resguardo de la privacidad informativa.

Cordero (2023) en su trabajo titulado "Protección jurídica, Habeas Data y la Ley Orgánica de Protección de Datos Personales frente a la autodeterminación informática y la protección de datos personales", estudio el marco legal ecuatoriano que protege los datos personales y determino los problemas que la codependencia de los derechos fundamentales como la intimidad, la privacidad y otros similares tienen con sus mecanismos de efectivización, problema que se comprueba mediante el cotejo comparativo que realiza con marcos normativos internacionales, su análisis refleja que Ecuador no posee un avance significativo a consecuencia de sus vacíos normativos no subsanados, así como tampoco se posee una cultura vinculada a la protección de datos personales, además de hacer mención al desconocimiento de la ley y sus concordancias con otras vías jurídicas de protección como la constitucional, penal y demás afines, concluyendo que la promulgación de una ley específica no es suficiente para cumplir efectivamente con los mecanismos de control y participación activa de quienes son generadores de datos.

Pascual & Vázquez (2022), desde su perspectiva investigativa en su trabajo "Protección de datos y uso ético de la tecnología para una didáctica sostenible", tuvieron como propósito examinar el ámbito educativo y su vínculo ético con el uso de las plataformas tecnológicas por parte de docentes y estudiantes, siendo enfáticos en los contextos educativos digitales y su protección de datos personales, resaltando la insuficiencia de conocimientos previos respecto a lo que el uso de estas técnicas conlleva en perjuicio de los datos generados en su aplicación, resaltan los campos que deben ser trabajados continuamente en beneficio del fortalecimiento de una cultura precavida y responsable de información generada en los entornos educativos, resaltando su uso respetuoso hacia el normativo jurídico respectivo que protege los derechos fundamentales colectivos.

Arenas (2020), en su exégesis "Transparencia y protección de datos personales en el ámbito universitario: hacia una universidad abierta," detalla el conflicto existente entre la necesidad de que las universidades sean transparentes y la obligación que se tiene para

salvaguardar los derechos fundamentales que envuelven a la protección de datos personales de los miembros que pertenecen al ámbito académico superior, en este sentido se revela que las instituciones de educación superior contienen grandes cantidades de datos que se generan a diario como consecuencia del uso de los sistemas digitales, formula la incógnita de poseer una universidad transparente y comprometida la cual respete la intimidad ganando la confianza de quienes la conforman, señala que a pesar de los avances tecnológicos notorios y la conciencia de las personas respecto al amparo que le dan sus derechos, existen dificultades para acceder a una clasificación de información como demanda de carreras profesionales, mallas curriculares, personal docente capacitado, acceso a calificaciones o perfiles profesionales, por ello es necesario mantener una moderación entre los principios de transparencia y la protección de datos privados, dejando en evidencia que un entorno universitario debe ser pionero de un gobierno abierto pero crítico ante una participación activa en el entorno generador de datos.

Díaz & Fonseca (2019) en su tesis "Vulneración de la intimidad y privacidad por el indebido tratamiento de datos personales en el Ecuador" el goce de derechos a la protección de la intimidad y privacidad que el poder constitucional le otorga a los ciudadanos hoy en día es transgredido por entes públicos y privados lo cual afecta la seguridad jurídica que genera la ausencia de protocolos representativos de una realidad legal carente de sanciones las cuales sean equivalentes y proporcionales a sus accionantes infractores, siguiendo esta idea se impulsa la manifestación obligatoria de mecanismos efectivos para el tratamiento y protección adecuado de datos personales, así como también un delegado principal y encargado de darle la relevancia necesitada.

Porcelli (2019), en su indagación científica "La protección de los datos personales en el entorno digital. Los estándares de protección de datos en los países iberoamericanos", elaboró un estudio detallado respecto al presente que enfrenta el derecho a la privacidad en una era moderna y digital reconociendo la realidad iberoamericana, comparando los cuerpos legales que se encargan de preservar la generación de datos que a su vez deben ser protegidos, observando de esa manera las problemáticas a las que se enfrentan sus vacíos legales e incluso dejando en evidencia la insuficiencia de protocolos que perfilen el correcto desarrollo de los estándares previos en diferentes países que han adoptado la cultura de protección los cuales reconocen ejes fundamentales como el derecho al olvido, en concordancia con la autodeterminación informativa y explicando la necesidad de portar

una garantía de privacidad digital con enfoque evolutivo y formativo acorde al desarrollo tecnológico.

González (2021), en su trabajo doctoral "Los Datos Personales en la web: intervención de los poderes públicos" revela la importancia y el valor que las tecnologías de la información y comunicación han asumido con el paso del tiempo, pues su desarrollo digital hace accesible a que diferente tipo de información sea divulgada casi instantáneamente, hecho por el cual se genera una gran cantidad de datos que se almacenan en instituciones públicas como privadas dejando que la globalización de estos medios sea vertiginosa, dentro de este marco, se refleja el desarrollo de personalidad que la gente adopta en vista del comportamiento que exteriorizan las plataformas digitales dejando ver las afectaciones que pueden conllevar el verse inmerso en un mundo el cual no contempla la importancia jurídica al mostrar las causas y efectos del actuar que tienen diferentes usuarios ajenos a una cultura de protección de datos.

1.2.- Antecedentes Históricos

1.2.1 La Protección de Datos y su origen en la Intimidad como derecho fundamental

En una época marcada por la digitalización de la información y la continua exposición pública en virtud de las injerencias tecnologías y sociales se convierte en un desafío para la contemporaneidad de los cuerpos normativos la protección de los datos personales en cualquier núcleo de desarrollo, el derecho a la intimidad constituye un pilar fundamental y relevante de cara a la protección de la dignidad humana en conjunto con el libre desarrollo a la personalidad, donde la privacidad de un solo individuo puede influir en el desarrollo de una agrupación familiar o en contextos similares a los cuales no se permite la intromisión de sujetos externos a su núcleo generador, este apartado surge con el objetivo de explotar el conocimiento recopilado dentro de la naturaleza jurídica y las facultades que se le han otorgado con el pasar del tiempo (Hernández, 2025).

1.2.2 Origen del Derecho a la Intimidad

El análisis del derecho humano a la intimidad y su delimitación con el derecho fundamental de libre desarrollo de la personalidad, dan origen al conocimiento y comprensión de la obligación y derecho a la protección de datos personales, por ello, resulta imprescindible traer a conocimiento a su precursor conceptual originado en el activismo legal e interpretación judicial *"common law"* que surge en el siglo XIX época en la cual dos magistrados de la honorable Corte Suprema de los Estados Unidos conocidos como Louis

Brandeis y Samuel Warren crean la obra *"The Right to Privacy, 1890"* obra en la que despliegan el conflicto emergente que generaba el derecho a la información como consecuencia de sus vivencias respecto a la constante exposición pública de su vida privada por la prensa que en su momento representaba la crítica y exposición continua de los hábitos en los que incurrían (Warren & Brandeis, 1890).

Si bien es cierto el derecho a la intimidad y su reconocimiento como un derecho humano, surge como un fenómeno característico del siglo XX a partir de la Declaración Universal de los Derechos Humanos (1948) el cual establece en su artículo 12 que *"nadie será objeto de injerencia en su vida privada"* lo que se traduce como una protección legal ante las intromisiones de terceros en la vida privada de un sujeto (Asamblea General de las Naciones Unidas, 1948).

Dicha concepción se refleja en otros textos legales como el Pacto Internacional de Derechos Civiles y Políticos (1966) dentro de sus dos primeros incisos del artículo 17 donde se estable que "*Nadie podrá ser objeto de injerencias arbitrarias o ilegales en su vida privada …"* además de señalar que cualquier persona debe ser objeto de protección en cuanto a su privacidad por la norma frente a la vulneración de la intimidad (Asamblea General de las Naciones Unidas, Pacto Internacional de Derechos Civiles y Políticos, 1996).

De manera particular, resulta fundamental señalar que siguiendo este hilo de ideas se reconoce e identifica lo establecido en el artículo 11 de la Convención Americana de Derechos del Hombre celebrada en San José de Costa Rica (1969) donde se indica la protección de una persona frente a la divulgación de su información de carácter privado y que a su vez instaura mecanismos de cumplimiento por medio de la aplicación de la norma (Organización de los Estados Americanos, 1969).

El marco normativo internacional (convencionalidad) previamente citado sentó las bases para que diferentes países acojan este criterio convencional dentro de sus cuerpos legales constitucionales al derecho a la intimidad, en una sucesión cronológica se encuentra Venezuela en el año 1961, posteriormente a Bolivia y a Ecuador ambos en el año 1967, más adelante en el mundo oriental esta Egipto en 1971, Europa se hace presente con España en 1971 y Chile en 1980, en contraposición las grandes potencias mundiales como Estados Unidos, Alemania, Italia y Francia no adoptaron la constitucionalización de este derecho,

sin embargo, fueron países que aportaron con doctrina y jurisprudencia lo que a futuro los obligo a aceptar este cambio generacional de derechos (Rosas & Pila, 2023).

1.2.3 ¿Qué es el derecho a la intimidad?

El vínculo existente entre el desarrollo generacional de la tecnología y los derechos fundamentales genero una obligación en los especialistas del derecho a que por medio de la doctrina se refinen las conceptualizaciones tradicionales de la intimidad que se adapten a los nuevos cambios generacionales que la sociedad necesita, para ser analizada desde una perspectiva de protección de datos resulta indispensable acudir al campo doctrinario que recopila sus implicaciones existentes, en palabras de Gonzalo Gallo (2008) autor de "La protección de datos personales" obra que se destaca en la doctrina del derecho informático en la que define al derecho a la intimidad como:

> *"El derecho que poseen las personas de poder excluir a las demás del conocimiento de su vida, es decir de sus sentimientos, emociones, datos bibliográficos y personales, de su imagen. En términos técnico - jurídicos, se puede hacer una distinción entre el Derecho al honor, el Derecho a la intimidad personal y el Derecho a la propia imagen"* (Gallo, 2008, pág. 17).

A partir de esta definición el autor revela la amplitud y la caracterización principal que posee este derecho al otorgarle autonomía en cuanto al control de su información privada y que a su vez da a entender que se engloban emociones y sentimientos que se reflejan en la imagen del sujeto. En este sentido, es preciso señalar la relación latente de la intimidad con la privacidad dejando entrever las diferencias que existen, de modo que la intimidad ha crecido progresivamente hasta llegar al punto en el que se ve legislado y requiere solicitar permisos de accesibilidad o almacenamiento de información personal, espacio en el que las personas deciden quien puede ser confidente o beneficiario de lo indicado siempre y cuando el tercero interesado goce del consentimiento del propietario.

Profundizando en lo anterior Morales (2016, pág. 78), conceptualiza este derecho como un espacio propio de cada individuo que se encuentra en libertad de generar información sin injerencia de terceros que deseen acceder a la misma sin permiso del titular y que de ser ese el caso, sin que se relacione con el derecho al honor se podrá exigir una reparación integral a la víctima en vía civil o penal según se configure la situación dejando claro que la protección de este derecho es directa a diferencia del honor que generalmente se lo tutela posteriormente a su violación.

Es así como la composición del derecho a la intimidad en principio y de manera general se subdivide en dos posturas, la primera comprende la inviolabilidad a la vida privada del individuo al mantener en discreción los asuntos de carácter personal que de ser violentados se constituiría una infracción directa; y, la segunda que comprende la autonomía del titular para tutelar su propio derecho al decidir quién es beneficiario consentido de su información y quien no es beneficiario del consentimiento.

No obstante esta garantía del derecho fundamental, a partir de la arbitrariedad de los terceros se configura cuando estos invaden aquellos límites que les impone el propietario de la información, este posee la capacidad de qué tipo de información desea hacerla pública y cual merece ser reservada para el público en general, este tipo de comportamientos conectan con el derecho al libre desarrollo de la personalidad al poseer su libertad de conciencia siendo el único responsable de sus acciones máxima jurídica "el ejercicio de un derecho propio concluye donde comienza el derecho ajeno".

La libertad de que las personas posean una vida privada se determina en base a los fenómenos políticos, sociales y económicos en los que se encuentra el generador de información de entre los que se pueden nombrar, según Nogueira (2003, pág. 113), la vida privada da cabida a ideas y creencias, vida sexual y sentimental, situaciones familiares, enfermedades físicas o psicológicas, comunicaciones personales, pasado judicial, comportamiento social, entre otras que pueden existir y vincularse directamente.

1.2.4 Aspectos que conforman el Derecho a la Intimidad

El proceso evolutivo que ha tenido el ámbito jurídico respecto al derecho a la intimidad reconocido como derecho fundamental en virtud de la vida privada de los sujetos generadores de información dan paso a que en su estudio se examine la composición elemental que le otorgan diferentes autores y legislaciones a lo largo del tiempo, para ello es preciso traer a colación el conocimiento desarrollado por Morales (2016) en su trabajo "Derecho a la Intimidad" donde se desglosa aquellos elementos esenciales de la intimidad.

1.2.4.1 Tranquilidad

En una de las primeras definiciones que el derecho le otorga a la intimidad por parte de un honorable miembro perteneciente al Tribunal Supremo de Michigan el juez Thomas Cooley en el año 1879 en su obra *"Treatise on the Law of Torts"* sostuvo el teorema de que todo ser humano debe contar con la posibilidad de estar solo o aislado y en tranquilidad,

expresión que posee un significado que supera las barreras de un estado de calma o en silencio, se entiende que las personas no deben ser perturbadas en su intimidad y al cual una sociedad civilizada le debe respeto para su desarrollo pleno como ser humano (Díaz M. , 2011, pág. 282).

El vínculo de relación que se genera al estar "solo" con el libre desarrollo de la personalidad, trae consigo implícitamente la autoformación o definición del humano, al no sentirse rodeado de injerencias ajenas al resultado deseado, sin embargo, si este origen se ve afectado se constituye un agravio que es susceptible de reparación, independientemente de si esta vulneración afecta leve o gravemente a la víctima, esta idea de invasión es una ofensa en sí misma por ende se exige que se compensen las angustias o preocupaciones de quien fue sujeto de ataques a su espacio personal.

1.2.4.2 Autonomía

Como parte integral del derecho, la autonomía es considerada como una capacidad única del ser humano, que goza de libertad para la toma de múltiples decisiones las cuales influyen en el desarrollo de su vida sin que estas se vean afectadas por el criterio o evaluación de otros que puedan llegar a limitar la voluntad que fundamenta la alternativa seleccionada por el sujeto, esto implica que la libertad va de la mano con el control que los individuos tengan para decidir sobre lo que les conviene o no en determinadas circunstancias (Ramírez, 2011, pág. 18).

La transformación que se da en la autonomía gira en torno a la misma esfera de *"reserva"* que se manifiesta en la tranquilidad del ser humano, es así como se convierte en un derecho activo de control sobre su proyecto de vida personal, se entiende que el único capaz de tomar decisiones importantes que definan su identidad u existencia en el entorno social es el mismo ser que desea tomar un rumbo direccionado por sus creencias o relaciones afectivas que gestionen su imagen propia, dejando de lado las medidas de imposición que un tercero o el mismo Estado le quiera asignar arbitrariamente en sus elecciones.

1.2.4.3 Control de la información

El control y gestionamiento de la información es la base fundamental del derecho a la intimidad, considerado por muchos juristas como la justificación para que se brinde mecanismos o formas protección necesaria, permite sujetarse de dos alternativas presentes, siendo la primera la reserva de ciertos aspectos privados referentes a la vida personal del

sujeto que deben permanecer ocultos y el segundo, que abarca el flujo de determinada información en organizaciones públicas o privadas que han sido confiadas por el titular de los datos (Díaz M. , 2011).

Ejercer el derecho citado parte de la concepción de que los individuos poseen control total de sus datos personales, esto significa que el titular no solamente otorga consentimiento del uso de sus datos, sino que también tiene la posibilidad de exigir la actualización, modificación o rectificación de los datos que han sido compartidos.

Sin embargo, la gestión o control de la información resulta conflictivo al poseer distintas perspectivas de protección y vulneración, por un lado, se encuentra la protección al derecho a la intimidad y por otro se evidencia la difusión de información que promueven los medios de comunicación como los periódicos, la prensa radial, prensa televisiva y medios actuales como la internet al tratar de cumplir con las funciones que les han sido encomendadas por la misma sociedad (Flores et al., 2025).

De entre sus funciones se encuentra la investigación y la difusión de información que recolectan mediante la interacción directa con aquellos sujetos generadores de detalles comunicativos que captan el interés o morbo social, este argumento podría desencadenar una vulneración de derechos al momento en que se dejan de resguardar los principios y las normas como consecuencia de una falta de ética y moral de quienes investigan los hechos que serán divulgados públicamente (Monereo, 2025).

Desafortunadamente, no es habitual que los sujetos reclamen abiertamente cuando la prensa se inmiscuye en la intimidad de la gente para obtener el núcleo de la información que desean exponer al público que no necesariamente se ve interesado en dicha información, continuamente la prensa ignora lo establecido en los cuerpos normativos y viola directamente el derecho a la intimidad, en vista de que no se tiene un limitante que responda por los daños, genera incertidumbre en aquella minoría que conoce de sus derechos y la protección que le otorga a su intimidad, la normalización de que estos riesgos se haga efectiva en una sociedad despreocupada, justifica a los medios su forma invasiva de recolección de datos por una supuesta “demanda” de audiencia o público que esté de acuerdo con esta exhibición (Vasco et al., 2025).

1.2.5 Titulares del Derecho a la Intimidad

Una vez que se han definido los aspectos que conforman el derecho a la intimidad, se torna transcendental que se identifiquen a los sujetos que gozan de su titularidad, en este sentido, resulta obvio el origen de este derecho, la persona física o natural es quien abarca lo indicado con anterioridad, pues su fundamento y desarrollo se encuentra en la dignidad humana y en el libre desarrollo de la personalidad además del respeto hacia el orden jurídico establecido (Ávila, 2019).

1.2.5.1 Las personas naturales

El Código Civil en su artículo 1461 define los actos y declaraciones de voluntad que las personas pueden tener, el artículo 40 define a las personas naturales como tal, el artículo 1462 establece quienes gozan de capacidad legal, por otro lado también define a las personas que son absolutamente incapaces en su artículo 1463, con este preámbulo se debe resaltar que la titularidad del derecho es universal, sin embargo, se debe llevar a cabo una diferenciación de cuando el individuo posee y cuando no posee capacidad jurídica para ejercer sus derechos, primero cuando se consiente el uso de datos o registros personales a terceros, al consentir su tratamiento se refleja la capacidad de decidir si el control de su información será el adecuado al aceptar las políticas de protección que el tercero le otorga al entregar sus datos en vista de que el titular tiene la comprensión total del asunto (Código Civil, 2024).

Y por otro lado las personas incapaces que no gozan de la plenitud de sus facultades para otorgar el consentimiento de forma autónoma ya que en su lugar quienes toman esas decisiones son sus representantes legales o quienes se encuentren facultados para actuar en beneficio de los intereses de quien no lo puede hacer o a quien se encuentran representando (artículo 1464 del Código Civil), existe la posibilidad de que el incapaz tenga discernimiento de las actuaciones, en este caso excepcional quien se encuentre representándolo será quien consienta el uso de sus datos a más del titular, esto incluye la demostración de la autorización judicial que lo faculta para realizar estos procesos.

1.2.5.2 Personas Fallecidas

La aplicación de estos criterios indicados es exclusivamente para aquellos seres vivos que aún pueden velar por sus intereses, no obstante, el escenario post mortem se torna complejo en vista de que los doctrinarios expertos contradicen sus teorías respecto al tratamiento de

esta información, por un lado, la jurisprudencia norteamericana sostiene que las personas pierden este derecho al fallecer y por otro lado la jurisprudencia europea contrapone esta idea al señalar que la privacidad de los datos generados por una persona antes de su muerte deben seguirse protegiendo, con el argumento de que estos datos han formado y creado historia en el mundo humano (Código Civil, 2024).

Dentro de la legislación Argentina, específicamente en los artículos 31 y 32 de la ley 11723 catalogada como "Régimen Legal de la Propiedad Intelectual" promulgada por el Honorable Congreso de la Nación Argentina, expresan los límites que las personas tienen cuando desean utilizar información perteneciente a una persona que ya falleció, entendiéndose que las personas aun estando muertas gozan de este derecho siempre y cuando se cumplan los requisitos que la ley les exige (Honorable Congreso de la Nación Argentina, 1933).

1.2.5.3 Personas Jurídicas

Marín (2007) indica que la privacidad de una persona jurídica se tutela de diferentes formas a las que se tutela en una persona natural, menciona que, si bien es cierto, comparten ciertas similitudes como el derecho a tener una identificación propia (nombre), o una dirección domiciliaria lo cual les permitiría poseer su intimidad, para ellos concurre otra posibilidad de verse envueltos en consecuencias legales que responsabilicen el daño provocado a sus derechos más importantes como personas jurídicas antes que como personas naturales

La norma civil ecuatoriana establece una definición para las personas jurídicas en su artículo 564, para las personas jurídicas el marco del derecho a la intimidad no los envuelve en vista de que los legisladores han sostenido el criterio de que una afectación moral a una persona jurídica no se materializa como tal y por ende no es necesario emplear un mecanismo de protección a la intimidad.

1.2.6.- Antecedentes de la Protección de Datos Personales

La necesidad de registrar y administrar correctamente la información personal surge de los riesgos que estos conllevan cuando se ven expuestos indebidamente, su práctica es inherente a cualquier forma de organización social tanto en la administración pública como en la administración privada, por lo que la visualización de este actuar no solamente se centra en recopilación de datos, sino en cómo se la consigue y que tratamiento se le está brindando (Código Civil, 2024).

La recolección de datos en papel fue el punto de partida para que el ser humano y sus delegaciones sociales se encarguen del tratamiento de datos personales, su evolución con el paso del tiempo se ha vuelto evidente por la continua actualización de mecanismos informáticos los cuales hoy en día se encargan de organizar y almacenar los datos que cualquier persona genera o comparte con aquellos individuos que gozan de su confianza o cuentan con la autorización de observarlos (Díaz & Fonseca, 2019).

Actualmente, los archivos físicos se conservan pero a su vez han sido digitalizados en bases de datos que se encuentran compuestas por información personal recopilada diariamente, principalmente por las ingeniosas características técnicas con las que cuentan las computadores de uso general, estas máquinas permiten que cualquier sujeto almacene y gestione grandes volúmenes de información personal y en algunos casos información ajena, esta masificación de datos ha provocado que el Estado deba intervenir por medio de la promulgación de leyes para que se regulen los procesos de tratamiento de datos personales.

En 1951 en Estados Unidos la creación de la Oficina Intergubernamental para Informática (IBI) asumió la carga de ser pioneros en el tratamiento de datos personales al detectar los riesgos que influyen sobre la sociedad al utilizar herramientas tecnológicas, asumió el papel de alertar y recomendar a los otros Estados mundiales a que acoplen en sus legislaciones parámetros jurídicos que se adecuen a la protección de la información para que los datos personales fueran usados únicamente en beneficio de la sociedad y que a su vez mediante solicitud de parte se permita la rectificación o actualización de la información que proporcionan (Ávila, 2019).

Posteriormente, otros países priorizaron su avance con estos parámetros jurídicos, un ejemplo claro de esta actualización de criterios se dio a conocer en el artículo 35 numeral 3 de la Constitución Portuguesa (1976), texto en el cual se establecieron criterios racionales con respecto a cómo se llevan a cabo la gestión de datos, siendo este el momento en el que las creencias filosóficas, las convicciones religiosas, políticas y demás aspectos que conforman la vida privada del individuo se excluyen de ser requeridos digitalmente, sino que únicamente estos datos sean requeridos para establecer datos estadísticos relacionados y que de esa forma se preserven los intereses sociales (Asamblea Constituyente de Portugal, 1976).

Siguiendo este precepto constitucional en 1978 el estado Español estableció un mandato que limita el uso de la informática con el objetivo de que se proteja la intimidad de los

ciudadanos, en su artículo 18 numeral 4 determina como las herramientas digitales (informática) se ven restringidas en sus facultades para que de esa manera se pueda garantizar el derecho al honor y la intimidad de las personas en conjunto con sus familias (Cortes Generales, 1978).

La unión de naciones Europeas por intermedio de su parlamento dispuso una amplia gama de lineamientos normativos que se centran en dar el debido cuidado jurídico a la protección de datos dentro del campo tecnológico esto incluye comunicaciones electrónicas o físicas que contengan información de diferente referente a su intimidad.

1.3.- Antecedentes Conceptuales

1.3.1 Conceptualización de Datos Personales

El análisis adecuado de la protección de datos personales inicia con su origen en los datos personales, el estudio de su objeto jurídico se tutela en base a sus principios básicos, a partir de la conceptualización se pueden definir las articulaciones que garantizan derechos y obligaciones relacionadas, por eso la doctrina cumple un papel fundamental en el entendimiento de este conocimiento (Sanz, 2025).

En este sentido es preciso señalar que un dato es sinónimo de información, pero no necesariamente es lo mismo, puesto que el dato es una micro unidad que ha recabado hechos por medio de la experiencia del sujeto, en cambio la información es un proceso que transforma al dato para que obtenga su funcionalidad por lo tanto se entiende que la información contiene al dato (Naranjo, 2017).

En Madrid los juristas Dozo & Martínez (2017, pág. 33) dentro de su obra "Glosario Iberoamericano de Protección de Datos" en sus palabras definen particularmente al "dato personal" como la información cuantificable que incluye rasgos físicos, así como características de la personalidad que pertenecen e identifican a una persona de forma en que se pruebe o se materialice su existencia.

Para una mejor comprensión, es la forma en la que a los humanos se nos puede diferenciar de los otros e identificar individualmente, partiendo desde nuestro nombre, los años de vida, lugar en donde crece y se desarrolla (domicilio), huellas dactilares, firmas manuscritas o digitalizadas, rasgos físicos que forman las características por las cuales se vuelve única la existencia de un individuo o por las cuales sus semejantes (familia o amigos) conocen e identifican al sujeto. Cabe resaltar que el formato en el que se

encuentren los datos recopilados, por ejemplificar, en papel, discos duros informáticos y demás afines se compactan totalmente y se incluyen dentro de las políticas de tratamiento y gestión.

Las diversas entidades que pertenecen al sector público y privado entre ellas las universidades, centros de salud, bancos, lugares de hospedaje, entre otras, son receptoras de información personal que sirven para realizar diferentes actividades las cuales beneficien su estructura física a la par que se desarrolla la confiabilidad y buen nombre de la institución al adquirir un producto o celebrar la contratación de un servicio.

1.3.2 Conceptualización de Protección de Datos Personales

Conde (2005), define a la protección de datos personales como la tutela jurídica que los sujetos generadores poseen para ejercer y exigir su protección en los órganos de justicia ante la posible configuración de una vulneración debido al deficiente tratamiento y uso de datos por parte de terceros que no poseen autorización o consentimiento, este mecanismo imposibilita la creación información falsa llegue a afectar el entorno social o entorno profesional donde se desenvuelve el individuo, su importancia se refleja en las limitaciones que protegen el derecho constitucional de la intimidad.

Siguiendo este criterio doctrinario, las características de la protección de datos personales se resumen en tres aspectos claves; la primera se refiere a que la información sin importar su naturaleza (digital o física) sea susceptible de ser técnicamente procesable; la segunda es la forma inequívoca en que se identifique la titularidad de sujeto (información que no sea falsa); y la tercera describe la falta de legitimidad para que las operaciones de tratamiento de datos se ejecuten (Ávila, 2019).

La protección de datos personales es considerada como un elemento esencial para el ejercicio de derechos conexos a la dignidad humana que generan funcionalidad dentro de la sociedad, según lo analiza Betancour (2018), entre ellos se desenvuelve la conexión latente con el derecho al acceso a la información, la autonomía intelectual del individuo para gobernar su razonamiento expresivo (libertad de pensamiento), la manifestación u exteriorización de ideas respecto al pensamiento del individuo (libertad de expresión), el pluralismo cultural (la diversidad cultural) como un valor positivo para la sociedad y el derecho práctico efectivo que tiene toda persona a exigir un conjunto mínimo de garantías en la justicia (acceso al debido proceso).

En algunas prácticas que involucran la protección de datos se ven inmersos actores sociales (administración pública y privada) quienes son controladores de datos en virtud de las funciones de recolección, recopilación y gestión que realizan continuamente con ayuda de mecanismos tecnológicos o manuales los cuales se utilizan con fines prácticos en áreas de salud, educación o dentro del sistema financiero, cuya funcionalidad depende del vínculo que se mantiene con aquellos particulares que generan la información.

Al establecer los actores sociales, la funcionalidad e importancia de los datos en el mundo del derecho, es oportuno dar a conocer los elementos que vuelven a una persona determinable, en palabras del jurisconsulto Álzate (2016) los datos son generados a partir del nacimiento de la persona y sus rasgos genéticos (huellas dactilares, iris, demás físicos), que datos pueden ser cuantificables numéricamente o reconocidos sensitivamente por gráficos e incluso sonidos, su diversificación provoca una continua actualización de información en lo que se conoce respecto a una persona.

La operatividad efectiva de la protección de los datos inicia con la "cesión voluntaria de derechos o consentimiento" por parte de su titular al momento de registrar documentalmente su nacimiento hasta el registro de su fallecimiento, su tutela depende de las políticas de uso y destino que el Estado proporciona para restringir la difusión ilícita de los mismos, es pertinente señalar que toda persona tiene la capacidad de saber quién se encuentra facultado para utilizar sus datos, para garantizar al titular su derecho a obtener la rectificación de sus datos cuando estos se encuentren incompletos, inexactos o su información sea incorrecta.

Tabla 1.

Intimidad vs Protección de datos personales

Intimidad	**Protección de Datos Personales**
Protege datos no procesados	Protege datos procesados y no procesados
Protege datos íntimos	Protege todo tipo de datos incluyendo públicos
Previene el acceso no autorizado a la intimidad	Protege el uso, la gestión y circulación de datos

Su protección requiere la invasión ilegítima a la intimidad, pero su tutela es posterior a una vulneración	Su protección se activa desde que se recolecta y se trata los datos, incluso antes de una vulneración
Preserva la intimidad	Garantiza la autodeterminación informativa

Elaborado por: *Merino (2025)*

1.4.- Antecedentes Legales

1.4.1 Ley Orgánica de Protección de Datos Personales en el Ecuador

La convencionalidad entre Estados da lugar a que se desarrollen instrumentos jurídicos concretos con la finalidad de responder a las realidades amenazantes que la humanidad enfrenta no solo en contextos físicos sino también digitales, en la actualidad los derechos fundamentales como la protección de datos personales deben contar con un sistema garantista de funcionamiento adecuado y respetuoso.

Con el paso del tiempo las organizaciones internacionales han creado múltiples instrumentos como las "Directrices de la Organización para la Cooperación y el Desarrollo Económico" en la década de los 80, documento en el cual se establecieron principios sumamente importantes para lo que hoy en día llamamos protección de datos personales, entre los principios que se establecieron figura la minimización de datos, calidad, especificación de fines, limitación de uso, transparencia, acceso a la información por parte del titular de los datos y el libre flujo de información, estos principios señalados forman parte del espíritu de las legislaciones nacionales e internacionales con la finalidad de que se armonicen las relaciones entre Estados (Organización para la Cooperación y el Desarrollo Económico, 1980).

En este sentido, las interacciones entre Estados fueron avanzando y de esa forma generaron la "Resolución 45/95 de la ONU" en los años 90, al sentir la necesidad de guiar apropiadamente a la legislaciones internas de los países para proteger el derecho a la intimidad, se instauraron los principios directores de la digitalización de datos personales de esa forma el estándar de protección posee una guía en principios de licitud, exactitud, seguridad, control y sanción como complementos a los principios antes enunciados en la década de los 80 (Asamblea General de las Naciones Unidas, 1990).

La evolución no se detuvo y llegó al desarrollo de 12 principios que estableció la "Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas" en el año 2012, para que los miembros de esta organización entre ellos Ecuador, evalúen sus leyes e implementen principios de confidencialidad y consentimiento previo, en resumidas cuentas, era lo que la actualidad les exigía en asuntos de seguridad y defensa nacional a los Estados (Comité Jurídico Interamericano, 2012).

Estas discusiones enriquecieron la protección de datos personales, sin embargo, su evolución no termino allí y en el año 2015 se promulgaron dos fuentes esenciales del derecho digital como la "Resolución A/HRC/RES/28/16 del Consejo de Derechos Humanos" y la "Guía Legislativa sobre la Privacidad y la Protección de Datos Personales en las Américas", instrumentos en los que oficialmente se expresó la preocupación por parte de los Estados ante la amenaza que representaban los delitos informáticos al derecho a la privacidad e integridad de las personas (Consejo de Derechos Humanos, 2015).

La evolución informática en la humanidad hizo que en el año 2017 la preocupación por mejorar los mecanismos de protección de datos personales revele la "Estrategia de la Red Iberoamericana de Datos Personales" y el "Protocolo de Adhesión de Ecuador al Acuerdo Comercial Multipartes con la Unión Europea", concluyendo con bases sólidas como los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos" y la "Estrategia de la Red Iberoamericana de Datos Personales 2021 - 2025" en el año 2020, estos documento se proyectaron a controlar la violencia digital a través del trabajo en equipo por parte de autoridades administrativas de diferentes instituciones, entre ellas las academias universitarias basándose en los principios de acceso y corrección de información así como el tratamiento especializado en información sensible (Red Iberoamericana de Protección de Datos, 2017).

En el territorio Ecuatoriano, la primera referencia de amparo constitucional para la protección de datos personales se registra en el año 1996 dentro de la enmienda a la carta magna de 1976, esto en virtud de que los legisladores se vieron en la necesidad de establecer el habeas data como garantía jurisdiccional (Naranjo, 2017). No obstante, la asamblea constituyente de Montecristi en 2008 fue quien reconoció el derecho a la protección de datos de carácter personal con precisión en el artículo 66 numeral 19 garantizando un cierto grado de tutela en atención al avance social que significaron los estándares de protección establecidos internacionalmente.

La base de la protección de datos personales tiene sus cimentos en el poder de disposición de la información personal, esto es un control autónomo de gestión y transmisión de información por parte del individuo generador, explicando que quien recopila los datos debe respetar los derechos del otro, de esa forma la defensa del bien jurídico protegido se ampara en los límites que la ley les impone a los sujetos (principio de legalidad). Es decir, si no existiría una tutela semejante dentro del texto supremo, la vulneración a derechos fundamentales de un individuo no permitiría la armonía dentro de la sociedad motivo de anarquía total (Naranjo, 2017).

Dentro del texto supremo es fácil identificar este derecho, sin embargo, no aporta mayor conocimiento respecto a los datos personales al no definir claramente aquello que es considerado como un dato personal, argumento sumamente necesario para quien necesite defender su vínculo con los demás derechos fundamentales conexos para no caer en una simple interpretación de la norma, esta no es la única problemática que nuestra carta magna exhibe, de ninguna forma se determina una estrategia o mecanismo que regule preventivamente el uso y tratamiento de datos ni en el sector público y mucho menos en el sector privado.

La República del Ecuador incorporó públicamente en su Registro Oficial Suplemento 459 con fecha 26 de mayo de 2021 a la LOPDP, para la promulgación de esta norma el legislador ecuatoriano se fundamentó en el criterio internacional que antecede y a su vez asumió el mandato constitucional directo, en este punto es importante señalar el tiempo que le tomo al país incorporar una norma que responda a los estándares internacionales de protección de datos personales (LOPDP, 2021).

Dentro del considerando del cuerpo legal se analiza que el Ecuador es un Estado de derechos en él que se proclama la justicia, ciertamente el derecho a la protección de datos que reconoce la constitución es fuente de inspiración para que el legislador concuerde con el refuerzo que la garantía del Habeas Data le otorga al pueblo para acceder a su propia información y que responde al criterio vinculante con las nuevas tecnologías de acceso universal.

El objeto y finalidad de la ley se encuentra plasmado en su artículo 1 el cual en resumen garantiza la forma y el estado en el que la sociedad ecuatoriana hace valer su derecho fundamental por medio de su autonomía al acceder y rectificar la información que los caracterice por medio de la aplicación de principios y formas de tutela efectivos que se

hallan establecidos. La aplicación material como territorial de esta norma incluye a civiles vivos y muertos, además de aquellos que no han sido identificables para el sistema, lo más importante es que no se limita únicamente a los mencionados, sino que sus artículo 2 y 3 respectivamente contempla otras formas en las que su aplicación se puede ver involucrada.

1.4.2 Tipos de Datos según la LOPDP y la doctrina jurídica

Los datos que son considerados de tipo personal parten de la conceptualización de "dato" según la Real Academia de la Lengua de España es aquel antecedente el cual comprende información que supone consecuencias legales a partir de la divulgación del contenido de un conocimiento obtenido por medio de un proceso de interacción o comunicación entre el generador emisor y el receptor que lo procesa; su valor radica en el conocimiento recopilado, motivo por el cual se pueden llegar a concluir ciertos aspectos positivos o negativos que poseen un valor indeterminable para quien generó y proporcionó esa información .

El valor de la información en los sectores público o privado es incalculable, puesto que los datos son considerados como un activo importante en el ámbito informático, la forma en la que se opera con los datos transforma radicalmente el funcionamiento de cualquier entidad, el "acceso libre" a datos personales determinaría una clara vulneración a la intimidad personal de cualquier individuo, por ello, su protección debe ser permanente y continua con apego a las normas o protocolos de protección que se encuentre establecidos.

En el artículo 4 de la Ley Orgánica de Protección de Datos Personales (2021) en el Ecuador se establecen términos y definiciones de los datos de la siguiente manera:

> a) Dato biométrico: Dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros (LOPDP, 2021).
>
> b) Dato genético: Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobre la fisiología o salud de un individuo (LOPDP, 2021).
>
> c) Dato personal: Dato que identifica o hace identificable a una persona natural, directa o indirectamente (LOPDP, 2021).

d) Datos personales crediticios: Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera (Asamblea Nacional del Ecuador, 2021).

e) Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos, datos relativos a las personas apátridas y refugiados que requieren protección internacional, y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales (LOPDP, 2021).

f) Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud (LOPDP, 2021).

g) Datos sensibles: Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales (LOPDP, 2021).

Es importante destacar las definiciones que el legislador ecuatoriano le entrega a la clasificación de los datos, sin embargo, los datos personales no se limitan únicamente a los citados, puesto que se crearía un catálogo cerrado que fallaría estrepitosamente en su objetivo de protección y para ello es necesario dar a conocer otro tipo de datos personales que se categorizan en el artículo 25 de la LOPDP y otros que se definen por medio de la doctrina investigativa, que involucran a los actores sociales que pertenecen al entorno universitario, por lo que a continuación se mencionaran los siguientes:

a) Datos Sociales: Son aquellos datos que contienen información creada a partir del contacto entre humanos, los cuales detallan hábitos, aficiones compartidas en foros o asociaciones sociales (Lasso, Franco, & Estrada, 2022).

b) Datos Académicos: Es aquella información que determina la valoración o preparación académica de un sujeto por medio de su interacción con el ámbito educativo por medio de títulos o calificaciones consignadas por su actuar, que se

almacena y administran en una institución educativa (Travieso & Hernández, 2025).

c) Datos de salud o médicos: Son aquellos datos que identifican el estado de salud física o mental de un individuo, que se detallan controles médicos y según su frecuencia se plasman en historias clínicas que se conservan en instituciones de salud (Muñoz, Modragón, Duro, Rueda, & Sorokin, 2023)

d) Datos Administrativos: Es aquella información que contiene aspectos técnicos dentro de procedimientos que la administración sigue en contra de un sujeto o viceversa como reclamaciones, solicitudes y recurso interpuestos por el administrado o particular en contra de la administración (Álvarez, 2021).

e) Datos Judiciales: Es información sensible que contiene el pasado judicial de un individuo que se ha visto involucrado en procesos con la justicia (Guerrero, 2020).

f) Datos Públicos: Son aquellos datos que no están sometidos a ser reservados ni tampoco gozan de la privacidad y que por lo general se ven expuestos en documentos públicos como sentencias o resoluciones del poder público (Dozo & Martínez, 2017).

g) Datos de acceso: Es aquella información que mantiene el carácter de reserva y que para poder acceder a ella se deben identificar las credenciales de acceso o consentimiento del titular dentro de una plataforma digital en una institución pública o privada (Nieves & Ponjuan, 2021)

La definición terminológica proporcionada y su complemento en la LOPDP sigue sin ser suficiente, al existir la posibilidad de que con el pasar del tiempo se continúen desarrollando clasificaciones de datos las cuales posibiliten el reconocimiento de futuros derechos que se vinculen a la protección de datos. Sin embargo, las definiciones recopiladas permiten que el entendimiento de la protección de datos se certero y no una simple o vaga interpretación en caso de que se presenten problemáticas que requieran de su conceptualización y definición.

1.4.3 Principios de la LOPDP

La autonomía del sujeto al gestionar su información determina el control que posee respecto a los datos que genera en un entorno físico como digital, pues el individuo es quien se encarga de crear información para sí mismo o para un tercero que lo requiera, el impacto

que posee la protección datos en la sociedad se refleja en la dignidad que envuelve al sujeto el cual goza de igualdad y autonomía en su actuar (Herrán, 2003). El vínculo existente entre la autonomía del sujeto y el marco jurídico que lo respalda garantiza que cualquier individuo al cual se le haya vulnerado su derecho goce de una normativa que cuenta con principios que respaldan su seguridad jurídica en caso de que así se lo necesite.

Las normas en general definen los principios que la rigen, el caso de la LOPDP no es ajeno a esa realidad pues dentro de su artículo 10 se introducen y se definen aquellos mecanismos de optimización a la ley que armonizan con el texto constitucional al igual que con los instrumentos que forman parte de la convencionalidad que el Ecuador reconoce y del cual forma parte.

En lo que respecta a los 13 mecanismos que optimizan la norma de protección de datos, el que encabeza una definición como tal es principio de juridicidad a quien se lo concibe como una forma de sumisión total por parte de quien realiza el tratamiento de datos hacia todo el conjunto normativo establecido; el principio de lealtad por su parte determina que para conseguir datos y tratarlos no se debe incurrir en engaños para hacerlo posible porque existen formas legales de hacerlo.

Así mismo menciona que el principio de transparencia exhorta a que el sujeto encargado de tratar los datos ofrezca detalles sencillos de comprender respecto a su accionar en los datos personales; el principio de finalidad por su parte determina que la recolección y procesamiento de datos solo se podrán usar para lo que se solicitó como único propósito a excepción de que si surgiera un nuevo propósito este sea compatible con su motivo principal (LOPDP, 2021).

Continuando con este desglose, el principio de pertinencia y minimización de datos personales limita al recolector de datos a que si su finalidad y propósito se cumplió no debe excederse en seguirlo haciendo, es así como concuerda con el principio de proporcionalidad del tratamiento el cual indica que la acción de procesar datos debe adecuada, necesaria, equilibrada y justa con la meta propuesta; el principio de confidencialidad restringe la revelación o divulgación de datos con personal que no se encuentre autorizado ya que de esa forma se conserva el sigilo de su operación, en este sentido el principio de calidad y exactitud promueve la garantía de que los datos procesados sean correctos, completos, actualizados y en caso de ser incorrectos estos sean rectificados o suprimidos inmediatamente (LOPDP, 2021).

La armonía que representan estas conceptualizaciones con la realidad persiste, en este caso es pertinente explicar el principio de conservación, este mecanismo exige un límite de tiempo para conservar datos ya que si su finalidad se cumplió no se los necesita más, sin embargo, se excluyen aquellos datos que poseen fines específicos de conservación como los de interés público; el principio de seguridad de datos personales determina que el responsable de conservar los datos se ve en la obligación de protegerlos efectivamente; el principio de responsabilidad proactiva y demostrada señala que el responsable no puede esperar pasivamente a que surja un problema para que se preocupe por cumplir con la ley sino que se debe demostrar que se anticiparon a los posibles riesgos a los que se puede enfrentar (LOPDP, 2021).

En este orden de ideas, el principio de aplicación favorable al titular implica que la interpretación con dudas respecto a la celebración de voluntades o el ejercicio de voluntad soberana de documentos legales que generen controversia ante un órgano autoritario se encargará de beneficiar a la individualidad de la persona con el contexto que mejor se aplique a su realidad y por último el principio de independencia del control establece que necesariamente debe existir una autoridad la cual goce de objetividad (independencia, imparcialidad y autonomía) para que resuelva controversias de forma que no existan conflictos de interés en medio de sus resoluciones (LOPDP, 2021).

Dados estos principios se entiende que guardan relación con el manejo de datos a gran escala que el entorno universitario comprende con los sujetos generadores como los estudiantes, docentes, servidores públicos y trabajadores, el solo hecho de que la norma los establezca como fuente del derecho obliga a las instituciones y a sus autoridades a adoptar una cultura de protección de datos incluyendo la transparencia del uso de la información desde su inicio hasta su final sin incurrir en posibles vulneraciones que afecten el desarrollo común de sus integrantes, el tratamiento de datos en las instituciones de educación superior debe responder a una finalidad exacta, de esa forma la confianza en su funcionamiento será mayor por quienes conforman la universidad (Travieso & Hernández, 2025).

De este modo, la autonomía universitaria y el eje de protección de datos personales crean un espacio en el que la responsabilidad compartida nutre la cultura de seguridad que los instrumentos internaciones y la constitución buscan con el establecimiento de sus normas en respuesta a lo que la sociedad con sus cambios demanda, legitimando los roles preventivos que las administraciones asumen al ser portadoras de recursos valiosos, pero a su vez vulnerables como los datos personales.

1.4.4 Parámetros Jurídicos de la LOPDP

Los actores principales que componen el sistema de protección de datos se encuentran establecidos en el artículo 5 del cuerpo normativo en estudio, en se identifican seis involucrados independientes uno del otro que responden a la conformación del sistema, el primero responde a la titularidad del derecho en el caso de las universidades son los estudiantes, docentes, servidores públicos y trabajadores, el segundo responde como un responsable del tratamiento de datos, el tercero es el encargado de tratar los datos, el cuarto se identifica como el destinatario, en el quinto se materializa a la autoridad de protección de datos personales y el sexto integrante del sistema es el delegado de protección de datos personales miembro que estrictamente debe pertenecer a la institución que lo requiere (LOPDP, 2021).

El ejercicio pleno de los derechos que la ley le faculta al individuo se harán efectivos por intermedio del "responsable del tratamiento" de datos pues es quien cumple la responsabilidad de adoptar mecanismos razonables que permitan ejercer el derecho al acceso de información en el entorno universitario puede ser un miembro activo de la misma, sin embargo, el ejercicio de los derechos no se limita en el responsable, sino que su exigencia también se la realiza por medio de la "Autoridad de protección de datos personales" al ser un órgano que se encuentra facultado para dictar normativa complementaria en procesos de carácter administrativo que necesiten solución, por último se encuentran los "jueces competentes" quienes responden a los procedimientos que leyes complementarias establecen para reclamar una posible reparación según lo determina el artículo 6 de la LOPDP y el artículo 12 del Reglamento de la LOPDP.

Para el entorno universitario estas tres figuras adquieren gran relevancia debido a que los bancos de datos que manejan incluyen información sensible de sus principales actores, por ello, el desarrollo de mecanismos efectivos a la interna es sumamente necesario para tutelar efectivamente el derecho que envuelve a la comunidad usuaria de la tecnología, asimismo, la conexión con autoridades de protección administrativas o judiciales permite que se recepten directrices que fortalezcan las políticas desarrolladas internamente y así se resuelvan las brechas que se presenten (Sanz, 2025).

La legitimidad del tratamiento de los datos personales requiere que se cumplan ciertas condiciones explicitas que garanticen legalidad, transparencia y respeto a los derechos que el titular posee, el artículo 7 de la LOPDP establece que la legalidad del tratamiento es

válida cuando se cuenta con el consentimiento del titular, también lo es cuando se cumplen ordenes legitimas de autoridades competentes, sigue siendo legal cuando se cumplen objetivos de interés público (políticas públicas), del mismo modo, goza de legitimidad cuando se cumplen ordenes establecidas dentro de las celebraciones de voluntades (contratos), la legalidad se incluye cuando el tratamiento versa sobre la integridad de una persona (salud vital); y por último se concibe como legal el uso de datos personales sin consentimiento cuando el responsable de tratarlos posee una razón válida para hacerlo sin que esta razón menoscabe derechos fundamentales como la privacidad (Asamblea Nacional del Ecuador, 2021).

En las instituciones de educación superior se goza del consentimiento de sus actores cuando estos acceden a formar parte de la universidad puesto que, al incorporarse voluntariamente se proporcionan datos que permitan identificarlos dentro de su establecimiento legitimando de esta forma su tratamiento de datos, no obstante, este consentimiento no es ilimitado puesto que el objetivo de su recopilación tiene un propósito con un fin garantizado, la declaración de propósitos por parte de la institución lo convierte en un acto completamente informativo para los titulares por lo que estos saben que pueden acceder e incluso modificar su información si así se lo desea.

De igual forma, el cuerpo legal destaca la irrenunciabilidad de los derechos por parte del titular, además implementa un apartado en el que indica una de las obligaciones que los actores del sistema de protección de datos deben cumplir, entre los principales se destaca la presencia del Estado como el ente de mayor jerarquía del cual forman parte los otros actores como las entidades educativas y sociedades u organizaciones que proveen servicios de información, tienen la obligación de impartir capacitaciones especializadas en el adecuado uso y tratamiento de datos al compendio generalizado de titulares o representantes legales del derecho, la ley proporciona un rango de edades para que se ejerzan sus derechos ante la autoridad pertinente, el primero comprende un rango de edad que va desde los mayores a doce años hasta los menores de quince años para que su derecho sea reclamado por medio de sus representantes legales, de igual forma faculta la autonomía de ejercer su derecho al grupo que comprende las edades de mayores de quince años hasta los menores de dieciocho años según corresponde al artículo 24 de la LOPDP.

La obligación de impartir capacitaciones especializadas en el entorno universitario significa que esta institución no solamente debe proteger los datos que recopila y almacena de sus estudiantes, docentes y personal administrativo que lo rodean, sino que a su vez debe

cumplir con un rol proactivo y mandatario como formador por medio del diseño de programas efectivos con los que se pueda llegar a su audiencia masiva, sin embargo, es precisamente en este punto donde se evidencia el problema que este parámetro jurídico implica para la institución educativa porque fallan al ejecutar esta obligación al verla como una carga burocrática para cumplir parcialmente con lo que la norma le exige antes de ser vista como una misión de formación ética.

1.4.5 Derechos que reconoce la LOPDP a sus titulares

El estado en el que este derecho es concebido por parte de la convencionalidad internacional parte de la naturaleza como un derecho fundamental para el desarrollo autónomo de los datos que genera, estas facultades otorgan control y decisión sobre el accionar que el titular mantiene respecto a sus datos personales en cuanto a su procesamiento en aquellas bases que contienen sus datos, como consecuencia lógica del avance sistemático de las tecnologías se han vinculado ciertos derechos como la oposición al tratamiento inadecuado de datos entre otros que se pueden establecer como una fuente de reclamo o modificación que se requiera por parte de su titular (Flores et al., 2025).

Las universidades al ser una entidad que ejerce las funciones de recopilar y tratar datos de sus miembros activos como estudiantes y docentes en su mayoría, deben asumir el papel de agentes controladores e informadores de acuerdo a su implicación jurídica con la LOPDP, es de vital importancia que se difunda la variedad de derechos que se vinculan con la protección de datos y con aquellos que la norma de datos les faculta a los miembros de la comunidad universitaria, de esa forma las posibles vulneraciones que se generan dentro del establecimiento puedan ser solventadas mediante mecanismos efectivos que los protejan por medio de un reglamento interno.

1.4.5.1 Derecho a la información

La importancia de este derecho como un pilar fundamental de la protección de datos se deriva de la transparencia que presentan las políticas de protección de los sujetos recopiladores como un antecedente de informar previamente a la recopilación de datos detallando los aspectos específicos y definiendo el propósito para el cual fueron compilados de forma gratuita, lo que como consecuencia permite tomar decisiones informadas, ya que sin ella, la efectivización de derechos por parte del titular no se verían ejercidos en su totalidad si posteriormente este desea suprimir o rectificar sus datos proporcionados, la irregularidad de este tratamiento ha significado un verdadero reto para aquellos tratadistas

que se han involucrado con la problemática actual de las nuevas tecnologías (Gacitúa, 2014)

La LOPDP aplica los parámetros jurídicos de lealtad y transparencia como fuente del derecho a la información en su artículo 12 determinando principalmente que este derecho le pertenece únicamente al titular de la información y sobre el versan detalles sumamente relevantes que se deben considerar cuando se recopila información para un determinado objeto, es así como la ley lo define en 17 aspectos que expresan la precisión de su uso frente a quien proporciona los datos, de igual forma indica el ciclo de vida que el dato posee de principio a fin cumpliendo con uno de los propósitos que la ley mantiene al tratar de eliminar cualquier ambigüedad que se materialice y asegurando la comprensión plena de su titular.

La norma es estricta al momento de plantear los posibles escenarios en los que se puede recopilar información, ya sea con el consentimiento pleno de su titular para que así se dote de un control autónomo o si esta se obtiene indirectamente, para el segundo apartado se establecen plazos para que se notifique con un lenguaje de fácil comprensión al titular actuando como una forma de transparencia informativa respecto a sus datos, evitando la incapacidad de que el titular ejerza sus derechos fundamentales al acceso, rectificación o supresión de información que el recopilador posee (LOPDP, 2021).

Las instituciones de educación superior como sujetos responsables del tratamiento de datos por medio de sus políticas de protección se ven en la obligación de cumplir con la transparencia y veracidad del objetivo por el cual se recopilan datos en nombre de sus titulares directa o indirectamente, verificando que sus notificaciones sobrepasen la barrera de un simple comunicado y que de esa forma la institución formule un aviso claro de privacidad hacia estudiantes, docentes, servidores públicos y trabajadores, conservando el control informado de su derecho fundamental en caso de ser necesario para diferentes actuaciones que se requieran.

1.4.5.2 Derecho de acceso

De acuerdo con Gacitúa (2014), la trascendencia de este derecho dentro del marco jurídico de protección de datos personales exterioriza su importancia cuando el monitoreo de datos está limitado a un control parcial por su propio sujeto generador el cual en un principio fue informado de su recolección para que un tercero ajeno a su realidad mantenga la capacidad de conservarlos posterior a su tratamiento. En este sentido, se entiende como una facultad

legal que inviste a su titular con varias herramientas para que conozca el origen de sus registros de datos con los objetivos determinados de su recopilación inicial, permitiendo que a su vez acceda libremente a sus bancos de información que contienen datos de carácter personal.

De este modo, la LOPDP concede una definición propia a este derecho en su artículo 13 en el que inicialmente se puntualiza que el titular de la información puede conocer sus datos de forma gratuita cuando se lo requiera y que su almacenador deberá responder oportunamente a su requerimiento con detalles exactos de lo solicitado en un principio sin necesidad de que su titular motive su solicitud en un plazo de quince días, sin embargo, la ley también restringe su acceso siempre y cuando se verifique esta solicitud presentada por parte de su titular constituya un abuso del derecho que lo faculta (Asamblea Nacional del Ecuador, 2021).

Al comprender las conceptualizaciones teóricas y legales que envuelven este derecho, resulta inevitable que se profundice su aplicación en entornos almacenadores de datos como las instituciones de educación superior ya que estas se ven obligadas a brindar servicios de calidad que cumplan con los estándares de responsabilidad sobre el tratamiento y protección de datos de sus estudiantes, docentes, servidores públicos como titulares de información producida o proporcionada dentro del establecimiento, para lo cual se necesita de procedimientos o parámetros jurídicos internos que establezcan ordenes de fácil acceso para sus titulares cuando estos deseen contar con los registros de datos tratados por su institución almacenadora de forma efectiva y sin dilaciones o impedimentos que le permitan ejercer su derecho .

1.4.5.3 Derecho de rectificación

Gacitúa (2014), explica que este derecho posee un fuerte vínculo con aquellos principios legales de calidad y veracidad que la ley exige para que se responda a una realidad sin adulteraciones, indica que el titular de la información tiene la capacidad de realizar peticiones de corrección o rectificación sobre su información a quien solicito su permiso para recolectar la información, cabe destacar que cuando se presenta la problemática común de recopilación de datos existen escenarios en los que sus almacenadores dejan sus datos incompletos o inexactos y esto a su titular lo puede afectar directamente al no contar con información exacta, el ejercicio de este derecho puede ser inmediato cuando su titular

se percata de que su información proporcionada fue erróneamente recopilada o su vez en otro escenario posterior a su recolección.

Ciertamente, la LOPDP establece ciertos parámetros a seguir para el ejercicio de este derecho en el artículo 14 remarcando principalmente la responsabilidad que el almacenador tiene para corregir aquellos errores que se pudieron producir al momento de la recopilación de datos, su actualización y corrección de contenidos puede ser solicitada por su titular con una justificación debida ante quien se responsabilizó de recolectarlos en un plazo determinado de quince días informando a quien corresponda sobre las modificaciones que hayan surgido como consecuencia de su corrección u actualización (LOPDP, 2021).

Como es lógico, la confluencia entre lo legal y lo teórico incide directamente en aquellos parámetros jurídicos que una institución de educación superior debe contemplar para su correcto funcionamiento, pues su visión debe abarcar soluciones efectivas para aquellas dificultades que pueden influir en el desarrollo de su comunidad, por ejemplificar, en el caso de los estudiantes y docentes al momento de enmarcar sus calificaciones en los sistemas, un dato inexacto o erróneo puede perjudicar gravemente a un estudiante ya que se le puede privar de valiosas oportunidades como lo son accesos a becas y demás, por errores involuntarios de su docente al momento de procesar dicha información, al contar con un protocolo adecuado para tratar estas problemáticas se cumple con el objeto de la ley ya que no se vulnerarían los derechos del titular.

1.4.5.4 Derecho de oposición, eliminación y bloqueo

La oposición a que ciertos datos personales pertenecientes a un sujeto generador sean tratados por un sujeto encargado de tratarlos debido a una situación legitima justificada hace que se lo reconozca como un derecho fundamental del titular, esto implica que el tratamiento de datos no debe realizarse sin antes haberse resuelto aquello que lo impide. Gacitúa (2014) indica que si el tratamiento de datos se efectuó y si su titular deseaba oponerse, pero los datos ya fueron tratados, la manera de cancelarlos solo se podría dar si se cumple con lo que se menciona en un inicio y con una debida justificación del por qué se deseaba hacerlo, a ello se lo conoce como el derecho de eliminación o cancelación; existe otro escenario en el que el tratamiento de datos debe detenerse pero que su eliminación es improcedente, a este apartado se lo denomina como bloqueo de datos.

La norma de protección de datos en el Ecuador establece individualmente la forma y el contenido de los derechos que se ejercen por parte del titular, el derecho de eliminación

por su parte permite que el titular pueda solicitar la supresión de los datos personales que fueron recopilados según el artículo 15, este derecho se puede exigir en siete formas establecidas, por ejemplo, cuando se usan los datos de forma incorrecta, así como cuando existe orden legal de borrarlos o incluso cuando el titular se arrepiente de haber proporcionado esa información. De igual forma el derecho a la oposición mantiene su reconocimiento en el artículo 16 estableciendo principalmente la oposición o negación a que los datos de carácter personal pertenecientes a un individuo sean tratados previa solicitud de su titular que debe ser atendida por quien se encarga de tratar sus datos en un plazo de 15 días, conjuntamente determina tres limitaciones en las que no se puede ejercer este derecho. Por último, el artículo 19 establece condiciones en la cuales la suspensión del tratamiento de datos personales se podrá presentar si se cumplen con ciertas condiciones (LOPDP, 2021).

Induciendo este parámetro jurídico en el entorno de las instituciones de educación superior, se debe indicar que es necesario contar con canales de atención especializada en ámbitos que involucran la protección de datos de su comunidad contemplando principios de accesibilidad, transparencia y celeridad que garanticen la plenitud del derecho, e imponiendo un orden por medio de reglamentos o lineamientos internos en los que se especifiquen las competencias y responsabilidades a quienes se les ha encargado el tratamiento y protección de datos por medio de capacitaciones constantes de su personal generando de esta forma una armonía con aquello que la ley propone.

1.4.5.5 Derecho a recurrir

En lo que respecta a este derecho tiene su inicio cuando se hace presente la inconformidad del titular frente a la toma de decisiones que han resuelto conflictos referentes a derechos que no han sido respetados como consecuencia de que no se ha dado seguimiento a lo que establecen las normas, de acuerdo con Gacitúa (2014), recurrir no solamente es un derecho sino también es una obligación que el Estado debe garantizar a quienes realicen un reclamo como consecuencia de que se les ha vulnerado sus derechos por no ajustarse a los presupuestos que establecen las disposiciones legales frente una autoridad máxima o incluso desencadenar un recurso judicial sobre el que la justicia evalúa la situación a detalle.

Frente a esta situación la norma de protección no determina un apartado exacto sobre el derecho a recurrir, sin embargo, la constitución del ecuador propone como una garantía

básica del debido proceso el derecho a recurrir al fallo sobre procedimientos en los que los derechos de las personas se vean envueltos dentro del artículo 76 numeral 7 literal m, la LOPDP en su artículo 20 establece herramientas (recurrir) que permiten ir en contra de decisiones que han sido producto de la automatización y para ello en su literal e claramente indica la impugnación de decisiones que pueden llegar a salirse del respeto a las normas claras y previas, dentro de este apartado también se producen límites que no permiten el abuso de este derecho en cuatro formas adecuadas que eviten esta situación, finalmente, agrega dos protecciones clave para aquellas situaciones complejas que muchas de las veces limita el ejercicio de este derecho por eso la ley faculta que ningún individuo será obligado a renunciar a este derecho (LOPDP, 2021).

La autonomía de una institución de educación superior se ve cuestionada cuando se aplican este tipo de parámetros jurídicos, ya que en muchas ocasiones estas instituciones tienden a interpretar su forma de autonomía como una facultad absoluta de resolución de conflictos, olvidándose de aquellos lineamientos que las normas previas establecen para que se dé cumplimiento en este tipo de situaciones.

Su autonomía siempre tendrá un límite mientras el marco jurídico no modifique el sentido de su contenido, este desafío exige a los entornos universitarios a que adopten medidas que armonicen con la realidad de posibles víctimas del autoritarismo inmotivado. La implementación de reglas claras cuyas formas de actuación sean eficaces ante las problemáticas que surgen repentinamente, generaran confianza en aquellos estudiantes, docentes, servidores públicos y trabajadores que conforman la comunidad universitaria cuando sus derechos se ven en juego por un desorden estructural provocado por una pobre política de protección de datos personales,

1.4.5.6 Derecho de reparación

Como regla general, hay que destacar la importancia que la reparación tiene cuando un sujeto ha sido afectado moral o materialmente por otro como consecuencia del desacato de normas previas en materia de protección de datos personales. Travieso & Hernández (2025), advierten que estos daños pueden surgir incluso cuando se celebra un vínculo contractual previo con aquellos sujetos que tratan y almacenan los datos de las personas, explica que no por el hecho de que exista un consentimiento previo del titular significa que sus encargados tienen permitido dañar a su proveedor, ya que con el solo hecho de demostrar un daño real y la muestra de la culpa sobre una vulneración directa a su bien

jurídico protegido es suficiente para que su titular reclame una reparación acorde a su vulneración.

En este sentido la ley de protección de datos no determina un apartado específico para este derecho, este omisión normativa provoca que la reparación a las víctimas por los daños que se les ha provocado moral o materialmente se quede en un limbo jurídico al no tener certeza del alcance que tienen los posibles medios de reparación en las diferentes vías judiciales como la administrativa, civil o constitucional para que se cuantifique el daño y consecuentemente se proporcione su reparación, estos efectos adversos dificultan que los jueces competentes se pongan de acuerdo en el criterio de cómo manejar las pruebas o cuando se le declara a alguien responsable del daño, de esta forma también se ralentiza la efectivización de una tutela efectiva de derechos, su ausencia en general merma la eficacia de aquellos parámetros jurídicos que deberían proteger los datos personales (LOPDP, 2021).

Las instituciones de educación superior en su calidad de organismos encargados de la protección de datos personales de su comunidad activa, deben responder ante estas posibles problemáticas que tarde o temprano surgirán en su establecimiento, considerando diferentes aspectos que se ven involucrados como la obligación de reparar los daños ocasionados cuando se usan indebidamente los datos personales o cuando se filtran datos sensibles ante el público, la norma expresa debe reflejarse en protocolos que determinen seguridad en el accionar de aquellos delegados de proteger los datos personales, se deben señalar formas en las que se incluyan procedimientos de verificación de daños para que posteriormente se establezca una compensación simbólica por los daños causados y respetando la dignidad de cada persona.

1.4.6 Parámetros de delegación de protección de datos personales

La figura de un responsable a quien se le asignaran funciones que hagan cumplir los establecimientos legales de protección de datos personales es sumamente importante en cualquier institución y más aún en establecimientos de educación superior que manejan grandes cantidades de datos personales, el capítulo VII de la LOPDP determina a los responsables, las funciones y al delegado de protección de datos personales.

El artículo 47 de la LOPDP establece el conjunto de obligaciones que el integrante del sistema de protección de datos personales (responsable) debe seguir y llevar acabo para que su funcionamiento sea adecuado, según la ley existen 15 obligaciones que se deben

materializar, entre ellas destaca principalmente la función de cumplir y hacer cumplir lo que faculta la ley y sus principios básicos, de igual forma se debe demostrar que se cumplen con estas puntualizaciones de forma periódica, consecuentemente se obliga a contar con políticas internas que indique el manejo de los datos en la institución, seguidamente se establece que este representante debe analizar posibles riesgos por medio de evaluaciones de seguridad, que desencadenen el desarrollo de medidas prevención encargándose de notificar posibles incidentes a la autoridad directa. Mantienen la obligación de controlar la cantidad de datos que se piden o se guardan, se encarga de firmar acuerdos de confidencialidad, así como seleccionan con quien se asocian para proteger las bases de datos, se debe mantener una actualización constante de los protocolos de seguridad y en especial se debe designar un delegado de protección de datos para supervisar su cumplimiento internamente, debe aceptar la colaboración de auditorías con las autoridades de protección de datos (LOPDP, 2021).

La forma en que estos parámetros jurídicos se vinculan al funcionamiento de las instituciones de educación superior también se refleja en la evolución de la cultura institucional hacia una actualización con mejor desenvolvimiento técnico el cual involucra la anticipación de posibles ataques a los datos personales como forma preventiva desarrollada por parte de sus gestores hacia sus generadores, al expresar esta ideología se demuestra que en la actualidad se debe fortalecer la corresponsabilidad de los miembros activos del establecimiento en conjunto con sus autoridades o delegados de mantener el orden cuando se involucra el tratamiento de datos personales y más aún si se afectan derechos fundamentales que necesiten una tutela adecuada.

Se deben exigir procesos de control, monitoreo y evaluación de riesgos motivados en la normativa para que se impulse la modernización y adaptación a ciertos avances tecnológicos implementados irresponsablemente (uso de IA) sin antes haber realizado un estudio previo de aplicación y protección legal, las formas en las que se alcanzarían los resultados deseados es precisamente cumpliendo con aquellas obligaciones que la norma proporciona, como las capacitaciones hacia las propias autoridades, así como también a sus subordinados y demás miembros, para que se sienten bases sólidas de lo que es un modelo de gobernanza institucional que cumple con los estándares establecidos internacionalmente respecto a los datos personales.

En esta línea de análisis, el artículo 48 de la norma citada establece que se debe designar un delegado de protección de datos necesariamente para que se cumplan los estándares de

protección de cierta forma, el artículo enumera algunos casos en los que se debe contar con un delgado. Como es el caso de los organismos que forman parte del sector público esto incluye instituciones de educación superior y demás establecimientos que manejan grandes cantidades de datos, se ven en la necesidad de tratar datos y por ende controlarlos constantemente para brindarles seguridad y confianza en su funcionamiento, especialmente cuando su fundamento se centra en proteger la categorización de datos considerados como sensibles o especiales (LOPDP, 2021).

En lo que respecta a las funciones y atribuciones que el delegado debe cumplir la norma es exacta al detallar sus aspectos en el artículo 49 y 50 empezando por otorgarle roles estratégicos que lo reconozcan como un agente de gobernanza digital el cual oriente las formas de organización que respeten los derechos fundamentales de quienes confían en él, por medio de supervisiones formales que incluyan análisis de riesgos conjuntamente con sus posibles formas de manejo, siendo el pionero en cambiar el paradigma establecido cuando este se introduce como una figura equilibrada de conocimientos jurídicos, tecnológicos y administrativos que garanticen el equilibrio de la innovación demandada.

Esta necesidad se manifiesta de manera que las organizaciones educativas que pertenecen al sector público sean quienes comprenden que el derecho a la protección de datos no es un obstáculo de burocracia formal, sino es una respuesta básica para la legitimidad institucional por ser independientes y con acceso a recursos económicos suficientes que provienen del Estado, el poder legislativo a través del cuerpo legal busca evitar que las funciones de un delegado sean decorativas o subordinadas, ya que aseguran el peso en la toma de decisiones que respondan al ejercicio formal de derechos en un establecimiento universitario.

1.4.7 Autoridad de Protección de Datos Personales

El Reglamento de la LOPDP en su artículo 79 determina que su sede principal de operaciones será en el Distrito Metropolitano de Quito y la designación de quien funja como representante principal de este organismo supremo (SUPERINTENDENTE) será designado según la terna que el poder ejecutivo (PRESIDENTE) remita posteriormente a una evaluación previa que determine el cumplimento de los requisitos necesarios que se le exigen en el segundo inciso del artículo 77 de la LOPDP, una vez que su designación haya sido materializada su periodo de funcionamiento será de cinco años y deberá cumplir con lo que manda el artículo 80 del Reglamento a la LOPDP.

La autoridad máxima goza de autonomía administrativa, técnica, operativa y financiera pertenece a la Función de Transparencia y Control Social principalmente, se encarga de velar el cumplimiento a lo dispuesto en tratados internacionales, norma constitucional y la Ley Orgánica de Protección de Datos Personales en el Ecuador es el Superintendente de Protección de Datos, entre las funciones que se le otorgan son las realizar actuaciones previas que recaben información pertinente sobre procesos que hayan reflejado una posible irregularidad actuando de oficio o a petición de parte según lo establece el artículo 75 de la LOPDP.

Las instituciones de educación superior se encuentran bajo la vigilancia directa del órgano máximo en materia de protección de datos, su obligación jurídica de estar vinculadas conjuntamente equilibra la autonomía universitaria respecto a las funciones que sus encargados de tratar los datos tienen para proteger la intimidad y los datos personales que pertenecen a estudiantes, docentes, servidores públicos y trabajadores que presenten sus peticiones si se llegaran a sentir afectados por las formas de operación que la institución brinda.

El artículo 76 de la LOPDP introduce y establece las funciones que la autoridad máxima debe cumplir a nivel nacional, se puede concebir que su papel no se limita a sancionar únicamente a quienes incumplen las disposiciones que emiten o las inobservancias a la norma por parte de los integrantes del sistema de protección de datos personales, sino que además supervisa que tanto responsables como encargados del tratamiento de datos den seguimiento a los parámetros jurídicos que los envuelven, asumen la función de emitir normativas especializadas y de estricto cumplimiento para el sector público y privado, a su vez, supervisa las interacciones internacionales con los miembros activos del sistema con el objetivo de fortalecer los esquemas de seguridad y privacidad.

Su influencia en el contexto universitario es directa puesto que esta entidad que se encuentra subordinada al control de la Superintendencia por el constante flujo de información recopilada en sus diferentes sucursales, en materia de protección de datos deberán responder legalmente a los requerimientos de supervisión que la máxima autoridad plantea para sobrellevar un correcto funcionamiento del sistema digital con estándares de transparencia, responsabilidad y tutela efectiva de derechos hacia los miembros del sistema universitario.

1.4.8 La Autonomía Universitaria y la aplicación de la LOPDP

El avance tecnológico trae consigo consecuencias de carácter jurídico que cualquier administración pública debe desarrollar una vez que estas se ven incorporadas en su funcionamiento, en el caso de las instituciones de educación superior principalmente deben operar con transparencia ya que son el origen del conocimiento y de cambios sociales se ven involucradas en el manejo de nuevas tecnologías e información que se integran a su estructura funcional.

Los principios que se establecen en la Ley Orgánica de Protección de Datos Personales deben armonizar con la autonomía universitaria, sin embargo, la autonomía que se le otorga a esta institución pública no se debe de entender como una igualdad con la Ley para que su convivencia persista, sino que debe ser vista como una forma de subordinación por parte de la institución de educación superior ante un mandato que comprende la voluntad soberana de un pueblo.

Dentro de la organización funcional de una institución de educación superior es importante destacar el servicio que ofrecen a su comunidad cuando se permiten recolectar y almacenar grandes cantidades de datos que posteriormente son procesados para usarlos con determinados fines de comunicación y que fungen como información para la toma de decisiones académicas o administrativas, por lo que su operatividad es vista como un sistema que depende del flujo y la calidad de datos que se manejan (Arenas, 2020).

La autonomía universitaria se ve reconocida dentro del texto supremo, específicamente en el artículo 355 en el que se establece el régimen de libertades institucionales el cual garantiza y fortalece el ejercicio pleno de la misión universitaria, sin embargo, la autonomía no debe ser vista como un privilegio que está exentó de control y fiscalización, sino como un respaldo jurídico que orienta la protección de una libertad de catedra para producir nuevos conocimientos a través de las políticas que establece un autogobierno democrático y que a su vez responde a la transparencia de su actuar frente a la sociedad que le otorga confiabilidad al vincularse estrictamente con el desarrollo de perfiles profesionales, la autonomía no es absoluta pero si garantista.

De esta forma su operatividad responde automáticamente a las normas propias (Reglamentos y Estatutos) la cuales determinan su funcionamiento y que de esa manera respondan únicamente a fines educativos sin intromisión externa estas instituciones sostienen el objeto de que la información sea abierta y accesible, a pesar de este

razonamiento, se sabe que en gran parte deberían contar con filtros de protección que anonimicen cualquier dato sensible perteneciente a un miembro activo de la comunidad asegurándose que se respete el derecho a la protección de datos personales (Arenas, 2020).

El correcto desempeño de una institución educativa depende de múltiples factores que se interconectan entre sí, comprendiendo la calidad de educación hasta una gestión administrativa eficiente que toma en cuenta lo dictaminado legalmente. Esta obligación legal de asegurar la transparencia y a su vez la protección de datos personales conduce a que sus autoridades se vean en la necesidad de desarrollar políticas internas que respondan específicamente a la armonización entre los requerimientos que la ley los obliga a realizar y su autonomía funcional.

1.4.8.1 Política de Protección de Datos de la Universidad Técnica de Ambato

En cumplimiento de los parámetros jurídicos de la LOPDP, la Universidad Técnica de Ambato implementó una política de protección de datos personales que parcialmente le permite a esta entidad cumplir con los requerimientos y estándares establecidos para un correcto funcionamiento, en el que principalmente se garantiza una protección de datos personales comprendiendo a estudiantes que ya son miembros de la institución, postulantes que son quienes desean formar parte de la institución, servidores públicos y trabajadores que la integran e incluyendo a beneficiarios de relaciones institucionales (Univesidad Técnica de Ambato, 2025).

La política de protección de datos que tiene la Universidad Técnica de Ambato ofrece un limitado marco de análisis, dentro de sus puntualizaciones desarrolladas se demuestra un objeto, ámbito de aplicación, se nombra a los responsables del tratamiento de datos personales, principios y categorías de datos que se deben aplicar, su estructura establece una estructura general de medidas de seguridad incluyendo realizar evaluaciones periódicas de impacto, se mencionan pautas para el tratamiento de datos pertenecientes a sus miembros.

Al contrastar una política institucional con exigencias de la LOPDP se advierte que la normativa universitaria, aunque sea bien intencionada, todavía presenta vacíos operativos que deben ser corregidos en ciertos casos y en otros casos se deberían incluir con la finalidad de que se asegure un mayor cumplimiento a los estándares de protección de datos personales exigidos a medida que avanza el tiempo.

Puntualizando una de las exigencias de la LOPDP, principalmente en el artículo 47 numeral 12 se requiere que aquellos responsables del tratamiento de datos registren formalmente cada una de sus bases de datos en conjunto con la actividades desarrolladas ante el Registro Nacional de Protección de Datos (RNPD) de manera que se deben documentar las finalidades, las categorías de datos que se tratan, sus destinatarios, mecanismos de interconexión y medidas de seguridad que se deben aplicar generalmente a los datos identificados previamente, en el caso de la política desarrollada por la UTA se menciona generalizadamente estas actividades descritas, pero no se establece un proceso institucional concreto para que se garantice el registro de datos ni tampoco señala los mecanismos internos con los que se debe administrar.

Otro aspecto donde se evidencian los desajustes con la ley es en el ejercicio de derechos por parte de sus titulares (miembros de la institución), la política asigna un correo electrónico como un canal para presentar solicitudes que tengan que ver con protección de datos, sin embargo, la LOPDP exige que los responsables definan procedimientos claros en plazos concretos, pasos verificables que den seguimiento al requerimiento, así como formatos que aseguren una atención adecuada dentro del establecimiento, la UTA se expone a incumplimientos involuntarios por parte de la institución con su mero señalamiento de un canal de contacto, puesto que es insuficiente al exigir una estructura procedimental integral que garantice la satisfacción de requerimiento presentado en caso de que su titular requiera acceder, rectificar, eliminar, oponerse al tratamiento de datos.

Continuando con el análisis, la LOPDP en sus articulados 40 y 42 en materia de evaluaciones de impacto establece su proceder, la política alude la necesidad de realizarlas, pero no desarrolla cómo se deben ejecutar ni tampoco se menciona qué metodología se aplicará dentro de la institución, ni cuáles actividades requieren obligatoriamente una evaluación o quiénes son los encargados de elaborarla y mucho menos su periodicidad. Este vacío es crítico, considerando que la institución trabaja con grandes volúmenes de datos sensibles pertenecientes a estudiantes, docentes, personal administrativo y demás actores que se involucran directamente con el establecimiento.

A partir de este análisis crítico, se vuelve evidente que la sola existencia de una política, aunque necesaria, no es suficiente para cumplir con los requerimientos exigidos por la LOPDP, el entorno universitario debe avanzar hacia una cultura que implemente mecanismos adicionales los cuales consoliden una mejor estructura de protección de datos qué gestionen de manera eficiente los derechos de los titulares. Esta transformación exige

que el entorno universitario y en general aquellas entidades que almacenan datos dejen de concebir a la protección de datos como un documento formal o un mandato normativo únicamente, y que se la integre como un proceso necesario que anticipe las posibles problemáticas de funcionalidad y vulneración de derechos.

1.5.- OBJETIVOS

1.5.1 Objetivo General

Investigar la incidencia de la Ley de Protección de Datos en el entorno Universitario.

1.5.2 Objetivos Específicos

- Analizar los parámetros jurídicos de la Ley de Protección de Datos Personales que han sido adoptados en el entorno Universitario.
- Describir los principales aspectos jurídicos respecto de la Ley de Protección de Datos Personales que podrían ser considerados en el entorno Universitario
- Establecer los desafíos de la Ley de Protección de Datos Personales en el entorno Universitario.

1.5.3 Pregunta de Investigación

¿De qué manera incide la Ley de Protección de Datos en el entorno Universitario?

CAPÍTULO II

METODOLOGÍA

2.1 Tipo de Investigación

El presente estudio se enmarca en un enfoque cualitativo, en palabras de Fernández et al. (2014), es un estudio que busca comprender una realidad social basada en la interpretación de experiencias y documentos de manera que captan la complejidad del problema en estudio, por lo tanto esta investigación se orienta a comprender como la protección de datos mantiene su incidencia en el entorno universitario, tomando como punto de partida la experiencia y la percepción de actores que se encuentran vinculados directamente a la toma de decisiones respecto a la problemática.

2.1.1 Diseño

La presente investigación es de diseño no experimental y de campo, no experimental porque no existe la manipulación de variables en la investigación, de campo ya que la información principal fue obtenida directamente de los actores involucrados en su entorno, es decir dentro del contexto universitario donde se desarrolla el fenómeno estudiado. Además, es importante mencionar que también es de tipo transversal porque la recolección de datos se realizó en un solo momento temporal sin hacer seguimientos ni mediciones a lo largo del estudio.

2.1.2 Alcance

La investigación es de tipo exploratoria y también descriptivo porque cumple simultáneamente dos propósitos metodológicos; es exploratoria porque estudia el fenómeno de incidencia de la normativa dentro del entorno universitario que ha sido poco estudiado localmente, así como, existe pocas investigaciones respecto a cómo las instituciones educativas gestionan los datos internamente a la vez se buscó identificar parámetros jurídicos y desacuerdos entre la normativa con la aplicación.

Es descriptiva porque su objetivo general es investigar la incidencia la ley de protección de datos personales en el entorno universitario sin que se manipulen variables, ya que el análisis se centra entre lo que la normativa plantea y aquello que se emplea en el contexto institucional, exponiendo y comprendiendo como el problema se encuentra actualmente.

2.2 Métodos de investigación

2.2.2 Método Documental

Es documental porque se analizó documentos científicos relacionados a la temática, cuerpos legales de protección de datos personales y una política institucional que construye una base conceptual de la investigación.

2.2.3. Método Analítico y Descriptivo

Es analítico y descriptivo porque se examinó la información obtenida en la entrevista que se relacionan con los documentos científicos los cuales describen e identifican agrupaciones conceptuales, patrones reiterativos e información relevante.

2.2.4. Técnicas e Instrumentos

Se utilizó la técnica de la entrevista semiestructura aplicada conocedores del fenómeno estudiado a través de sus campos de conocimiento en el marco de protección de datos personales y que son miembros activos de la institución de educación superior.

La entrevista estuvo formada por ocho preguntas que contenían una relación directa con el objetivo general y los objetivos específicos, los entrevistados respondieron las siguientes preguntas:

1. ¿Cómo considera usted que la Ley Orgánica de Protección de Datos Personales (LOPDP) está incidiendo en el manejo de la información en la institución de educación superior que usted trabaja?

2. ¿De qué manera la institución en la que usted trabaja ha comenzado a adaptar en su norma interna, procedimientos que den cumplimiento a las disposiciones de la Ley Orgánica de Protección de Datos Personales (LOPDP)?

3. ¿Qué aspectos jurídicos de la Ley Orgánica de Protección de Datos Personales considera que todavía no han sido suficientemente desarrollados o comprendidos en la institución en la que usted trabaja?

4. Desde su experiencia, ¿cree que las políticas institucionales del establecimiento en el que usted trabaja reflejan adecuadamente los principios de la Ley, como el consentimiento o la finalidad? ¿Por qué?

5. ¿Describa cómo la institución en la que usted trabaja gestiona el cumplimiento y la comunicación de sus obligaciones ante la Superintendencia de Protección de Datos Personales?

6. Considerando la estructura organizacional de una universidad, ¿Qué políticas técnicas administrativas debería implementar las instituciones de educación superior para asegurar el cumplimiento de principios que operan el tratamiento de datos personales?

7. ¿Cómo actúa la institución en la que usted trabaja frente a denuncias o reportes de presuntos incumplimientos a la Ley de Protección de Datos Personales?

8. ¿Qué acciones está implementando la institución en la que usted trabaja para evolucionar hacia una verdadera cultura institucional de respeto a la privacidad y protección de los datos personales de toda su comunidad?

5. Población y Muestra

La población utilizada correspondió a un muestreo no probabilístico por conveniencia debido a que se integraron a los sujetos disponibles que podían aportar información relevante sobre la protección de datos en el entorno universitario.

5.1 Criterios de inclusión y exclusión

Los criterios de inclusión son:

- Experticia verificable,
- vinculación institucional,
- experiencia mínima en áreas relacionadas,
- disponibilidad y consentimiento

Los criterios exclusión son:

- falta de experticia,
- vinculación indirecta,
- indisponibilidad,
- conflicto de intereses e
- información insuficiente

5.2 Consentimiento

En el consentimiento informado se explicó el objetivo de la investigación y otros puntos importantes como:

1. Propósito del estudio
2. Naturaleza de la participación
3. Voluntariedad
4. Confidencialidad y anonimato
5. Riesgos

6. Uso de la información

7. Derecho a realizar preguntas

8. Declaración de consentimiento que decía textualmente:

"Declaro que he leído y comprendido la información anterior; que se le ha explicado el propósito del estudio y la naturaleza de mi participación; se me garantiza confidencialidad y voluntariedad; autorizo participar en esta investigación de manera libre y consiente".

CAPÍTULO III

3.1 Resultados y Discusión

3.1.1 Análisis y discusión de los resultados

En este capítulo se expondrá la reproducción de conocimientos recopilados en las respuestas obtenidas a través de las entrevistas realizadas a los conocedores de la materia quienes son especialistas en materia legal y que ocupan cargos relacionados al tema de estudio conforme el tamaño de la muestra a conveniencia que atentamente manifestaron su experiencia. Igualmente, la información recopilada será procesada indicando únicamente lo pertinente que sustenta los conceptos desglosados previamente en la doctrina y los requerimientos legales que se incorporan en los cuerpos normativos, para concluir con el análisis e interpretación correspondiente de resultados investigativos.

Los colaboradores que fueron entrevistados brindaron la facilidad de ser contactados de forma presencial e incluso virtual en ciertos casos, esta flexibilidad minimizó las barreras de acceso a la información, a los entrevistados se les proporciono la guía de entrevista con la finalidad de que sus conocimientos previos de la materia sean de calidad impidiendo que sus respuestas sean una simple opinión con un recuerdo vago de sus conocimientos.

Las tablas a continuación reflejan un análisis de las respuestas brindadas por los expertos, se realizó un análisis de cada experto para encontrar similitudes y coincidencias.

Tabla 2

Entrevista Pregunta 1

Pregunta	**Resultados**

1. ¿Cómo considera usted que la Ley Orgánica de Protección de Datos Personales (LOPDP) está incidiendo en el manejo de la información en la institución de educación superior que usted trabaja?	Los expertos reconocieron que la LOPDP fue un detonante para cambios internos de su institución, coincidiendo que se encuentran en una etapa de transición y adecuación, no obstante, N1 y N2 difieren del criterio empleado por N3 respecto a la profundidad del impacto en sus instituciones fue parcial, N3 menciona una variable que se relaciona con la limitación de recursos técnicos y económicos de la institución.

Referencia: *Información obtenida de los instrumentos de entrevista aplicadas a destacados profesionales en el área de derecho en el Ecuador, respuestas que fueron agrupadas en la tabla.*

Elaborado por: *Merino (2025)*

Análisis:

En la tabla 2 que corresponde a la pregunta 1 los expertos coinciden que en sus instituciones se encuentran adaptando los parámetros jurídicos de la LOPD, sin embargo, su operatividad se encuentra limitada puesto que los ajustes normativos y técnicos seguirán siendo un proceso gradual y adaptativo conforme se le dé la importancia correspondiente por sus máximas autoridades.

Conclusión:

Aunque los expertos coinciden en que la LOPDP ha impulsado transformaciones internas y ha situado a las instituciones en una fase de transición y adecuación, persisten diferencias en la valoración de su impacto real. Mientras N1 y N2 consideran que los avances han sido parciales, N3 atribuye esta limitación a la insuficiencia de recursos técnicos y económicos. En conjunto, esto demuestra que la implementación de la normativa avanza, pero enfrenta barreras estructurales que impiden su consolidación plena. Su implementación práctica sigue siendo un proceso gradual e incompleto para todas las instituciones.

Tabla 3

Entrevista pregunta 2

Pregunta	Resultados
2. ¿De qué manera la institución en la que usted trabaja ha comenzado a adaptar en su norma interna, procedimientos que den cumplimiento a las disposiciones de la Ley Orgánica de Protección de Datos Personales (LOPDP)?	Los expertos indican que la adaptación de LOPDP en la institución se encuentra en una fase incompleta ya que las instituciones se encuentran en etapas preliminares, N1 y N2 coinciden que los mecanismos de sus instituciones no logran materializar una ejecución efectiva internamente ya que están dando sus primeros pasos, mientras que N3 indica que en su institución la toma de decisiones en materia de protección de datos se retrasa por la dependencia aprobatoria de procedimientos que funcionen internamente.

Referencia: *Información obtenida de los instrumentos de entrevista aplicadas a destacados profesionales en el área de derecho en el Ecuador, respuestas que fueron agrupadas en la tabla.*

Elaborado por: *Merino (2025)*

Análisis:

En la tabla 3 que corresponde a la pregunta 2 los expertos coinciden que en sus instituciones se encuentran en una fase incompleta de adaptación, han dado los primeros pasos para establecer directrices claras sobre el tratamiento lícito internamente, en el caso específico de una entidad Universitaria se cuenta con una limitación en la toma de decisiones respecto a la protección de datos puesto que sus autoridades no le dan la importancia suficiente para aprobar estos mecanismos de protección.

Conclusión:

La adaptación de la LOPDP en las instituciones analizadas permanece en un estado inicial, reflejado en la falta de mecanismos efectivos y en la prevalencia de procesos preliminares.

En conjunto, el panorama revela una implementación fragmentada y lenta, donde la protección de datos aún no se integra plenamente en la gestión institucional.

Tabla 4

Entrevista pregunta 3

Pregunta	Resultados
3. ¿Qué aspectos jurídicos de la Ley Orgánica de Protección de Datos Personales considera que todavía no han sido suficientemente desarrollados o comprendidos en la institución en la que usted trabaja?	Los expertos comparten el criterio de que la aplicación de la LOPDP es deficiente debido a la limitada comprensión técnica y jurídica, por su parte N1 advierte que las instituciones desconocen el principio de responsabilidad proactiva y por ende operan de forma reactiva, N2 indico que el gestionamiento de procesos básicos de tratamiento de datos tiene falencias en procesos básicos de recolección, por último, N3 enfatiza en la obsolescencia institucional de respuesta e implementación de mecanismos jurídicos a los avances tecnológicos como la IA.

Referencia: *Información obtenida de los instrumentos de entrevista aplicadas a destacados profesionales en el área de derecho en el Ecuador, respuestas que fueron agrupadas en la tabla.*

Elaborado por: *Merino (2025)*

Análisis:

En la tabla 4 que corresponde a la pregunta 3 los expertos confirman que el cumplimiento de las obligaciones legales es parcializado debido a la limitada comprensión del marco jurídico y técnico que envuelve a la protección de datos personales, incluso se muestra vulnerable ante el continuo avance e implementación de avances tecnológicos como la IA.

Conclusión:

La deficiente aplicación de la LOPDP responde a una comprensión técnica y jurídica insuficiente que atraviesa a todas las instituciones analizadas. N1 evidencia que la falta de responsabilidad proactiva mantiene a las universidades en un modelo reactivo; N2 muestra fallas estructurales incluso en procesos básicos de recolección y tratamiento; y N3 expone

la incapacidad institucional para responder a los avances tecnológicos, especialmente a la IA.

Tabla 5

Entrevista pregunta 4

Pregunta	Resultados
4. Desde su experiencia, ¿cree que las políticas institucionales del establecimiento en el que usted trabaja reflejan adecuadamente los principios de la Ley, como el consentimiento o la finalidad? ¿Por qué?	Los expertos coinciden en que las políticas universitarias no reflejan los principios en la práctica de aplicación, N1 advierte que el principio de consentimiento es un formalismo sin validez permitiendo el desleal uso de datos, N2 señala que la aplicación de principio únicamente ha sido plasmada en documentos pero no en su aplicación real y N3 afirma que las políticas se corrigen sobre la marcha y el pasar del tiempo.

Referencia: *Información obtenida de los instrumentos de entrevista aplicadas a destacados profesionales en el área de derecho en el Ecuador, respuestas que fueron agrupadas en la tabla.*

Elaborado por: *Merino (2025)*

Análisis:

En la tabla 5 que corresponde a la pregunta 4 los expertos coinciden en que en sus instituciones no reflejan plenamente aplicación de principios básicos como el consentimiento, advierten que de cierta forma el desarrollo de una política de protección de datos es débil y se limita a ser un formalismo para no ser sancionado por el ente de control por incumplir con lo establecido en la norma, por último, se evidencia la falta de un enfoque preventivo a posibles vulneraciones.

Conclusión:

Las instituciones universitarias muestran una aplicación insuficiente de los principios de la LOPDP, pues las políticas existentes no se traducen en prácticas efectivas. N1 evidencia

que el consentimiento se reduce a un formalismo sin validez real; N2 confirma que los principios se limitan a documentos sin operatividad concreta; y N3 revela que las políticas se ajustan de forma improvisada, sin un enfoque preventivo.

Tabla 6

Entrevista pregunta 5

Preguntas	**Resultados**
5. ¿Describa cómo la institución en la que usted trabaja gestiona el cumplimiento y la comunicación de sus obligaciones ante la Superintendencia de Protección de Datos Personales?	Las instituciones no cuentan con procedimientos claros ni con mecanismos formales para gestionar el cumplimiento y la comunicación de sus obligaciones ante la Superintendencia de Protección de Datos Personales, evidenciando una carencia de seguridad, estructura y control en materia de protección de datos.

Referencia: *Información obtenida de los instrumentos de entrevista aplicadas a destacados profesionales en el área de derecho en el Ecuador, respuestas que fueron agrupadas en la tabla.*

Elaborado por: *Merino (2025)*

Análisis:

En la tabla 6 que corresponde a la pregunta 5 los expertos coinciden que en sus instituciones carecen de procedimientos formales que permitan articular el cumplimiento y la comunicación con los entes de control como la SPDP por lo que se crea un escenario de riesgo normativo.

Conclusión:

Persiste una insuficiencia evidente en la seguridad destinada a la protección de datos, lo que demuestra que las instituciones aún no cuentan con mecanismos técnicos ni organizativos capaces de garantizar un tratamiento adecuado y confiable.

Tabla 7

Entrevista pregunta 6

Preguntas	Resultados
6. Considerando la estructura organizacional de una universidad, ¿Qué políticas técnicas administrativas debería implementar las instituciones de educación superior para asegurar el cumplimiento de principios que operan el tratamiento de datos personales?	Existe una evidente insuficiencia en las políticas técnicas y administrativas destinadas a garantizar la seguridad en la protección de datos, lo que demuestra que las instituciones de educación superior aún no cuentan con mecanismos sólidos para asegurar el cumplimiento efectivo de los principios que regulan el tratamiento de datos personales.

Referencia: *Información obtenida de los instrumentos de entrevista aplicadas a destacados profesionales en el área de derecho en el Ecuador, respuestas que fueron agrupadas en la tabla.*

Elaborado por: *Merino (2025)*

Análisis:

En la tabla 7 que corresponde a la pregunta 6 los expertos señalan que carecen de políticas técnicas y administrativas que permitan un cumplimiento de principios de tratamiento con el debido tratamiento operativo, por lo que se refleja una necesidad urgente de construir un marco integral de políticas que fortalezcan la seguridad y la administración del ciclo de vida de los datos que se almacenan internamente.

Conclusión:

La falta de políticas técnicas y administrativas robustas refleja que las instituciones de educación superior aún no han consolidado un sistema integral de protección de datos personales.

Tabla 8

Entrevista pregunta 7

Preguntas	Resultados
7. ¿Cómo actúa la institución en la que usted trabaja frente a denuncias o reportes	Se coincide que las instituciones carecen de un sistema adecuado para gestionar denuncias o reportes de presuntos

de presuntos incumplimientos a la Ley de Protección de Datos Personales?	incumplimientos a la Ley de Protección de Datos Personales, lo que evidencia una ausencia de mecanismos de seguridad y protocolos efectivos que garanticen una respuesta oportuna y conforme a la normativa vigente.

Referencia: *Información obtenida de los instrumentos de entrevista aplicadas a destacados profesionales en el área de derecho en el Ecuador, respuestas que fueron agrupadas en la tabla.*

Elaborado por: *Merino (2025)*

Análisis:

En la tabla 8 que corresponde a la pregunta 7 los expertos señalan que el sistema de gestión de incidentes es deficiente, pues carecen de infraestructura técnica y organizativa lo cual compromete la aplicación de principios legales.

Conclusión:

La ausencia de un sistema institucional para gestionar denuncias o reportes de incumplimientos a la LOPDP revela una debilidad estructural en la protección de datos. Esta carencia impide respuestas oportunas y adecuadas, compromete el cumplimiento normativo y expone a las instituciones a riesgos operativos y sancionatorios.

Tabla 9

Entrevista pregunta 8

Preguntas	**Resultados**
8. ¿Qué acciones está implementando la institución en la que usted trabaja para evolucionar hacia una verdadera cultura institucional de respeto a la privacidad y protección de los datos personales de toda su comunidad?	Coinciden en que la institución no está implementando acciones suficientes para construir una verdadera cultura de respeto a la privacidad, evidenciándose una falta de seguridad y de medidas efectivas que fortalezcan la protección de datos personales dentro de la comunidad universitaria.

Referencia: *Información obtenida de los instrumentos de entrevista aplicadas a destacados profesionales en el área de derecho en el Ecuador, respuestas que fueron agrupadas en la tabla.*

Elaborado por: *Merino (2025)*

Análisis:

En la tabla 9 que corresponde a la pregunta 8 en conjunto muestran que las instituciones permanecen en una fase de desarrollo, dejando en evidencia que no poseen políticas culturales y operativas que consoliden un entorno de respeto y responsabilidad al tratamiento de datos personales por lo que se debe seguir trabajando para que se integren procesos seguros y respetuosos a los datos personales.

Conclusión:

La ausencia de acciones concretas para fortalecer una cultura institucional de respeto a la privacidad confirma que la protección de datos aún no es una prioridad efectiva dentro de las universidades.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

La LOPDP ha generado un impacto evidente en las instituciones de educación superior, pero su incidencia es principalmente formal y aún no se traduce en una implementación sólida de tratamiento de datos. Los expertos coinciden en que las universidades atraviesan una etapa de transición caracterizada por ajustes parciales, limitada comprensión jurídica y técnica, ausencia de políticas sólidas, y carencias estructurales en seguridad, gestión de denuncias y cultura institucional. La falta de recursos, de liderazgo directivo y de mecanismos operativos ha impedido que la normativa se consolide en la práctica, manteniendo a las instituciones en un modelo reactivo y de cumplimiento mínimo.

Los parámetros jurídicos han sido incorporados de manera fragmentada e incompleta. Los expertos revelan que principios como consentimiento, finalidad, seguridad y responsabilidad proactiva no se aplican adecuadamente en la práctica, existiendo un

desfase entre la normativa y su operacionalización. Las instituciones se limitan a documentos o avisos formales sin mecanismos que garanticen su cumplimiento real, lo que evidencia una débil interiorización de los principios de la ley.

Los expertos coinciden en que aspectos esenciales como la responsabilidad proactiva, la recolección lícita de datos, el consentimiento válido, la seguridad de la información y la gestión de riesgos no han sido comprendidos ni desarrollados plenamente. Las instituciones operan con desconocimiento técnico, procesos improvisados y estructuras obsoletas que dificultan la aplicación real de los aspectos jurídicos más relevantes de la LOPDP.

Los principales desafíos identificados son estructurales y operativos: falta de políticas robustas, ausencia de sistemas de gestión de denuncias, insuficiencia de recursos técnicos y económicos, debilidad en la cultura de privacidad, políticas reactivas, decisiones institucionales demoradas y falta de mecanismos preventivos frente a riesgos tecnológicos, especialmente los asociados a la IA. En conjunto, estos desafíos impiden consolidar una protección de datos efectiva.

4.2 Recomendaciones

Se recomienda fortalecer la gobernanza institucional en materia de protección de datos mediante la creación de unidades técnicas especializadas, asignación de recursos, adopción de políticas integrales y estandarización de procesos de cumplimiento. Además, es necesario promover una cultura institucional de protección de datos basada en formación continua, responsabilidad proactiva y mecanismos preventivos que permitan materializar la LOPDP más allá del formalismo documental.

Para fortalecer los parámetros jurídicos, es necesario desarrollar una coordinación entre las áreas jurídicas, técnicas y administrativas de la institución de educación para garantizar procesos que otorguen herramientas operativas accesibles para los miembros de la institución, lo que implica guías internas redactadas en un lenguaje sencillo y de fácil interpretación para los actores de la comunidad universitaria permitiéndoles acceder fácilmente a los derechos que la LOPDP les faculta.

Se recomienda que las universidades revisen integralmente sus instrumentos normativos internos, asegurando que los principios de la LOPDP se traduzcan en procedimientos verificables, mecanismos de control, registros actualizados y medidas técnicas que

permitan demostrar cumplimiento. Es indispensable adoptar políticas claras, actualizadas y con enfoque preventivo, acompañadas de capacitación obligatoria para quienes realizan tratamiento de datos.

Las universidades deben priorizar la implementación de programas de formación jurídica y técnica sobre la LOPDP, diseñar manuales internos que establezcan responsabilidades claras y desarrollar protocolos que permitan gestionar adecuadamente el ciclo de vida del dato. Se sugiere también incorporar auditorías internas periódicas que evalúen el cumplimiento de los aspectos jurídicos fundamentales.

Las instituciones deben adoptar un enfoque estratégico basado en la planificación a mediano y largo plazo, priorizando la inversión en tecnología, talento humano y herramientas de gestión. Además, deben implementarse sistemas formales para la recepción y atención de denuncias, desarrollar políticas de seguridad de la información, y establecer modelos de gobernanza digital que respondan a los avances tecnológicos y a las exigencias normativas.

MATERIALES DE REFERENCIA

Referencias bibliográficas utilizadas en el presente trabajo:

Álvarez, G. (2002). *Metodología de la investigación jurídica: hacia una nueva perspectiva.* Santiago de Chile: Universidad Central de Chile.

Álvarez, J. (2021). Inteligencia Artificial, derecho administrativo y protección de datos personales. Entre la dignidad de la persona y la eficacia administrativa. *Ius et Scientia*, 304-326. Obtenido de https://revistascientificas.us.es/index.php/ies/article/download/16146/15167

Álvarez, J., & Hernández, G. (2024). Protección de Datos Personales en Plataformas Educativas Digitales en el Sistema de Educación Superior de Ecuador. *Journal Scientific MQRInvestigar*, 5324-5339. doi:https://doi.org/10.56048/MQR20225.8.3.2024.5324-5339

Álzate, J. (2016). *Análisis de la ley colombiana de protección de datos.* Medellin: Andigraf.

Arenas, M. (2020). Transparencia y protección de datos personales en el ámbito universitario: hacia una universidad abierta. *Revista CEFLegal*, 93-120. Obtenido de https://revistas.cef.udima.es/index.php/ceflegal/article/download/9667/9395

Asamblea Constituyente de Portugal. (1976). *Constitución de la Republica Portuguesa.* Diário da República. Obtenido de https://www.parlamento.pt/Legislacao/Paginas/constituicaorepublicaportuguesa.aspx

Asamblea General de las Naciones Unidas. (1948). *Declaración Universal de los Derechos Humanos.* Naciones Unidas. Obtenido de https://www.un.org/es/about-us/universal-declaration-of-human-rights

Asamblea General de las Naciones Unidas. (1990). *Principios rectores para la reglamentación de los ficheros computadorizados de datos personales.* Naciones Unidas. Obtenido de https://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf

Asamblea General de las Naciones Unidas. (1996). *Pacto Internacional de Derechos Civiles y Políticos.* Naciones Unidas. Obtenido de

https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Asamblea Nacional del Ecuador. (2005). *Código Civil.* Quito: Registro Oficial 506. Obtenido de https://www.asambleanacional.gob.ec/sites/default/files/shop/documentos_legislativos/codigo_civil_1.pdf

Asamblea Nacional del Ecuador. (2016). *Protocolo de Adhesión del Ecuador al Acuerdo Comercial entre la Unión Europea y sus Estados Miembros, por una parte, y Colombia y el Perú, por otra.* Registro Oficial. Obtenido de https://www.produccion.gob.ec/acuerdo-comercial-ecuador-union-europea/

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales.* Quito: Registro Oficial. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Asamblea Nacional del Ecuador. (2024). *Código Civil.* Quito: Registro Oficial Suplemento 46. Obtenido de https://www.asambleanacional.gob.ec/sites/default/files/shop/documentos_legislativos/codigo_civil_1.pdf

Astudillo, P., Once, V., Alvarado, L., & García, H. (2024). Aplicación de la Ley Orgánica de Protección de Datos Personalesen el sistema empresarial privado ecuatoriano. *Revista Lex, 7*(25), 567-582. doi:https://doi.org/10.33996/revistalex.v7i25.201

Ávila, C. (2019). El Derecho a la intimidad y la protección de datos personales en el marco jurídico ecuatoriano. *Tesis.* Universidad Central del Ecuador, Quito. Obtenido de http://www. dspace. uce. edu. ec/bitstream/25000/23527/1/UCE-FJCPS-CD-Avila% 20Christian. pdf)

Barrantes, R. (2021). *Investigación: un camino al conocimiento.* Editorial UNED. Obtenido de https://www.academia.edu/38766459/Investigacion_un_camino_al_conocimiento_Barrantes_Echavarr%C3%ada

Bascuñan, A. (1971). *Manual de técnica de la investigación jurídica* (Cuarta ed.). Santiago de Chile: Editorial Jurídica de Chile.

Bastidas, J. (2019). Fundamentos para la redacción de objetivos en los trabajos de investigación de pregrado. *Mextesol*. Obtenido de https://www.mextesol.net/journal/index.php/journal/article/view/1090

Betancour, V. (2018). *Protección de Datos Personales.* Quito: Universidad Andina.

Cabezas, E., Andrade, D., & Torres, J. (2018). *Introducción a la metodología de la investigación científica.* Universidad de las Fuerzas Armadas: Sangolquí. Obtenido de https://unimetonline.aiemcr.co.cr/pluginfile.php/3057/mod_data/content/59/Introduccion%20a%20la%20Metodologia%20de%20la%20investigacion%20cientifica.pdf

Carvajal, R. (2020). *Metodología de la Investigación: investigación bibliográfica/documental.* ULADECH. Obtenido de https://repositorio.uladech.edu.pe/handle/20.500.13032/19082

Comité Jurídico Interamericano. (2012). *Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas.* Organización de los Estados Americanos. Obtenido de http://www.oas.org/es/sla/cji/docs/CJI-RES_186_LXXX-O-12.pdf

Comité Jurídico Interamericano. (2015). *Guía Legislativa sobre la Privacidad y la Protección de Datos Personales en las Américas.* Organización de los Estados Americanos. Obtenido de http://www.oas.org/es/sla/cji/docs/CJI-RES_212_LXXXVI-O-15.pdf

Conde, C. (2005). *La protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad.* Cádiz: Servicio de Publicaciones de la Universidad de Cádiz. Obtenido de https://rodin.uca.es/handle/10498/26396

Consejo de Derechos Humanos. (2015). *El derecho a la privacidad en la era digital.* Naciones Unidas. Obtenido de https://undocs.org/es/A/HRC/RES/28/16

Consejo Superior de la Judicatura. (2021). *Manual de metodología de investigación jurídica para la práctica judicial en la Escuela Judicial "Rodrigo Lara Bonilla".* Escuela Judicial Rodrigo Lara Bonilla. Obtenido de https://www.ramajudicial.gov.co

Constante, E. (2024). Medidas de seguridad para la protección de datos sensibles de estudiantes y ex estudiantes de Uniandes. *Tesis de Maestría.* Universidad Regional Autónoma de los Andes, Ambato. Obtenido de https://dspace.uniandes.edu.ec/handle/123456789/18751

Cooley, T. (1879). *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract.* Chicago: Callaghan and Company.

Cordero, S. (2023). Protección jurídica, habeas data y la Ley Orgánica de Protección de Datos Personales frente a la autodeterminación informática y la protección de datos personales. *Tesis.* Universidad de Cuenca, Cuenca. Obtenido de http://dspace.ucuenca.edu.ec/handle/123456789/43392

Cortes Generales. (1978). *Constitución Española.* Madrid: Boletín Oficial del Estado. Obtenido de https://www.boe.es/legislacion/documentos/ConstitucionES.pdf

De la Calle, J., & Blanco, E. (2015). *Metodología de la investigación jurídica.* Ecuador: CEP. Obtenido de https://gc.scalahed.com/recursos/files/r161r/w25442w/Metodologia_de_la_investigacion_juridica.pdf

Díaz, D. (2023). Transparencia y protección de datos personales en el ámbito universitario: ¿avance o retroceso? *Revista Española de la Transparencia*, 201-224. doi:https://doi.org/10.51915/ret.311

Díaz, G., & Fonseca, M. J. (2019). Vulneración al derecho de la intimidad y privacidad por el indebido tratamiento de datos personales en el Ecuador. *Tesis.* Universidad Católica de Santiago de Guayaquil, Guayaquil. Obtenido de http://repositorio.ucsg.edu.ec/handle/3317/13108

Díaz, M. (2011). El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego. *Teoría y Realidad Constitucional*, 279-312. Obtenido de https://revistas-pre.uned.es/index.php/TRC/article/download/6960/6658

Dozo, D., & Martínez, P. (2017). *Glosario Iberoamericano de Protección de Datos.* Madrid: XVII Premios Proteccion de Datos Personales.

Fernández, C., Baptista, M. d., & Hernández, R. (2014). *Metología de la Investigación* (Sexta ed.). México D.F: McGraw-Hill. Obtenido de https://bida.uclv.edu.cu/bitstream/handle/123456789/10917/Metodolog%C3%ADa%20de%20la%20Investigaci%C3%B3n.%20Sampieri%206ta%20edici%C3%B3n.pdf?sequence=1&isAllowed=y

Fernández, J., Casal, L., Fernández, J., Fernández, C., & Cebreiro, B. (2022). Protección de datos personales en la universidad: hábitos, actitudes y conocimiento del profesorado. *Profesorado, Revista De Currículum Y Formación Del Profesorado, 26*(3), 337-352. doi:https://doi.org/10.30827/profesorado.v26i3.21193

Flores, J., Juiña, C., Nacimba, D., Tandalla, F., & Guanoquiza, A. (2025). Auditoría de controles de cifrado y protección de la información. *Ciencia Latina Revista Científica Multidisciplinar, 9*(2), 423-433. doi:https://doi.org/10.37811/cl_rcm.v9i2.16856

Gacitúa, A. (2014). El derecho fundamental a la protección de datos personales en el ámbito de la prevención y represión penal europea (en busca del equilibrio entre la libertad y la seguridad). *Tesis Doctoral.* Universidad Autónoma de Barcelona, Barcelona. Obtenido de https://www.tesisenred.net/handle/10803/132147

Gallo, G. (2008). *La protección de datos personales.* Madrid: Legister.

González, D. (2021). Los datos personales en la web: intervención de los poderes públicos. *Tesis Doctoral.* Universidad de Oviedo, Oviedo. Obtenido de https://digibuo.uniovi.es/dspace/bitstream/handle/10651/61352/TD_DianaPaolaGonzalezMendoza.pdf?sequence=2

Guerrero, B. (2020). Protección de datos personales en el Poder Judicial: Una nueva mirada al principio de publicidad de las actuaciones judiciales. *Revista chilena de derecho y tecnología, 9*(2), 33-56. doi:https://doi.org/10.5354/0719-2584.2020.54372

Hernández, J. (2025). Protección de datos, intimidad y acceso a la información pública. Ponderación y proporcionalidad. *Revista Canaria de Administración Pública*(5), 73-105. doi:https://doi.org/10.36151/RCAP.5.4

Herrán, A. (2003). *El derecho a la protección de datos personales en la sociedad de la información.* Bilbao: Universidad de Deusto.

Honorable Congreso de la Nación Argentina. (1933). *Régimen Legal de la Propiedad Intelectual (Ley 11.723).* Boletín Oficial de la República Argentina. Obtenido de https://www.argentina.gob.ar/normativa/nacional/ley-11723-42755/texto

Lasso, L., Franco, D., & Estrada, R. (2022). Aplicaciones de la Datificación y Big Data en América Latina entre el 2015 y 2019. *Revista Logos Ciencia & Tecnología, 14*(2), 125-143. doi:https://doi.org/10.22335/rlct.v14i2.1594

Marín, T. (2007). Derecho al honor, personas jurídicas y tribunal constitucional. *InDret*. Obtenido de https://www.raco.cat/index.php/InDret/article/download/78728/102804

Monereo, J. (2025). Deber de información del uso de dispositivos de vigilancia y sistema de garantías de los derechos a la protección de datos personales y derechos digitales. De nuevo sobre la prueba de videovigilancia. *REVISTA DE JURISPRUDENCIA LABORAL*(3), 1-17. doi:https://doi.org/10.55104/RJL_00623

Morales, J. (2016). *Tus Derechos: El Derecho a la intimidad.* Lima: Universidad Nacional de San Marcos.

Morles, V. (1971). *Guía para la elaboración y evaluación de proyectos de investigación.* Bogotá: Instituto Colombiano de Pedagogía.

Muñoz, A., Modragón, L., Duro, E., Rueda, L., & Sorokin, P. (2023). Protección de datos de salud: el reto de la armonización legislativa en América Latina. *Revista del Cuerpo Médico Hospital Nacional Almanzor Aguinaga Asenjo*. doi:https://doi.org/10.35434/rcmhnaaa.2023.162.1886

Naranjo, L. (2017). El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador. *Foro: Revista de Derecho*, 63-82. Obtenido de http://scielo.senescyt.gob.ec/scielo.php?pid=S2631-24842017000100063&script=sci_arttext

Nieves, Y., & Ponjuan, G. (2021). Tratamiento de datos personales y acceso a la información. Visiones a partir de la academia. *Universitas-XXI, Revista de Ciencias Sociales y Humanas*, 167-185. doi:https://doi.org/10.17163/uni.n35.2021.08

Nogueira, H. (2003). *Teoría y dogmática de los derechos fundamentales.* México, D. F: UNAM, Instituto de Investigaciones Jurídicas. Obtenido de http://noduslex.mx/biblioteca/Dogmatica.pdf

Oña, O., Parrales, L., Vera, M., & Zhigue, F. (2025). La protección de datos personales en la era digital - Retos y oportunidades. *Revistalexenlace, 2*(1), 38-45. Obtenido de https://revistalexenlace.com/index.php/ojs/article/view/5

Organización de los Estados Americanos. (1969). *Convención Americana sobre Derechos Humanos.* Organización de los Estados Americanos. Obtenido de https://www.oas.org/dil/esp/tratados/b-32_convencion_americana_sobre_derechos_humanos.htm

Organización para la Cooperación y el Desarrollo Económico. (1980). *Directrices de la OCDE sobre la protección de la privacidad y los flujos transfronterizos de datos personales.* Paris: Publicaciones OCDE. doi:https://doi.org/10.1787/9789264201325-es

Pascual, C., & Vázquez, E. (2022). Protección de datos y uso ético de la tecnología para una didáctica sostenible. *Revista Electrónica Interuniversitaria de Formación del Profesorado*, 95-110. doi:https://doi.org/10.6018/reifop.529831

Porcelli, A. (2019). La protección de los datos personales en el entorno digital. Los estándares de protección de datos en los países iberoamericanos. *Revista Quaestio Iuris*, 465-497. Obtenido de https://www.e-publicacoes.uerj.br/quaestioiuris/article/download/40175/32567

Ramírez, M. (2011). Derecho a la intimidad. Análisis a la normativa ecuatoriana. *Tesis de Maestría.* Universidad del Azuay, Cuenca. Obtenido de https://dspace.uazuay.edu.ec/bitstream/datos/5520/1/08518.pdf

Red Iberoamericana de Protección de Datos. (2017). *Estándares de Protección de Datos Personales para los Estados Iberoamericanos.* Red Iberoamericana de Protección de Datos. Obtenido de https://www.redipd.org/sites/default/files/estandares_de_proteccion_de_datos_personales_para_los_estados_iberoamericanos_aprobados_por_la_ripd_el_20_de_junio_de_2017.pdf

Red Iberoamericana de Protección de Datos. (2020). *Plan Estratégico 2021-2025 Red Iberoamericana de Protección de Datos (RIPD) "Nuevos tiempos para la privacidad. Nuevas estrategias"*. Red Iberoamericana de Protección de Dato. Obtenido de https://www.redipd.org/documento/plan-estrategico-ripd-2021-2025.pdf

Romero, M., Rojas, C., Bustamante, W., Loaiza, R., Martel, C., & Castillo, R. (2023). *Metodología de la investigación: Técnicas e instrumentos de investigación.* Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú. Obtenido de https://bida.uclv.edu.cu/bitstream/handle/123456789/17350/80-M%C3%A9todolog%C3%ADa%2Bde%2Bla%2Binvestigaci%C3%B3n.pdf?sequence=1&isAllowed=y

Rosas, G., & Pila, G. (2023). La protección de datos personales en Ecuador: Una revisión histórica-normativa de este derecho fundamental en el país suramericano. *VISUAL REVIEW: International Visual Culture Review/Revista Internacional de Cultura Visual*, 1-16. doi:https://doi.org/10.37467/revvisual.v10.4568

Sanz, F. (2025). Derecho fundamental a la protección de los datos personales en América Latina: desafíos ante el alcance extraterritorial del Reglamento General de Protección de Datos de la Unión Europea. *Revista Derecho del Estado*(62), 143-169. doi:https://doi.org/10.18601/01229893.n62.06

Travieso, C., & Hernández, A. (2025). *Protección de datos personales, académicos y de investigación.* Repositorio GREDOS, Universidad de Salamanca. Obtenido de https://gredos.usal.es/bitstream/handle/10366/164857/Capi%cc%81tulo%2001_Proteccio%cc%81n%20de%20datos_AF.pdf?sequence=1&isAllowed=y

Troncoso, A. (2006). La publicación de datos de profesores y alumnos y la privacidad personal: acerca de la protección de datos personales en las Universidades. *Revista de Derecho Político*, 79-163. doi:https://doi.org/10.5944/rdp.67.2006.8999

Univesidad Técnica de Ambato. (2025). *Política de Protección de Datos Personales.* Ambato: Univesidad Técnica de Ambato. Obtenido de https://www.bing.com/ck/a?!&&p=d61a6a03e93bd96b73aa53cd64da04abbf3a46519cde0c558a2a1fc1e6ea63dbJmltdHM9MTc2MzU5NjgwMA&ptn=3&ver=2&hsh=4&fclid=001c3e1a-1310-6a44-25bd-

2d4012bf6b6d&psq=cuando+de+aprob%c3%b3+la+pol%c3%adtica+de+protecci%c3%b3n+de+datos+perso

Vasco, J., Ruiz, G., Macas, B., & León, V. (2025). Ciberseguridad y protección de datos personales: desafíos y perspectivas. *GADE: Revista Científica, 5*(1), 675-688. doi:https://doi.org/10.63549/rg.v5i1.642

Villabella, C. (2015). Los métodos en la investigación jurídica. Algunas precisiones. En C. Villabella, *Metodologías: enseñanza e investigación jurídicas* (págs. 317-334). México D.F: Universidad Nacional Autónoma de México. Obtenido de https://archivos.juridicas.unam.mx/www/bjv/libros/13/6226/12a.pdf

Villoria, M. (2015). La transparencia como política pública en España: algunas reflexiones. *Eunomía. Revista en Cultura de la Legalidad*, 85-103. Obtenido de https://e-revistas.uc3m.es/index.php/EUNOM/article/download/2234/1170

Warren, S., & Brandeis, L. (1890). *The right to privacy.* Boston: Harvard Law Review. Obtenido de https://jhhe.sempervifoundation.org/pdfs/JHHE%20V4n1%20Spring2018-PagesWeb.pdf#page=65

ANEXOS

ANEXO 1. GUÍA DE ENTREVISTA CON CONSENTIMIENTO



FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

CONSENTIMIENTO INFORMADO PARA PARTICIPACIÓN EN ENTREVISTA SEMIESTRUCTURADA

Título del estudio: "PARAMETROS JURIDICOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO UNIVERSITARIO"

Investigador responsable: Peter Andrés Merino Lara

Estudiante de la Universidad Técnica de Ambato perteneciente a la carrera de Derecho

Correo electrónico institucional: pmerino1425 @uta.edu.ec

1. Propósito del estudio

Usted ha sido invitado a participar en esta investigación cuyo objetivo general es:

Investigar la incidencia de la Ley de Protección de Datos en el entorno Universitario.

Y sus objetivos específicos son:

- Analizar los parámetros jurídicos de la Ley de Protección de Datos Personales que han sido adoptados en el entorno Universitario.
- Describir los principales aspectos jurídicos respecto de la Ley de Protección de Datos Personales que podrían ser considerados en el entorno Universitario
- Establecer los desafíos de la Ley de Protección de Datos Personales en el entorno Universitario.

Con la finalidad de identificar la incidencia de la LOPDP, los posibles riesgos y percepciones dentro de la institución educativa. Su participación es valiosa debido a la basta experiencia y conocimientos en áreas relacionadas con el ámbito de estudio

2. Naturaleza de la participación

Su participación consiste en responder una entrevista semiestructurada, con una duración aproximada de 20 a 40 minutos donde se abordarán temas relacionados a los parámetros jurídicos de la LOPDP en el entorno universitario, la entrevista se podrá realizar de manera presencial o telemática.

3. Voluntariedad

Su participación dentro de esta investigación es completamente libre y voluntaria, usted puede rechazar participar, interrumpir la entrevista, omitir preguntas, retirarse del estudio en cualquier momento, sin que ello genere perjuicio ni consecuencia alguna.

4. Confidencialidad y anonimato

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

La información que usted proporcione será tratada de forma confidencial, para este efecto su identidad será protegida mediante el uso de "NN1", "NN2", etc.

Los datos se almacenarán en archivos digitales y se utilizarán exclusivamente con fines académicos.

5. Riesgos

Este estudio no genera riesgos físicos, psicológicos, legales ni institucionales, su participación se limita únicamente a compartir información y su criterio profesional.

6. Uso de la información

La información será utilizada para fines académicos e investigativos, será analizada y agregada a la investigación.

7. Derecho a realizar preguntas

Usted tiene derecho a solicitar aclaraciones o información adicional antes, durante o después de la entrevista.

8. Declaración de consentimiento

Declaro que he leído y comprendido la información anterior; que se le ha explicado el propósito del estudio y la naturaleza de mi participación; se me garantiza confidencialidad y voluntariedad; autorizo participar en esta investigación de manera libre y consiente.

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

Entrevista para el Informe final del trabajo de titulación previo a la obtención del Título de Abogado.

Tema: "PARAMETROS JURIDICOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO UNIVERSITARIO"

Nombre del entrevistado: .....

Fecha: .....

I. Preguntas Guía

1. ¿Cómo considera usted que la Ley Orgánica de Protección de Datos Personales (LOPDP) está incidiendo en el manejo de la información en la institución de educación superior que usted trabaja?

.....

.....

.....

.....

.....

2. ¿De qué manera la institución en la que usted trabaja ha comenzado a adaptar en su norma interna, procedimientos que den cumplimiento a las disposiciones de la Ley Orgánica de Protección de Datos Personales (LOPDP)?

.....

.....

.....

.....

.....

Elaborador por: Peter Andrés Merino Lara	**Validado por**: Abg. Mg. José Luis Romo Santana

3. ¿Qué aspectos jurídicos de la Ley Orgánica de Protección de Datos Personales considera que todavía no han sido suficientemente desarrollados o comprendidos en la institución en la que usted trabaja?

.....

.....

.....

.....

.....

4. Desde su experiencia, ¿cree que las políticas institucionales del establecimiento en el que usted trabaja reflejan adecuadamente los principios de la Ley, como el consentimiento o la finalidad? ¿Por qué?

.....

.....

.....

.....

.....

5. ¿Describa cómo la institución en la que usted trabaja gestiona el cumplimiento y la comunicación de sus obligaciones ante la Superintendencia de Protección de Datos Personales?

.....

.....

.....

.....

.....

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

6. Considerando la estructura organizacional de una universidad, ¿Qué políticas técnicas administrativas debería implementar las instituciones de educación superior para asegurar el cumplimiento de principios que operan el tratamiento de datos personales?

.....

.....

.....

.....

.....

7. ¿Cómo actúa la institución en la que usted trabaja frente a denuncias o reportes de presuntos incumplimientos a la Ley de Protección de Datos Personales?

.....

.....

.....

.....

.....

8. ¿Qué acciones está implementando la institución en la que usted trabaja para evolucionar hacia una verdadera cultura institucional de respeto a la privacidad y protección de los datos personales de toda su comunidad?

.....

.....

.....

.....

.....

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

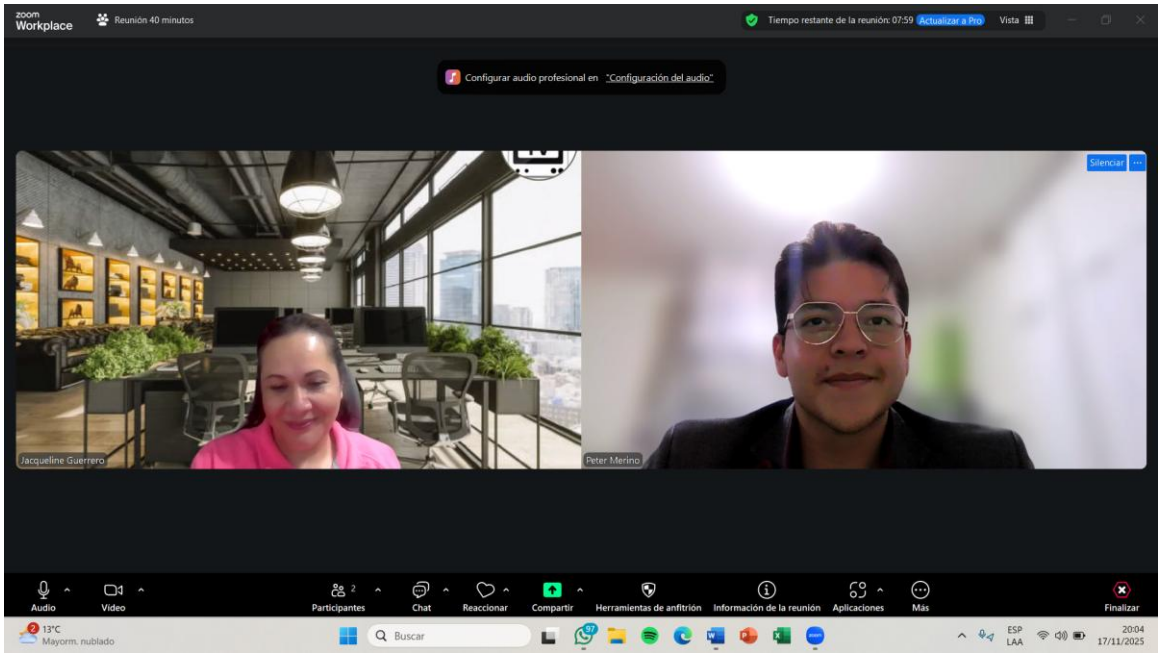
ANEXO 2. FOTOGRAFÍAS CON LOS ENTREVISTADOS

Entrevistado N°1 (NN1)

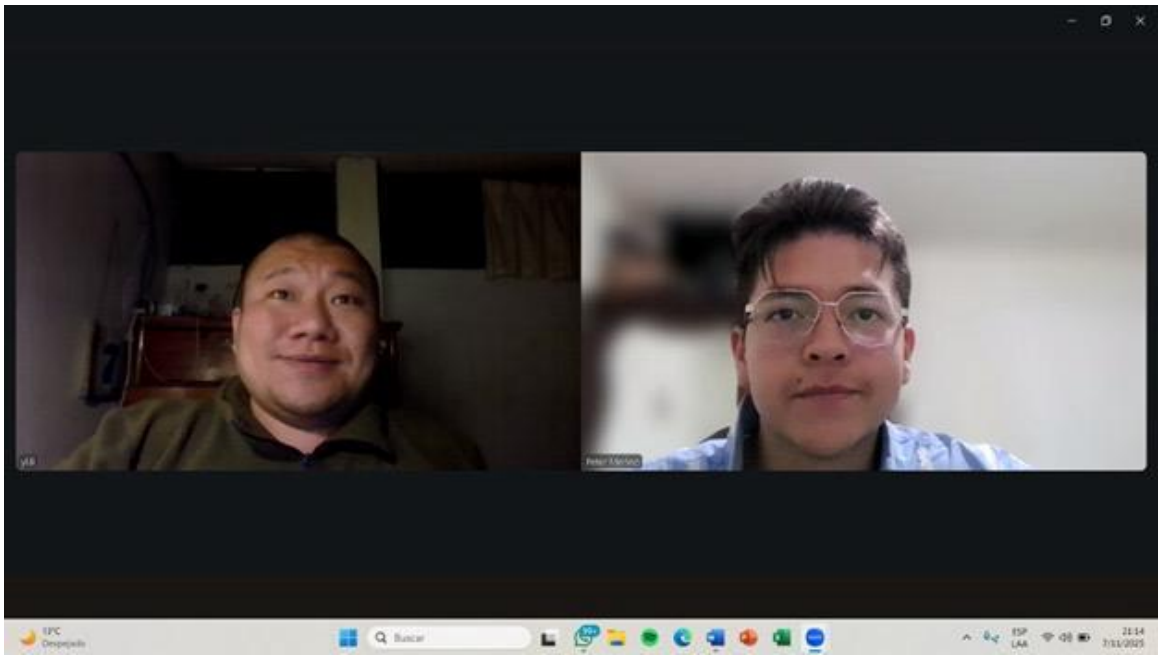




Entrevistado N°2 (NN2)



Entrevistado N°3 (NN3)





ANEXO 3. EVIDENCIA DE LAS ENTREVISTAS

Entrevista N°1 (NN1)

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

CONSENTIMIENTO INFORMADO PARA PARTICIPACIÓN EN ENTREVISTA SEMIESTRUCTURADA

Título del estudio: "PARAMETROS JURIDICOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO UNIVERSITARIO"

Investigador responsable: Peter Andrés Merino Lara

Estudiante de la Universidad Técnica de Ambato perteneciente a la carrera de Derecho

Correo electrónico institucional: pmerino1425 @uta.edu.ec

1. Propósito del estudio

Usted ha sido invitado a participar en esta investigación cuyo objetivo general es:

Investigar la incidencia de la Ley de Protección de Datos en el entorno Universitario.

Y sus objetivos específicos son:

- Analizar los parámetros jurídicos de la Ley de Protección de Datos Personales que han sido adoptados en el entorno Universitario.
- Describir los principales aspectos jurídicos respecto de la Ley de Protección de Datos Personales que podrían ser considerados en el entorno Universitario
- Establecer los desafíos de la Ley de Protección de Datos Personales en el entorno Universitario.

Con la finalidad de identificar la incidencia de la LOPDP, los posibles riesgos y percepciones dentro de la institución educativa. Su participación es valiosa debido a la basta experiencia y conocimientos en áreas relacionadas con el ámbito de estudio

2. Naturaleza de la participación

Su participación consiste en responder una entrevista semiestructurada, con una duración aproximada de 20 a 40 minutos donde se abordarán temas relacionados a los parámetros jurídicos de la LOPDP en el entorno universitario, la entrevista se podrá realizar de manera presencial o telemática.

3. Voluntariedad

Su participación dentro de esta investigación es completamente libre y voluntaria, usted puede rechazar participar, interrumpir la entrevista, omitir preguntas, retirarse del estudio en cualquier momento, sin que ello genere perjuicio ni consecuencia alguna.

4. Confidencialidad y anonimato

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

La información que usted proporcione será tratada de forma confidencial, para este efecto su identidad será protegida mediante el uso de "NN1", "NN2", etc.

Los datos se almacenarán en archivos digitales y se utilizarán exclusivamente con fines académicos.

5. Riesgos

Este estudio no genera riesgos físicos, psicológicos, legales ni institucionales, su participación se limita únicamente a compartir información y su criterio profesional.

6. Uso de la información

La información será utilizada para fines académicos e investigativos, será analizada y agregada a la investigación.

7. Derecho a realizar preguntas

Usted tiene derecho a solicitar aclaraciones o información adicional antes, durante o después de la entrevista.

8. Declaración de consentimiento

Declaro que he leído y comprendido la información anterior; que se le ha explicado el propósito del estudio y la naturaleza de mi participación; se me garantiza confidencialidad y voluntariedad; autorizo participar en esta investigación de manera libre y consiente.

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

Entrevista para el Informe final del trabajo de titulación previo a la obtención del Título de Abogado.

Tema: "PARAMETROS JURIDICOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO UNIVERSITARIO"

Nombre del entrevistado: Ab. Juan Pablo Santamaría Velasco, Mg.

Fecha: 18/11/2025

I. Preguntas Guía

1. ¿Cómo considera usted que la Ley Orgánica de Protección de Datos Personales (LOPDP) está incidiendo en el manejo de la información en la institución de educación superior que usted trabaja?

Aunque la Ley Orgánica de Protección de Datos Personales (LOPDP) aún no ha sido plenamente implementada en la institución de educación superior en la que trabajo, su existencia ha comenzado a generar un marco de reflexión interna sobre las obligaciones jurídicas vinculadas al tratamiento de datos personales.

Desde una perspectiva normativa, la ley establece principios y deberes que interpelan directamente a las universidades como responsables del manejo de información sensible de estudiantes, docentes y personal administrativo. Si bien aún no se han adoptado medidas concretas, el solo hecho de contar con esta legislación implica una reconfiguración progresiva de las responsabilidades institucionales, en especial en lo relativo a la obtención del consentimiento, la transparencia en el uso de datos y la obligación de garantizar medidas de seguridad adecuadas.

En este momento, el impacto se manifiesta principalmente en el plano normativo y en la necesidad de adecuación futura.

2. ¿De qué manera la institución en la que usted trabaja ha comenzado a adaptar en su norma interna, procedimientos que den cumplimiento a las disposiciones de la Ley Orgánica de Protección de Datos Personales (LOPDP)?

La institución en la que trabajo ha comenzado un proceso paulatino de adecuación normativa interna para dar cumplimiento a las disposiciones de la Ley Orgánica de Protección de Datos Personales (LOPDP). Uno de los primeros pasos ha sido la elaboración preliminar de políticas institucionales de protección de datos, orientadas a establecer directrices claras sobre el tratamiento lícito, transparente y seguro de la información personal que se gestiona en el ámbito académico y administrativo.

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

Asimismo, se han iniciado acciones preparatorias para la designación de un delegado de protección de datos (DPO), figura que será clave para asegurar la vigilancia del cumplimiento normativo dentro de la universidad. Esta preparación incluye tanto la revisión del perfil profesional requerido como la estructuración de sus funciones dentro del marco institucional. Aunque aún se encuentra en una fase de planificación, estos esfuerzos reflejan un compromiso con la implementación progresiva de la LOPDP y con la construcción de una cultura organizacional respetuosa de los derechos digitales.

3. ¿Qué aspectos jurídicos de la Ley Orgánica de Protección de Datos Personales considera que todavía no han sido suficientemente desarrollados o comprendidos en la institución en la que usted trabaja?

Uno de los aspectos jurídicos de la Ley Orgánica de Protección de Datos Personales (LOPDP) que aún no ha sido suficientemente desarrollado ni plenamente comprendido en la institución es el principio de *responsabilidad proactiva*. Este principio implica que no basta con cumplir formalmente con la norma, sino que la institución debe ser capaz de demostrar, en todo momento, que ha adoptado medidas técnicas, organizativas y jurídicas adecuadas para garantizar la protección efectiva de los datos personales. Esta exigencia va más allá del cumplimiento reactivo y requiere un enfoque preventivo que todavía no ha sido interiorizado plenamente.

Asimismo, persisten vacíos de comprensión respecto al alcance del consentimiento informado, especialmente en contextos académicos y administrativos donde la recolección de datos suele asumirse como parte del proceso institucional. No se ha reflexionado aún con la profundidad necesaria sobre cuándo el consentimiento es necesario, cómo debe ser recabado válidamente y en qué casos puede considerarse inválido o viciado.

Finalmente, otro aspecto poco desarrollado es la figura del encargado del tratamiento, así como las obligaciones contractuales que deben establecerse con terceros que acceden a datos personales por cuenta de la universidad. Este punto es especialmente sensible en un entorno crecientemente digitalizado, donde el manejo de datos a través de plataformas externas es una práctica común que aún carece del respaldo jurídico adecuado.

4. Desde su experiencia, ¿cree que las políticas institucionales de las institución en la que usted trabaja reflejan adecuadamente los principios de la Ley, como el consentimiento o la finalidad? ¿Por qué?

Desde mi experiencia, considero que las políticas institucionales actuales aún no reflejan de manera adecuada los principios fundamentales establecidos en la Ley Orgánica de Protección de

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

Datos Personales (LOPDP), particularmente en lo que respecta al consentimiento y a la finalidad del tratamiento de datos.

En cuanto al consentimiento, si bien existen formularios y procedimientos mediante los cuales se recaba información de estudiantes y personal, en la práctica no siempre se garantiza que este consentimiento sea libre, específico, informado e inequívoco, como exige la normativa. Con frecuencia, el consentimiento es tratado como un requisito formal y no como una manifestación real de voluntad del titular de los datos, lo que puede comprometer su validez jurídica.

Respecto al principio de finalidad, aún se observa una falta de claridad en la delimitación de los propósitos específicos para los cuales se recopilan y utilizan los datos personales. En varios casos, la información se utiliza para fines distintos a los inicialmente comunicados, sin que exista una base legal o un nuevo consentimiento que respalde dicho cambio.

En consecuencia, aunque la institución ha dado algunos pasos hacia la adecuación normativa, todavía es necesario un esfuerzo más estructurado para asegurar que sus políticas reflejen de forma efectiva los principios rectores de la LOPDP, evitando prácticas que puedan vulnerar los derechos de los titulares.

5. ¿Describa cómo la institución en la que usted trabaja gestiona el cumplimiento y la comunicación de sus obligaciones ante la Superintendencia de Protección de Datos Personales?

Actualmente, la gestión del cumplimiento y la comunicación de obligaciones ante la Superintendencia de Protección de Datos Personales por parte de la institución en la que trabajo se encuentra en una etapa inicial. Si bien existe conciencia sobre la necesidad de establecer mecanismos formales de interacción con la autoridad, aún no se han implementado procesos específicos o sistematizados para asegurar dicha relación conforme a los requerimientos de la Ley Orgánica de Protección de Datos Personales (LOPDP).

Hasta el momento, no se ha designado oficialmente a un delegado institucional encargado de actuar como canal directo con la Superintendencia, ni se ha creado un sistema de reportes o auditorías internas que permitan verificar y documentar el cumplimiento de las obligaciones legales. Del mismo modo, no se ha registrado un plan estructurado de respuesta frente a posibles requerimientos, inspecciones o sanciones administrativas.

En este contexto, puede decirse que la gestión del cumplimiento ante la autoridad de control aún depende de iniciativas aisladas, sin una política institucional consolidada. Esta situación representa un desafío importante, dado que el marco legal exige no solo el cumplimiento sustantivo, sino también la capacidad de demostrar dicho cumplimiento ante la Superintendencia, lo cual requiere una estrategia organizativa que todavía está en desarrollo.

6. Considerando la estructura organizacional de una universidad, ¿Qué políticas técnicas administrativas debería implementar las instituciones de educación superior para asegurar el cumplimiento de principios que operan el tratamiento de datos personales?

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

Para garantizar el cumplimiento de los principios establecidos en la Ley Orgánica de Protección de Datos Personales (LOPDP), las instituciones de educación superior deben adoptar una serie de políticas técnico-administrativas alineadas con su estructura organizacional. En primer lugar, es esencial contar con una política institucional formal de protección de datos que establezca principios, procedimientos y responsabilidades claras para todas las unidades académicas y administrativas.

Asimismo, debe designarse un Delegado de Protección de Datos (DPO), con autonomía y competencias técnicas, encargado de coordinar las acciones de cumplimiento y servir de enlace con la Superintendencia. A nivel técnico, es necesario implementar medidas como protocolos de seguridad, control de accesos, cifrado de información y gestión de incidentes.

También se deben establecer procedimientos para recabar el consentimiento informado de manera válida y transparente, así como mecanismos de auditoría interna y revisión periódica del cumplimiento normativo. Finalmente, la capacitación continua del personal es clave para generar una cultura organizacional orientada al respeto de los derechos de los titulares de los datos.

7. ¿Cómo actúa la institución en la que usted trabaja frente a denuncias o reportes de presuntos incumplimientos a la Ley de Protección de Datos Personales?

Hasta el momento, la institución en la que trabajo no cuenta con un protocolo específico ni con un canal formalizado para la gestión de denuncias o reportes vinculados a presuntos incumplimientos de la Ley Orgánica de Protección de Datos Personales (LOPDP). Si bien existe una estructura general para la atención de reclamos administrativos o quejas estudiantiles, esta no contempla mecanismos diferenciados ni especializados para tratar vulneraciones de derechos relacionados con la protección de datos personales.

En la práctica, los casos potenciales suelen canalizarse a través de instancias como las direcciones académicas, secretarías generales o unidades jurídicas, sin que exista una trazabilidad adecuada ni procedimientos estandarizados para su análisis, respuesta o documentación. Esta ausencia de protocolos específicos puede generar demoras, respuestas inconsistentes o incluso el riesgo de incumplimientos por omisión.

La falta de una unidad o figura institucional encargada específicamente de la protección de datos, como un Delegado de Protección de Datos (DPO), limita además la capacidad de la universidad para actuar de forma técnica y conforme a los principios de responsabilidad proactiva y atención al titular previstos por la ley. En consecuencia, se evidencia la necesidad urgente de desarrollar políticas institucionales claras y mecanismos eficaces para gestionar este tipo de situaciones de manera adecuada y conforme al marco normativo vigente.

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

8. ¿Qué acciones está implementando la institución en la que usted trabaja para evolucionar hacia una verdadera cultura institucional de respeto a la privacidad y protección de los datos personales de toda su comunidad?

La institución en la que trabajo ha comenzado a dar pasos preliminares para avanzar hacia una cultura institucional de respeto a la privacidad y protección de los datos personales, aunque este proceso aún se encuentra en una fase de sensibilización más que de consolidación.

Entre las acciones más relevantes se encuentra la inclusión del tema en espacios de formación interna, como talleres dirigidos a personal administrativo y académico, enfocados en los aspectos básicos de la Ley Orgánica de Protección de Datos Personales (LOPDP). Estos espacios buscan generar conciencia sobre la importancia del manejo adecuado de la información personal y sus implicaciones jurídicas.

Además, se está trabajando en la elaboración de políticas institucionales que servirán como base normativa para futuras acciones de cumplimiento. Aunque estas aún no han sido aprobadas formalmente, reflejan una voluntad institucional de avanzar hacia el cumplimiento regulatorio y ético.

No obstante, para que esta cultura realmente se consolide, será necesario implementar medidas más estructurales, como la designación de un Delegado de Protección de Datos, el desarrollo de programas permanentes de capacitación, la integración de la privacidad en los procesos digitales, y la promoción del principio de responsabilidad proactiva en todos los niveles organizacionales. La construcción de una cultura de protección de datos requiere tiempo, compromiso institucional y una visión clara de los riesgos y deberes que implica el entorno digital actual.



Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

Entrevista N°2 (NN2)

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

CONSENTIMIENTO INFORMADO PARA PARTICIPACIÓN EN ENTREVISTA SEMIESTRUCTURADA

Título del estudio: "PARAMETROS JURIDICOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO UNIVERSITARIO"

Investigador responsable: Peter Andrés Merino Lara

Estudiante de la Universidad Técnica de Ambato perteneciente a la carrera de Derecho

Correo electrónico institucional: pmerino1425 @uta.edu.ec

1. Propósito del estudio

Usted ha sido invitado a participar en esta investigación cuyo objetivo general es:

Investigar la incidencia de la Ley de Protección de Datos en el entorno Universitario.

Y sus objetivos específicos son:

- Analizar los parámetros jurídicos de la Ley de Protección de Datos Personales que han sido adoptados en el entorno Universitario.
- Describir los principales aspectos jurídicos respecto de la Ley de Protección de Datos Personales que podrían ser considerados en el entorno Universitario
- Establecer los desafíos de la Ley de Protección de Datos Personales en el entorno Universitario.

Con la finalidad de identificar la incidencia de la LOPDP, los posibles riesgos y percepciones dentro de la institución educativa. Su participación es valiosa debido a la basta experiencia y conocimientos en áreas relacionadas con el ámbito de estudio

2. Naturaleza de la participación

Su participación consiste en responder una entrevista semiestructurada, con una duración aproximada de 20 a 40 minutos donde se abordarán temas relacionados a los parámetros jurídicos de la LOPDP en el entorno universitario, la entrevista se podrá realizar de manera presencial o telemática.

3. Voluntariedad

Su participación dentro de esta investigación es completamente libre y voluntaria, usted puede rechazar participar, interrumpir la entrevista, omitir preguntas, retirarse del estudio en cualquier momento, sin que ello genere perjuicio ni consecuencia alguna.

4. Confidencialidad y anonimato

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

La información que usted proporcione será tratada de forma confidencial, para este efecto su identidad será protegida mediante el uso de "NN1", "NN2", etc.

Los datos se almacenarán en archivos digitales y se utilizarán exclusivamente con fines académicos.

5. Riesgos

Este estudio no genera riesgos físicos, psicológicos, legales ni institucionales, su participación se limita únicamente a compartir información y su criterio profesional.

6. Uso de la información

La información será utilizada para fines académicos e investigativos, será analizada y agregada a la investigación.

7. Derecho a realizar preguntas

Usted tiene derecho a solicitar aclaraciones o información adicional antes, durante o después de la entrevista.

8. Declaración de consentimiento

Declaro que he leído y comprendido la información anterior; que se le ha explicado el propósito del estudio y la naturaleza de mi participación; se me garantiza confidencialidad y voluntariedad; autorizo participar en esta investigación de manera libre y consiente.

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

Entrevista para el Informe final del trabajo de titulación previo a la obtención del Título de Abogado.

Tema: "PARAMETROS JURIDICOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO UNIVERSITARIO"

Nombre del entrevistado: Abg. Dra. Jaqueline Guerrero (Docente de la Universidad Internacional Del Ecuador, especialista en Derecho Digital)

Fecha: 17 de noviembre de 2025

I. Preguntas Guía

1. **¿Cómo considera usted que la Ley Orgánica de Protección de Datos Personales (LOPDP) está incidiendo en el manejo de la información en la institución de educación superior que usted trabaja?**

Lo primero que hay que precisar es que la LOPDP aplica exclusivamente al tratamiento de datos personales, no en general a la información que maneja la universidad, sino específicamente a los datos personales. La ley y toda la normativa de protección de datos aplica a la universidad debido a que la universidad es responsable de tratamiento de esos datos personales, lo que podría decir es que, al ser un régimen de cumplimiento obligatorio, no solamente la Universidad Internacional del Ecuador, sino en general todas las instituciones educativas específicamente han realizado procesos de adecuación para el cumplimiento de la norma y además han tomado medidas para poder modificar todo aquello que es necesario para cumplir la ley y por tanto que los tratamientos de datos personales sean tratamientos lícitos en términos de la ley de protección de datos.

2. **¿De qué manera la institución en la que usted trabaja ha comenzado a adaptar en su norma interna, procedimientos que den cumplimiento a las disposiciones de la Ley Orgánica de Protección de Datos Personales (LOPDP)?**

Puedo dar cuenta de aquello que se ha compartido con todos los actores internos e inclusive hacia afuera de la institución, una de las primeras medidas fue haber incorporado una política de protección de datos, un aviso de privacidad en el sitio web y luego haber incorporado ciertas cláusulas específicas de protección de datos en los contratos (confidencialidad), en términos de profesores o de proveedores, ya hay una cláusula de protección de datos a lo propio por ejemplo en los correos electrónicos o en los formularios que utiliza la universidad para recabar datos personales, entonces eso evidencia que se está haciendo pues internamente adecuaciones para poder, cumplir todo el marco normativo en materia de protección de datos.

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

3. **¿Qué aspectos jurídicos de la Ley Orgánica de Protección de Datos Personales considera que todavía no han sido suficientemente desarrollados o comprendidos en la institución en la que usted trabaja?**

Desde mi experiencia como docente, puedo señalar que desconozco todos los procesos internos de la universidad, considero que falta adaptar ciertas cosas, como puede ser mejorar precisamente los formularios que se utilizan en algunos casos para recabar datos, mejorar el uso de los datos para fines de envío, por ejemplo, de información respecto de los programas de la universidad. También considero que la universidad todavía no ha hecho el tema de obtener el consentimiento en los casos en los que se requiera del personal interno de la universidad, entonces puedo decir pues no hemos todavía hecho esa parte que es importante a los datos de los trabajadores, pienso que todavía hay mucho que se tiene que hacer, pero que eso va a viabilizarse un poco más o agilitarse un poco más con el pasar del tiempo.

4. **Desde su experiencia, ¿cree que las políticas institucionales del establecimiento en el que usted trabaja reflejan adecuadamente los principios de la Ley, como el consentimiento o la finalidad? ¿Por qué?**

El consentimiento es una base legitimadora, creo que los principios de la ley están parcialmente reflejados en algunos instrumentos de la universidad, por ejemplo el aviso de privacidad responde a un tema de lealtad y el derecho a la información, es decir, explicar todo aquello que los titulares de los datos deben saber de cómo se están tratando los datos pues por parte del responsable, entonces el rato que uno tiene ese aviso de privacidad está cumpliendo algunos principios, ahí creo que en principio también podríamos hablar de un tema de finalidad o de proporcionalidad, tal vez también.

5. **¿Describa cómo la institución en la que usted trabaja gestiona el cumplimiento y la comunicación de sus obligaciones ante la Superintendencia de Protección de Datos Personales?**

Yo diría que, si la universidad ha contratado un delegado de protección de datos o tiene un delegado de protección de datos, la comunicación con la superintendencia va a estar mediada por el delegado de protección de datos y la superintendencia, este organismo ha solicitado que las universidades reporten el nombre del delegado a quien se lo registrará como encargado de estos procesos. En cuanto a remitir información hacia la superintendencia no se ha definido nada en ese sentido, no se ha abierto el tema del registro de las bases o no ha pedido registros de tratamiento de datos, entonces no creo que la universidad de su información. La comunicación con la superintendencia debe ser desde la atención a lo que pida la autoridad de control y lo único que ha pedido es que se registre el nombramiento del delegado hasta el 31 de diciembre.

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

6. **Considerando la estructura organizacional de una universidad, ¿Qué políticas técnicas administrativas debería implementar las instituciones de educación superior para asegurar el cumplimiento de principios que operan el tratamiento de datos personales?**

Las medidas jurídicas, administrativas, técnicas son acorde a cada responsable de tratamiento, según lo que el responsable haga internamente, es decir, según sus procesos, según sus tratamientos, según lo que tenga. Por decir, si una institución de educación superior tiene sus registros en papel, una medida de seguridad puede ser un acceso con código, un acceso con huella al archivo físico. Pero si otra universidad ya prescindió del papel y tiene un registro, tiene un archivo más bien en la nube, la medida de seguridad no va a ser la misma. No es que las medidas son generales o genéricas para un sector. Las medidas de cualquier tipo son inherentes a cada responsable según lo que el responsable haga, según lo que el responsable tenga. Inclusive, en cuestión técnica, depende de la tecnología, depende de los sistemas, depende de con qué trabajen, podrá ver que sí puede pasar que alguien, por ejemplo, no tenga un servicio de respaldo en la nube. Es decir, que todavía tenga un almacenamiento propio, en cuyo caso no le aplicaría una medida que aplica si es que se tiene respaldos en la nube.

7. **¿Cómo actúa la institución en la que usted trabaja frente a denuncias o reportes de presuntos incumplimientos a la Ley de Protección de Datos Personales?**

Lo que un titular de datos puede hacer frente a la institución es ejercer sus derechos por el canal que haya definido el responsable de tratamiento y que esté especificado en el aviso de privacidad, entonces, la universidad debe tener un canal, que seguramente es un correo electrónico, si recibe una solicitud con un derecho, como podría ser la rectificación, la eliminación o la misma portabilidad, la universidad tiene que sujetarse a lo que dice la ley en cuanto al tiempo que tiene para responder según el derecho que se esté ejerciendo. No hay más, o sea, no hay más en relación con lo que tiene que hacer frente a un pedido. Si ya el titular, por ejemplo, no recibe una respuesta, ahí la queja ya no es ante el mismo responsable, sino tendría que interponerlo ante la autoridad de control directamente, es decir, pues yo seguí el canal que me dijeron, no me atendieron, por tanto, usted encárguese de verificar eso.

8. **¿Qué acciones está implementando la institución en la que usted trabaja para evolucionar hacia una verdadera cultura institucional de respeto a la privacidad y protección de los datos personales de toda su comunidad?**

Yo creería que la universidad está en un proceso de adecuación para cumplimiento, y el hablar de una cultura de privacidad implica muchos cambios que todavía no son tan evidentes, creo que el paso más importante en este último tiempo que yo he visto es el perfil que se para que alguien ocupe el papel de "delegado de protección de datos" debe contar con un perfil robusto, y eso permite ver que la institución quiere ir hacia lo que se conoce como un programa de gobernanza de datos personales, sí se pueda generar, en un mediano plazo, se puede generar la construcción

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

de una cultura de privacidad. Más allá de eso, pues no he visto, en realidad, nada adicional que involucre, por ejemplo, a nosotros que manejamos datos personales de los estudiantes.

Firmado electrónicamente por: ELSA JACQUELINE GUERRERO CARRERA
Validar documento con FirmaEC

Dra. Jaqueline Guerrero

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

Entrevista N°3 (NN3)

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

CONSENTIMIENTO INFORMADO PARA PARTICIPACIÓN EN ENTREVISTA SEMIESTRUCTURADA

Título del estudio: "PARAMETROS JURIDICOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO UNIVERSITARIO"

Investigador responsable: Peter Andrés Merino Lara

Estudiante de la Universidad Técnica de Ambato perteneciente a la carrera de Derecho

Correo electrónico institucional: pmerino1425 @uta.edu.ec

1. Propósito del estudio

Usted ha sido invitado a participar en esta investigación cuyo objetivo general es:

Investigar la incidencia de la Ley de Protección de Datos en el entorno Universitario.

Y sus objetivos específicos son:

- Analizar los parámetros jurídicos de la Ley de Protección de Datos Personales que han sido adoptados en el entorno Universitario.
- Describir los principales aspectos jurídicos respecto de la Ley de Protección de Datos Personales que podrían ser considerados en el entorno Universitario
- Establecer los desafíos de la Ley de Protección de Datos Personales en el entorno Universitario.

Con la finalidad de identificar la incidencia de la LOPDP, los posibles riesgos y percepciones dentro de la institución educativa. Su participación es valiosa debido a la basta experiencia y conocimientos en áreas relacionadas con el ámbito de estudio

2. Naturaleza de la participación

Su participación consiste en responder una entrevista semiestructurada, con una duración aproximada de 20 a 40 minutos donde se abordarán temas relacionados a los parámetros jurídicos de la LOPDP en el entorno universitario, la entrevista se podrá realizar de manera presencial o telemática.

3. Voluntariedad

Su participación dentro de esta investigación es completamente libre y voluntaria, usted puede rechazar participar, interrumpir la entrevista, omitir preguntas, retirarse del estudio en cualquier momento, sin que ello genere perjuicio ni consecuencia alguna.

4. Confidencialidad y anonimato

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

La información que usted proporcione será tratada de forma confidencial, para este efecto su identidad será protegida mediante el uso de "NN1", "NN2", etc.

Los datos se almacenarán en archivos digitales y se utilizarán exclusivamente con fines académicos.

5. Riesgos

Este estudio no genera riesgos físicos, psicológicos, legales ni institucionales, su participación se limita únicamente a compartir información y su criterio profesional.

6. Uso de la información

La información será utilizada para fines académicos e investigativos, será analizada y agregada a la investigación.

7. Derecho a realizar preguntas

Usted tiene derecho a solicitar aclaraciones o información adicional antes, durante o después de la entrevista.

8. Declaración de consentimiento

Declaro que he leído y comprendido la información anterior; que se le ha explicado el propósito del estudio y la naturaleza de mi participación; se me garantiza confidencialidad y voluntariedad; autorizo participar en esta investigación de manera libre y consiente.

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

Entrevista para el Informe final del trabajo de titulación previo a la obtención del Título de Abogado.

Tema: "PARAMETROS JURIDICOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO UNIVERSITARIO"

Nombre del entrevistado: Ing. Yu Lung Li (Delegado de Protección de Datos de la Universidad Técnica de Ambato)

Fecha: Viernes 7 de noviembre de 2025

I. Preguntas Guía

1. **¿Cómo considera usted que la Ley Orgánica de Protección de Datos Personales (LOPDP) está incidiendo en el manejo de la información en la institución de educación superior que usted trabaja?**

Respecto a LPDP mayormente las empresas desconocen lo que abarca, pero hoy en día se está tratando de proteger los datos personales que son usados de manera errónea para prevenir estos delitos, los recursos que poseemos en la institución son muy limitados para que se adapten totalmente a la realidad que pide la LPDP y las demás resoluciones que la Superintendencia de Protección de Datos emite, es una utopía que poco a poco se va destruyendo, por ello se debe continuar con una capacitación continua.

2. **¿De qué manera la institución en la que usted trabaja ha comenzado a adaptar en su norma interna, procedimientos que den cumplimiento a las disposiciones de la Ley Orgánica de Protección de Datos Personales (LOPDP)?**

Hoy en día hemos aprobado con el Honorable Consejo Universitario las políticas de protección de datos para como poder utilizar y tratar datos, estamos estableciendo formatos que aseguren que la información no sea divulgada y sea tratado conforme lo señala la ley, hoy en día los proveedores tienen acceso a la información de todos los datos para que traten los datos del entorno universitario, hacen consultorías para acceder al mismo y esto debe seguir un procedimiento de confidencialidad que se tratan de desarrollar para mejorar el funcionamiento de la institución, son los primeros pasos que se están realizando.

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana

3. **¿Qué aspectos jurídicos de la Ley Orgánica de Protección de Datos Personales considera que todavía no han sido suficientemente desarrollados o comprendidos en la institución en la que usted trabaja?**

Realmente la LODP hoy en día está en auge la Inteligencia Artificial, al tener esta herramienta que absorbe información de todas las personas y al no saber los alcances que estos avances tienen la ley no lograr abarcar todos estos aspectos jurídicos, es un camino que se va descubriendo y que la sociedad y la tecnología van desarrollando de la mano, hay muchos aspectos que nosotros debemos considerar para que se desarrollen mejores mecanismos de protección, es algo que con el tiempo la Superintendencia de Protección de Datos va realizando conforme se van presentando las situaciones pertinentes para resolverlas y adaptarlas a la realidad de la universidad.

4. **Desde su experiencia, ¿cree que las políticas institucionales del establecimiento en el que usted trabaja reflejan adecuadamente los principios de la Ley, como el consentimiento o la finalidad? ¿Por qué?**

Naturalmente, nuestras políticas mencionan que necesariamente se debe contar con el consentimiento de los sujetos que se ven inmersos en la universidad, esto es un proceso que con el tiempo se va actualizando para brindar una mejor atención conforme se van dando las problemáticas del día a día, recién se están realizando los procesos que determinaran si nuestra política soluciona o no los problemas que se enfrenta.

5. **¿Describa cómo la institución en la que usted trabaja gestiona el cumplimiento y la comunicación de sus obligaciones ante la Superintendencia de Protección de Datos Personales?**

Nosotros, hacemos un cumplimiento a los pasos que nos indican las resoluciones con matrices de riesgos, políticas de protección y demás mecanismos que nos obligan a seguir, se mantiene una comunicación continua con la Superintendencia de Protección de Datos Personales cuando existe una denuncia con un debido tiempo para realizar una investigación.

6. **Considerando la estructura organizacional de una universidad, ¿Qué políticas técnicas administrativas debería implementar las instituciones de educación superior para asegurar el cumplimiento de principios que operan el tratamiento de datos personales?**

Esto es algo que hoy en día se está realizando, se plantea una automatización de datos por parte de quienes desean formar parte de la institución, así como para servidores públicos y trabajadores, conforme las políticas establecidas, controlamos accesos y roles para poder garantizar la protección de datos. Además de implementar tiempos de usos para el almacenamiento de datos, garantizando que la información sea más integra y real

7. **¿Cómo actúa la institución en la que usted trabaja frente a denuncias o reportes de presuntos incumplimientos a la Ley de Protección de Datos Personales?**

Actualmente no hemos tenido denuncias, pero nosotros para poder actuar recibimos una denuncia por parte del titular para realizar una investigación en termino de 10 días y así determinar si es que

en verdad se ha dado un mal uso o incluso determinar si no es cierta la denuncia presentada, y así se determina si sería sujeto de sanción y posteriormente una subsanación.

8. **¿Qué acciones está implementando la institución en la que usted trabaja para evolucionar hacia una verdadera cultura institucional de respeto a la privacidad y protección de los datos personales de toda su comunidad?**

Se plantea utilizar capacitaciones a todos los miembros de su comunidad para que la gente se alinee al objetivo de la política de protección de datos y así comprendan la importancia de este tema, por publicaciones en redes sociales de la universidad, capacitaciones, publicidad en general.

Firmado electrónicamente por:
YU LUNG LI
Validar Documento con FirmaEC

Ing. Yu Lung Li

Elaborador por: Peter Andrés Merino Lara	**Validado por:** Abg. Mg. José Luis Romo Santana