Maestría en

Derecho Digital

Trabajo de investigación previo a la obtención del título de

Magíster en Derecho Digital con mención en innovación legal y nuevas tecnologías

AUTORES:

Astrid Karolina Salazar Jumbo

Diego Fernando Huiracocha Rueda

Darwin Jeovanny Quinche Labanda

Josué Israel Alvear Zapata

María Isabel Peña Mogrovejo

TUTORES:

Docente titulación

Francisco Játiva Yánez

Cristian Martínez

Juan Manuel de Faramiñán Fernández-Fígares

PROTECCIÓN DE DATOS PERSONALES EN LA UNIVERSIDAD TÉCNICA DE MACHALA

Quito, enero, 2025

Certificación de autoría

Nosotros, Astrid Karolina Salazar Jumbo, Diego Fernando Huiracocha Rueda, Darwin Jeovanny Quinche Labanda, Josué Israel Alvear Zapata y María Isabel Peña Mogrovejo, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador (UIDE), para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Firmado electrónicamente por:
ASTRID KAROLINA SALAZAR JUMBO

Astrid Karolina Salazar Jumbo

DIEGO FERNANDO HUIRACOCHA RUEDA

Firmado digitalmente por DIEGO FERNANDO HUIRACOCHA RUEDA

Diego Fernando Huiracocha Rueda

Firmado electrónicamente por:
DARWIN JEOVANNY QUINCHE LABANDA

Darwin Jeovanny Quinche Labanda

JOSUE ISRAEL ALVEAR ZAPATA

Firmado digitalmente por JOSUE ISRAEL ALVEAR ZAPATA

Josué Israel Alvear Zapata

Firmado electrónicamente por:
MARIA ISABEL PENA MOGROVEJO

María Isabel Peña Mogrovejo

Autorización de Derechos de Propiedad Intelectual

Nosotros, **Astrid Karolina Salazar Jumbo, Diego Fernando Huiracocha Rueda, Darwin Jeovanny Quinche Labanda, Josué Israel Alvear Zapata y María Isabel Peña Mogrovejo,** en calidad de autores del trabajo de investigación titulado **Protección De Datos Personales En La Universidad Pública**, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, 26 de enero de 2025

Firmado electrónicamente por:
ASTRID KAROLINA SALAZAR JUMBO

Astrid Karolina Salazar Jumbo

DIEGO FERNANDO HUIRACOCHA RUEDA

Firmado digitalmente por DIEGO FERNANDO HUIRACOCHA RUEDA

Diego Fernando Huiracocha Rueda

Firmado electrónicamente por:
DARWIN JEOVANNY QUINCHE LABANDA

Darwin Jeovanny Quinche Labanda

JOSUE ISRAEL ALVEAR ZAPATA

Firmado digitalmente por JOSUE ISRAEL ALVEAR ZAPATA

Josué Israel Alvear Zapata

Firmado electrónicamente por:
MARIA ISABEL PENA MOGROVEJO

María Isabel Peña Mogrovejo

Aprobación de dirección y coordinación del programa

Nosotros, **Juan Manuel de Faramiñán Fernández-Fígares y Francisco Játiva Yánez.,** declaramos que los graduandos: **Astrid Karolina Salazar Jumbo, Diego Fernando Huiracocha Rueda, Darwin Jeovanny Quinche Labanda, Josué Israel Alvear Zapata y María Isabel Peña Mogrovejo** son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.

DE FARAMIÑAN FERNANDEZ-FIGARES JUAN MANUEL - 74666256E

Firmado digitalmente por DE FARAMIÑAN FERNANDEZ-FIGARES JUAN MANUEL - 74666256E
Fecha: 2025.03.24 08:41:13 +01'00'

Juan Manuel de Faramiñán Fernández-Fígares
Director/a de la
Maestría en Derecho Digital con mención en Innovación Legal y Nuevas Tecnologías

Firmado electrónicamente por: FRANCISCO JOSE JATIVA YANEZ

Francisco Játiva Yánez.
Coordinador/a de la
Maestría en Derecho Digital con mención en Innovación Legal y Nuevas Tecnologías

DEDICATORIA

Dedicamos este trabajo con amor a nuestras familias, que con su guía, valores y apoyo incondicional han sido el pilar fundamental en nuestro camino.

A nuestros amigos, quienes con su compañía y aliento constante nos han inspirado a seguir adelante en los momentos de dificultad.

Y a nuestros compañeros de vida, que con su comprensión, motivación y confianza en nosotros nos han impulsado a alcanzar nuevos metas, este trabajo también es suyo, porque cada palabra y esfuerzo aquí plasmados llevan consigo el reflejo de su apoyo y amor.

AGRADECIMIENTOS

Agradecemos a nuestros profesores quienes nos guiaron de manera invaluable en toda la maestría y en la realización de este trabajo.

A nuestras familias por su amor y apoyo incondicional que nos impulsó a lo largo de este logro académico.

A nuestros amigos, que con su alegría y buen humor lograron motivarnos en los momentos complicados.

Y a nuestros compañeros de vida que con su amor, comprensión y apoyo incondicional fueron imprescindibles para poder alcanzar este logro.

RESUMEN

Este trabajo analiza la importancia de la protección de datos personales en la Universidad Técnica de Machala en el contexto de la Ley Orgánica de Protección de Datos del Ecuador, vigente desde mayo de 2021. En este contexto, se analiza la primera política de protección de datos personales aprobada por la referida Universidad en el año 2024. Para el efecto, se comienza con un análisis detenido de la política, para luego identificar aspectos que cumplen la normativa vigente y, respecto de aquellos que no lo hacen o no de una manera satisfactoria, se proponen regulaciones que pueden llevarse a cabo.

Palabras Claves: Datos personales, universidad pública, privacidad, protección.

ABSTRACT

This study examines the significance of personal data protection at the Technical University of Machala within the framework of Ecuador's Organic Law on Data Protection, effective since May 2021. In this context, the first personal data protection policy approved by the University in 2024 is analyzed. The analysis begins with a thorough review of the policy to identify elements that comply with current regulations. For those aspects that do not meet the standards or do so insufficiently, regulatory recommendations are proposed for implementation.

Keywords: Personal data, public university, privacy, protection.

UIDE Powered by Arizona State University

eig Business School

TABLA DE CONTENIDOS

INDICE DE TABLAS

CAPITULO 1

1.1. Introducción

En Ecuador, a partir del 26 de mayo de 2021 entró en vigor la Ley Orgánica de Protección de Datos que recoge los aspectos más importantes sobre la materia. En ella, constan definiciones importantes, procedimientos, autoridades y responsabilidades en torno a la materia en cuestión, todo lo cual, debe ser observado por quienes traten datos personales. Con lo cual, la protección de datos personales se torna en una obligación con normas cada vez más claras.

Actualmente, la protección de datos carácter personal se ha convertido en uno de los que más ha generado interés por parte de la comunidad jurídica no solo del Ecuador sino del mundo, tanto por su novedad, como porque se presenta, en buena medida, como una rama del Derecho en la que hay mucho por explorar. Cabe matizar que la anterior afirmación es más notable en países como Ecuador que, por su nivel de desarrollo tecnológico, está experimentando sus primeros pasos en la materia y dentro de nuestro país, el sector público es el espacio donde es posible notar un grado temprano de aplicación de la normativa vigente.

En este contexto, de novedad y oportunidad de desarrollo jurídico, en el presente trabajo se resaltan justamente las dos cualidades mencionadas pues, si bien en Ecuador ya se cuenta con una Ley y su respectivo Reglamento en la materia y en varios ámbitos ya se va aplicando la normativa existente, no es menos cierto que, especialmente en el ámbito público, se hace más notable que la protección de datos personales está en construcción.

En tal virtud, el presente trabajo ha considerado importante centrar su estudio en una entidad pública que presenta un desarrollo temprano de políticas de protección de datos personales y que maneja una considerable cantidad de estos, nos referimos a la Universidad Técnica de Machala.

Así, el presente trabajo, en su marco teórico, examina la evolución del concepto de protección de datos personales, fundamentando los derechos asociados y explorando los desafíos y retos en la implementación en universidades públicas. Se presentan definiciones clave como datos personales, datos sensibles, responsable y encargado del tratamiento, consentimiento informado y violación de la seguridad de los datos. El marco legal analiza la normativa y autoridades nacionales y compara el derecho con otros países, proporcionando una visión comparativa y contextual.

Posteriormente, se aproxima al tema central del presente trabajo, pues se aborda tres cuestiones relevantes: (i) un análisis con respecto a la política de protección de datos personales que maneja la Universidad, lo cual permitió, (ii) identificar y describir los aspectos que no incumplirían con las normas de protección de datos, a fin de (iii) proponer políticas de fortalecimiento, perfeccionamiento o a su vez en caso de ser necesario incluir la implementación de políticas de protección de datos acorde a la normativa vigente.

Este proyecto considera los desafíos y riesgos de la vulneración de la privacidad, el desconocimiento sobre cómo se puede utilizar datos personales de los miembros de las universidades públicas, la necesidad de un consentimiento y el resguardo de la privacidad de la comunidad en general tanto de manera presencial como la modalidad en línea, a su vez proponer alternativas de perfeccionamiento o solución en las políticas, prácticas y

procedimientos que pueden ser empleadas por la Universidad para asegurar un adecuado cumplimiento de la normativa vigente sobre tratamiento de datos personales.

Finalmente, este trabajo realiza recomendaciones prácticas a la Universidad Técnica de Machala que le permitirán ser una institución que cumpla de manera satisfactoria las normas vigentes de protección de los datos que trata.

1.2.Planteamiento del Problema e Importancia del Estudio

1.2.1. Definición del proyecto

El presente proyecto tiene por objeto resolver la siguiente pregunta: ¿Cuáles son las políticas que la Universidad Técnica de Machala debe implementar para la protección de datos personales que trata y así garantizar el cumplimiento de la normativa vigente?

1.2.2. Naturaleza o tipo de proyecto

Buscamos obtener una comprensión profunda y detallada de cómo la Universidad Técnica de Machala maneja los datos personales. Esto incluye evaluar si las políticas y prácticas actuales cumplen con las normativas legales y proponer mejoras para asegurar una gestión de los datos más segura y eficiente. Garantizar que la privacidad de los estudiantes, docentes y personal administrativo esté protegida y que se adopten las mejores acciones en cuanto a seguridad y manejo de la información.

Además, buscamos que esta investigación sirva como hoja de ruta para que la universidad implemente política y prácticas efectivas que garanticen la seguridad y privacidad de la información personal de estudiantes, profesores y personal administrativo. La identificación de los riesgos y vulnerabilidades actuales, proponiendo soluciones alineadas con las normativas nacionales e internacionales sobre protección de datos incluyendo la creación de

protocolos de manejo seguro de la información, la formación de una cultura de privacidad y responsabilidad digital entre la comunidad universitaria, y el establecimiento de sistemas de seguridad que protegen la integridad de los datos frente a amenazas tecnológicas

El fin último es fortalecer los mecanismos de protección de datos de la Universidad Técnica de Machala, a través del análisis, evaluación y propuesta de perfeccionamiento o solución de problemas en el tratamiento de los datos que gestiona la referida Universidad

1.3.Objetivos

1.3.1. Objetivo general

Analizar las políticas, procedimientos y prácticas de tratamiento de datos personales en la Universidad Técnica de Machala, con el fin de evaluar el cumplimiento de las normativas vigentes con base en lo cual se pueda proponer mejoras para garantizar una gestión segura y eficiente de los datos que trata la Universidad.

1.3.2. Objetivos específicos

- Identificar las políticas, prácticas y procedimientos actuales de tratamiento y protección de los datos personales que trata la Universidad Técnica de Machala.
- Evaluar las políticas, prácticas y procedimientos actuales de tratamiento y protección de los datos personales que trata la Universidad Técnica de Machala.
- Proponer alternativas de perfeccionamiento o solución en las políticas, prácticas y procedimientos que pueden ser empleadas por la Universidad Técnica de Machala para asegurar un adecuado cumplimiento de la normativa vigente sobre tratamiento de datos personales.

1.4. Metodología

Consideramos adecuado identificar los métodos de investigación que se van a utilizar, puesto que aquello es el fundamento metodológico que asegura la fiabilidad de nuestra investigación. Así, consideramos que nuestra investigación tiene un carácter mixto entre cualitativa y cuantitativa.

Cualitativa puesto que en este tipo de investigaciones se "selecciona cuando el propósito es examinar la forma en que los individuos perciben y experimentan los fenómenos que los rodean, profundizando en sus puntos de vista, interpretaciones y significados" (Hernández, 2014). Es decir, nuestro trabajo se centrará en obtener información teórica detallada y profunda sobre la implementación de un manual general de protección de datos dentro de una universidad pública. Las ventajas de este enfoque investigativo son, entre otras, las siguientes:

- Permite obtener información teórica precisa y actualizada
- Promueve la generación de nuevas teorías e hipótesis.

Para el efecto, se ha realizado una investigación mayormente bibliográfica la cual, además de considerar normativa y jurisprudencia nacional e internacional, incluye el estudio y análisis de libros y artículos científicos sobre el tema de esta investigación.

CAPITULO 2

2.1. Marco teórico y normativo

El presente trabajo aborda la protección de datos personales dentro de la Universidad Técnica de Machala. Se escogió esta institución de educación superior por cuando se contó con facilidad para acceder a la información necesaria para los fines de esta investigación.

En este sentido, el trabajo aborda, en primer lugar, un suficiente marco teórico que permite comprender dos teorías que explican la protección de datos personales como un desarrollo del derecho a la intimidad o a la privacidad, para luego hacer un análisis descriptivo de las normas con que cuenta la Universidad Técnica de Machala en la materia en mención y, finalmente, evaluar si aquello cumple o no con el mandato constitucional y legal de protección y, en los aspectos en los que no se cumpla o sea perfectible, esgrimir propuestas que satisfagan la obligación referida.

2.2.Principales teorías que explican la protección de datos personales

Es bastante conocido que el objeto del Derecho Digital es estudiar las prácticas argumentativas que nacen a propósito del uso generalizado de datos digitales en la sociedad. Es decir, el Derecho Digital se interesa por las relaciones jurídicas en torno al dato digital. En ese sentido, una de las principales aristas de esta rama del Derecho es la Protección de Datos Personales. Tal es así que “este acervo normativo de nuevo cuño pivota entre dos grandes tensiones: la necesidad de generar entornos que impulsen el uso de los datos digitales para potenciar la economía digital, por un lado, y la necesidad de regular y limitar su uso para asegurar que se crea una economía digital segura, democrática y justa, por otro” (López-Lapuente, 2021).

Ahora bien, para los fines de esta investigación, nos ceñiremos a los datos personales que son objeto de protección por el Derecho. Así, antes de intentar una conceptualización, es pertinente conocer el fundamento de la protección de datos, con el fin de abordar de manera integral la cuestión que se aborda.

Existen varias teorías que se utilizan como fundamento de la protección de datos, principalmente aquellas que desarrollan el derecho a la privacidad o a la intimidad. La primera que consideramos imprescindible traer a colación es la "Teoría de las Esferas". Como bien lo recoge Polo Roca (2022, p. 316) esta teoría de origen alemán fue propuesta por Heinrich Hubmann y luego desarrollada por el Tribunal Constitucional Alemán, así como por el Tribunal Federal de Justicia de Alemania. Esta teoría busca responder a la pregunta de ¿cuándo se vulnera el derecho a la intimidad? Para ello, explica que la intimidad de una persona está compuesta por tres esferas concéntricas, siendo la más interna la que mayor protección merece y, la más externa, la que menos. Hubmann propuso que la intimidad está compuesta, desde adentro hacia afuera, por: (i) la "esfera íntima", en la que se encuentran las cuestiones secretas de las personas; (ii) la "esfera privada", que corresponde a la vida de carácter privado, personal y familiar; y, (iii) la "esfera individual", en donde se encuentran cuestiones casi públicas como el honor o la imagen de la persona (Polo Roca, 2022, p. 317).

Como toda teoría, presenta variantes, principalmente respecto de la división entre una esfera y otra y la cantidad de aquellas. Sin embargo, "hay una posición generalizada de cuáles son las dos principales esferas: la esfera íntima […] y la esfera o círculo privados" (Polo roca, 2022, p. 319). Así pues, esta teoría acierta en explicar que la intimidad no es algo sencillo, pues para determinar su vulneración hace falta determinar el grado de relación que tiene la

información de la persona con su derecho fundamental a la dignidad. En otras, palabras, las esferas permiten ilustrar con cierta precisión que la intimidad tiene varios ámbitos según el desarrollo de la persona y que, dependiendo del grado de cercanía a la dignidad de la persona, mayor será el grado de protección que debe brindar el Derecho.

Sin embargo, consideramos que no es la óptima para describir el derecho a la intimidad y, a la larga, para comprender la protección de datos personales. Al respecto, conviene abordar otra teoría: la del Mosaico.

La denominada Teoría del Mosaico fue propuesta por Fulgencio Madrid Conesa en 1984, y concibe que los datos personales por sí solos no tiene información suficiente para poner en riesgo los derechos de sus titulares, sino que, como en un mosaico, el conjunto de datos es lo que permite evidenciar la relevancia de la información que se pretende proteger. Un ejemplo pertinente de esta teoría es el siguiente: al matricularnos en una institución educativa, proporcionamos datos como dirección, nombre completo, información de contacto e historial académico, entre otros. Individualmente, estos datos no representan un gran riesgo o vulneración de privacidad, pero al estar todos reunidos en un solo documento o ficha de información, el riesgo aumenta significativamente. Al estar concentra-dos en una única fuente, estos datos personales se convierten en un mosaico que, en su conjunto, expone información sensible.

En tal virtud, consideramos que el fundamento de esta teoría es adecuado para comprender la protección de los datos en el contexto de un estado constitucional. Así, conviene resaltar que lo que el derecho protege, más allá de datos, es el derecho a la intimidad

o a la privacidad. Dicho de otro modo, las reglas del Derecho de Protección de Datos Personales son garantías del derecho a la intimidad o a la privacidad.

2.3. Definiciones y conceptos clave

Como se anticipó en párrafos anteriores y considerando la relevancia de comprender el significado exacto de los términos que se emplearán en el desarrollo de este trabajo, resulta fundamental establecer definiciones claras y específicas de conceptos relevantes.[1] Esto no solo facilita la correcta interpretación del contenido, sino que también asegura la coherencia y precisión en el tratamiento de los temas abordados.

Datos personales. Según el Reglamento General de Protección de Datos (RGPD, 2016) los "datos personales son toda información sobre una persona física identificada o identificable … directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona." Los datos personales, de manera sencilla, comprenden toda la información que, directa o indirectamente, permite identificar que una persona sea identificada.

Datos personales sensibles. Son aquellos datos que poseen características particulares que los hacen diferentes caracterizándose por ser información delicada lo que hace que cuente con un tratamiento diferenciado y con mayor rigurosidad en comparación con otros tipos de información. Estos datos, al ser considerados delicados, van más allá de los que

[1] Así, la lista de términos recogidos no pretende ser exhaustiva.

cotidianamente podrían ser conocidos o utilizados en el ámbito general, ya que pueden revelar información extremadamente personal como, por ejemplo, los datos genéticos, biométricos, los cuales permiten identificar a un individuo de manera única mediante características físicas únicas; y los datos relacionados con el estado de salud, entre otros.

Responsable del tratamiento de datos. De acuerdo con la Ley Orgánica de Protección de Datos Personales ("LOPDP"), se trata de la "persona natural o jurídica, pública o privada, autoridad, u otro organismo, que solo o juntamente con otros decide sobre la finalidad y el tratamiento de datos personales." (LOPDP, 2021, art. 4). Considerando esta definición podemos entender que el responsable tiene la autoridad y la obligación de determinar los objetivos para los cuales se recopilan y procesan los datos personales, así como de establecer las condiciones y procedimientos.

Encargado del tratamiento de datos: De acuerdo con el artículo 4 de la LOPDP, el encargado es la "persona natural o jurídica, pública o privada, autoridad, u otro organismo que solo o juntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales." Considerando esta definición, podemos entender que el encargado de datos es quien procesa y gestiona los datos en nombre del responsable. Teniendo como diferencia que el responsable de datos tiene la obligación legal de garantizar el cumplimiento de la normativa de protección de datos, mientras que el encargado de datos trabaja a raíz de las instrucciones dadas por el responsable.

Consentimiento informado: De acuerdo con la CEPAL, "se denomina consentimiento informado, cuando antes de obtener el consentimiento, se describe al sujeto de investigación lo que se va a hacer con sus datos, quién tendrá acceso a ellos y cómo van a ser publicados".

(Comisión Económica para América Latina y el Caribe [CEPAL], s. f.,) Es decir el consentimiento informado es aquel que se otorga con total conocimiento, basado en la información proporcionada previamente. En esta se detalla qué tipo de datos se tratarán, los fines específicos de su uso y cualquier implicación asociada. Este proceso asegura que la persona comprenda cómo serán gestionados sus datos antes de aceptarlo.

Vulneración de datos personales. Consiste en acceder, tratar, apropiarse o manipular de manera ilegítima datos personales. En general se trata de una conducta genérica que describe la intromisión indebida en los datos personales, esto puede ocurrir de diferentes maneras y en múltiples escenarios, por ejemplo, cuando fallas en los sistemas de seguridad exponen información personal, dejándola accesible a terceros malintencionados.

2.4. Desafíos y retos en la Protección de Datos Personales en una institución de educación superior en Ecuador

La implementación de la protección de datos personales en las instituciones de educación superior en Ecuador enfrenta múltiples desafíos, que surgen tanto por la reciente promulgación de la Ley Orgánica de Protección de Datos Personales como por la realidad operativa de estas instituciones. Según Enríquez (2021) “la protección de datos personales en Ecuador está regulada de manera dispersa, imprecisa, y no está enfocada en los desafíos que presentan las tecnologías de la información”

Es decir, la falta de conocimiento y sensibilización sobre la normativa es uno de los obstáculos principales, muchas instituciones no han desarrollado políticas claras para garantizar el cumplimiento de la ley, lo que incluye aspectos como el consentimiento informado, la confidencialidad y la transparencia en el manejo de datos personales, este

problema no solo afecta a las áreas administrativas, sino también a la comunidad estudiantil y docente, que a menudo desconocen sus derechos y responsabilidades en esta materia.

Otro desafío importante radica en la infraestructura tecnológica. Muchas universidades no cuentan con sistemas adecuados para gestionar y proteger datos de manera segura, lo que las hace vulnerables a ciberataques y filtraciones de información. En este contexto, la interoperabilidad se presenta como una solución clave, ya que es un servicio creado y administrado por la Dirección Nacional de Registros Públicos (DINARP) mismo que consiste en facilitar a las entidades públicas el acceso e intercambio de información de los ciudadanos de manera controlada, segura, oportuna y transparente con base en las competencias de cada institución, mediante la construcción de servicios web para uso en aplicaciones. (Resolución 005-NG-DINARDAP, 2019)

Asimismo, existe un reto cultural en el ámbito educativo ecuatoriano. La protección de datos requiere un cambio de paradigma en la manera en que las instituciones gestionan la información, muchas veces, las prácticas tradicionales, como el uso de documentos físicos y sistemas informales, dificultan la adopción de procesos más seguros y estandarizados, esto se suma a la necesidad de capacitar al personal administrativo y académico, lo cual implica diseñar programas formativos que promuevan una cultura de privacidad y seguridad de la información en todos los niveles institucionales. En este contexto, Díaz señala que “las Universidades tratan diariamente un volumen muy alto de información, propiciado por el uso de herramientas que colaboran a la digitalización de la información y a su utilización más eficiente e inmediata”. (Díaz Lima, 2023)

Por lo que la Universidad Técnica de Machala enfrenta desafíos significativos en la implementación de la protección de datos, como la actualización de políticas internas para alinearlas con la Ley Orgánica de Protección de Datos Personales. Este proceso implica reestructurar procedimientos administrativos y académicos, lo que requiere un esfuerzo coordinado y un compromiso institucional entre todos los departamentos. Así, sabemos que "la universidad es probablemente uno de los agentes sociales que más datos personales maneja" (Conde y Cazurro, 2017, 3)

Al implementar estas recomendaciones, la institución podría enfrentar limitaciones presupuestarias y la falta de personal especializado, lo que retrasaría la adopción de soluciones tecnológicas y normativas adecuadas. Sin embargo, es crucial que la universidad mantenga un compromiso decidido para fomentar una cultura de privacidad, entendido no solo como una obligación legal, sino como un componente fundamental de su responsabilidad social y ética institucional.

Todo lo anterior, se puede sintetizar de la siguiente manera:

Infraestructura tecnológica limitada: el nivel de protección de datos personales es directamente proporcional al grado de tecnología que utiliza la Universidad. Una mayor capacidad tecnológica representa mayor posibilidad de implementar políticas y técnicas de protección, que si tuviera tecnología antigua o desactualizada.

Capacitación del Personal: así como es importante contar con tecnología propicia para la protección de datos, también lo es tener personal capacitado tanto en aspectos normativos como tecnológicos. Aquí también se puede observar una proporcionalidad, pues a mayor capacitación del personal, mayor seguridad en la protección de datos existe.

Recursos Financieros: Este es quizá uno de los retos más importantes que enfrenta la Universidad Técnica de Machala, pues, al igual que muchas instituciones públicas del país, sus recursos no siempre son los más generosos, considerando además que la implementación de sistemas confiables de protección de datos requiere, dependiendo de la situación de la institución, una inversión significativa.

Evaluaciones de impacto en la protección de datos: si bien es algo que está regulado por la Ley, las evaluaciones en mención no siempre son procesos sencillos ni económicos. Así, un reto en la implementación de un sistema de protección de datos para la Universidad debe considerar los recursos que se utilizarán en las evaluaciones que se requiera conforme la normativa vigente.

Cumplimiento normativo: la Universidad debe contar con personal capacitado y exclusivo a fin de no incurrir en faltas o vulneraciones de protección de datos. Esto que puede parecer evidente, puede convertirse en un reto para la Universidad si no designa a un profesional en la materia y que este dedique la mayoría de su tiempo a estas funciones.

2.5. Normativa nacional en materia de protección de datos

En el contexto actual, la protección de los datos personales se ha convertido en un derecho fundamental dentro de los sistemas jurídicos de diversos países, incluida Ecuador. A fin de proporcionar un análisis comprensivo, es crucial entender las bases normativas que respaldan la protección de datos personales, tanto en la Constitución de la República del Ecuador como en leyes específicas y regulaciones emitidas por instituciones de educación superior, como las universidades. Este análisis detallará cómo la Constitución de 2008 y la Ley Orgánica de Protección de Datos Personales (LOPDP) de 2021 establecen un marco

jurídico robusto para la protección de los datos personales, con especial énfasis en las responsabilidades de las universidades, como la Universidad Técnica de Machala.

2.5.1. Protección de Datos Personales en la Constitución de la República del Ecuador

La Constitución de la República del Ecuador, promulgada en 2008, reconoce la protección de los datos personales como un derecho fundamental que tenemos como humanos, lo que otorga una base sólida para su salvaguarda en todo el país. En este contexto, el artículo 66, numerales 19 y 20, establece de manera explícita los derechos de los ciudadanos en relación con sus datos personales.

Derecho a la intimidad y privacidad (Art. 66, Numerales 19 y 20)

El numeral 19 de la Constitución reconoce "el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley" (Constitución de la Republica del Ecuador, 2008). De esta manera podemos entender que el derecho a la protección de los datos personales busca garantizar que los individuos tengan acceso a su información personal y control sobre ella. Esto significa que cualquier tipo de recolección, almacenamiento, tratamiento o distribución cuente con el consentimiento del titular o el respaldo de una orden legal. Este principio de autodeterminación informativa permite a las personas decidir cómo se maneja su información personal.

Por otro lado, el numeral 20 de la Constitución extiende "El derecho a la intimidad personal y familiar." (Constitución de la Republica del Ecuador, 2008) lo cual nos permite entender que la protección a la intimidad personal y familiar busca resguardar a los ciudadanos contra cualquier tipo de intrusión indebida, incluyendo el uso no autorizado de sus datos personales. Este derecho a la privacidad se extiende no solo al ámbito físico, sino también a la esfera digital, donde los datos personales de los individuos están igualmente protegidos.

Obligaciones de las Instituciones Públicas y Privadas (Art. 92) El artículo 92 de la Constitución establece que "toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos." (Constitución de la Republica del Ecuador, 2008) de este artículo es posible entender que las personas tienen derecho a acceder a toda información que se haya recopilado en las bases de datos. Es importante destacar que este derecho tiene especial relevancia para las universidades, esto debido a que son responsables del tratamiento de datos personales de estudiantes, docentes y personal administrativo.

2.5.2. Ley Orgánica de Protección de Datos Personales

La Ley Orgánica de Protección de Datos Personales ("LOPDP"), que entró en vigor el 26 de mayo de 2021, establece un marco legal detallado para el tratamiento de los datos

personales en Ecuador. Esta ley sirve como refuerzo de las disposiciones constitucionales sobre la protección de los datos y especifica los principios, derechos y responsabilidades en su manejo. A continuación, se recoge su contenido más destacable:

Tema	Artículos
Objeto y finalidad	Art. 1
Ámbito de aplicación	Arts. 2 y 3
Definiciones	Art 4
Integrantes del sistema de protección de datos	Art. 5
Condiciones para el tratamiento legítimo de datos	Art. 7
Consentimiento y su validez	Art. 8
Interés legítimo	Art. 9
Principios	Art. 10
Derechos de los titulares de los datos	Arts. 11 al 24
Categorías especiales de datos	Art. 25
Tratamiento de datos especiales	Arts. 26 al 32
Transferencia y acceso a datos por terceros	Arts. 33 al 36
Criterios de seguridad de datos personales	Arts. 37 al 46
Responsable, encargado y delegado de protección de datos	Art. 47 al 51
Criterios de responsabilidad proactiva	Arts. 52 al 54
Transferencia internacional de datos	Arts. 55 al 61
Requerimientos directos y procedimiento administrativo de reclamo	Arts. 62 al 64
Régimen sancionatorio	Arts. 65 al 74
Autoridad de protección de datos personales	Arts. 75 al 77
Disposiciones Generales	Nueve
Disposiciones Transitorias	Cuatro
Disposiciones Reformatorias	Cuatro
Disposiciones Derogatorias	Cuatro
Disposición Final	Una

***Tabla 1**: Contenido destacados de la LOPDP*

Elaborada por Astrid Salazar, Diego Huiracocha, Darwin Quinche, Josué Alvear y María Peña

El propósito del cuadro anterior es presentar un esquema a manera de índice temático de los contenidos de la LOPDP, lo cual permite tener un breve vistazo de los aspectos que regula. Sin embargo, para los fines de esta investigación, se desarrollan algunos aspectos normativos más relevantes de la referida Ley.

Principios Rectores del Tratamiento de Datos (Art. 10). El artículo 10 de la LOPDP establece una serie de principios rectores que deben seguir las instituciones, incluyendo las universidades, al tratar los datos personales. Entre estos principios destacan:

- Transparencia: "El tratamiento de datos personales deberá ser transparente por lo que toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro." (LOPDP, 2021). Este principio nos da la posibilidad de entender que nuestros datos deben ser realizado de manera ética y transparente, basándose en el consentimiento informado del titular de los datos.
- Finalidad: "Las finalidades del tratamiento deberán ser determinadas, explícitas, legítimas y comunicadas al titular" (LOPDP, 2021). Entendiéndose que la finalidad con la que se utilicen los datos debe ser determinada, en este sentido las universidades solo pueden utilizar los datos personales para fines específicos, como la gestión académica, administrativa o de investigación, siempre y cuando así lo haya indicado el titular.
- Pertinencia y minimización de los datos: "Los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento" (LOPDP, 2021) Este principio nos establece que solo se

deben solicitar los datos que sean estrictamente necesarios, con respecto a este principio la universidad debe recoger solo aquellos datos que sean estrictamente necesarios para cumplir con sus fines.

- Confidencialidad: "El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley." (Ley orgánica de Protección de datos personales, 2021). Estos principios nos mencionan la importancia de la confidencialidad. Debido a esto las universidades deben garantizar la protección técnica de las bases de datos, implementando medidas que sean adecuadas para evitar el acceso no autorizado a los datos que tratan.

Consentimiento (Art. 8). La LOPDP establece que "Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo." (Ley orgánica de Protección de datos personales, 2021) Con esto se puede entender que el consentimiento es obligatorio y necesario para cualquier que sea posible la recolección y tratamiento de los datos de carácter personal, salvo algunas excepciones previstas en la ley, como cuando se trate de datos necesarios para la protección del interés público. Esto implica que las universidades para las universidades es obligatorio obtener el consentimiento explícito de los estudiantes, docentes y empleados antes de recolectar sus datos personales.

Datos Sensibles (Art. 4). La ley pone un énfasis especial en la protección de los datos sensibles, debido a que estos datos son los "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" (Ley orgánica de Protección de datos personales, 2021) Es por ello que las universidades al tratar una gran cantidad de datos que llegan a recabar deben ser especialmente cautelosas al manejar este tipo de datos, adoptando medidas adicionales de seguridad y asegurando que solo se recojan cuando sea estrictamente necesario y con el consentimiento adecuado.

Derechos de los Titulares de Datos (Art. 13, 14, 15, 16). La LOPDP otorga a los titulares de los datos varios derechos fundamentales, que incluyen:

- Acceso: La ley en su artículo 13 nos menciona que "el titular tiene derecho a conocer y a obtener, gratuitamente, del responsable de tratamiento acceso a todos sus datos personales y a la información detallada en el artículo precedente, sin necesidad de presentar justificación alguna." (LOPDP, 2021) Lo que nos permite ver que este es el derecho a tener conocimiento sobre qué datos son tratados por la universidad y cuál es su finalidad.
- Rectificación: El artículo 14 establece que "El titular tiene el derecho a obtener del responsable del tratamiento la rectificación y actualización de sus datos personales inexactos o incompletos." (Ley orgánica de Protección de datos personales, 2021) Esto implica el derecho de las personas de poder modificar y corregir datos que hayan sido erróneos.
- Eliminación: El artículo 15 establece que "El titular tiene derecho a que el responsable del tratamiento suprima sus datos personales" En este sentido por ejemplo podemos encontrar al derecho de eliminación de los datos, cuando estos ya hayan cumplido su fin y ya no sean necesarios.

- Oposición: La ley establece que “El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales” (LOPDP) De esta manera como su nombre bien lo indica este derecho nos permite oponernos al uso de nuestros datos personales cuando este no ha sido autorizado.

Estos derechos permiten que los estudiantes, docentes y empleados mantengan el control sobre su información personal en todo momento.

Responsabilidad (Art. 47). El artículo 47 de la Ley estable las obligaciones relacionadas al responsable y al encargado de tratamiento de datos personales. Con respecto al tema de investigación como responsables del tratamiento de los datos personales, las universidades tienen una serie de responsabilidades clave, que incluyen:

- La designación de un delegado de protección de datos personales.
- Implementar políticas internas de tratamiento de datos, incluidas las medidas de seguridad adecuadas.
- Notificar a las autoridades competentes y a los titulares en caso de violaciones de seguridad.

2.6.Normativa internacional en materia de protección de datos

Para los fines de este trabajo, no se podía dejar de lado una inclusión de normativa internacional en la materia, con el fin de corroborar que los contenidos desarrollados por la LOPDP tengan concordancia con criterios internacionales. Para el efecto, se ha considerado resaltar el Reglamento General de Protección de Datos de la Unión Europea (“RGPD”).

Dicho documento, que data del año 2016, es la normativa insigne en protección de datos que, como veremos, sirvió de fuerte inspiración para la LOPDP. Este documento contiene elementos fundamentales de la materia, mismos que se recogen a continuación:

Tema	Artículos
Objeto	Art. 1
Ámbitos de aplicación	Arts. 2 y 3
Definiciones	Art 4
Principios	Art. 5
Licitud y condiciones para el tratamiento de datos	Arts. 6 al 8
Tratamiento de categorías especiales de datos personales	Arts. 9 al 11
Derechos de los interesados	Arts. 12 al 23
Responsable y encargado del tratamiento de datos personales	Arts. 24 al 31
Seguridad de los datos personales	Arts. 32 al 34
Evaluación de impacto	Arts. 35 y 36
Delegado de protección de datos	Arts. 37 al 39
Códigos de conducta y certificación	Arts. 40 al 43
Transferencia de datos personales a terceros u organizaciones internacionales	Arts. 44 al 50
Autoridades de control	Arts. 51 al 76
Recursos, responsabilidad y sanciones	Arts. 77 al 84
Disposiciones relativas a situaciones específicas de tratamiento	Arts. 85 al 91
Actos delegados y actos de ejecución	Arts. 92 al 93
Disposiciones finales	Arts. 94 al 99

***Tabla 2**: Contenido de la RGPD*

Elaborada por Astrid Salazar, Diego Huiracocha, Darwin Quinche, Josué Alvear y María Peña

Ahora bien, de la tabla N° 2 se puede observar que el RGPD regula aspectos sustanciales de la protección de datos en el marco de la Unión Europea. Dado que los fines de esta investigación no se relacionan con un estudio comparativo de normativa, es suficiente con la información constante en la referida tabla. Así, la Tabla N° 2 es útil para esta investigación en

la medida en la que permite evidenciar que la normativa ecuatoriana se adecua de una buena manera a la normativa insigne de protección de datos.

Así, basta un vistazo general de los contenidos reseñados en las tablas N° 1 y N° 2 para notar que la normativa ecuatoriana, como se anunció antes, muestra una fuerte inspiración en el RGPD. Esta similitud es evidente no solo por la estructura de la norma sino también por los contenidos abordados, es decir, la LOPDP ha recogido buena parte de los criterios constantes en el RGPD.

Esto, cabe señalar, no parece ser producto de un mal ejercicio legislativo. La LOPDP ha logrado aterrizar las regulaciones constantes en el RGPD a la situación ecuatoriana, en la medida de que está consciente de que la actividad jurídica en la materia está en formación. En todo caso, lo analizado apoya los fines de la presente investigación porque, en el fondo, los criterios que debe cumplir la Universidad Técnica de Machala son, de alguna manera, los que se exigen en otras latitudes.

CAPITULO 3

Análisis del tratamiento y protección de datos actuales de la Universidad Técnica de Machala

3.1. Datos que trata la Universidad

La Universidad Técnica de Machala ("UTMACH") maneja una amplia variedad de datos que abarcan diferentes áreas académicas y administrativas.

Datos Académicos

- Tesis y Trabajos de Graduación: La UTMACH cuenta con un repositorio digital donde se almacenan y preservan tesis y trabajos finales de graduación.
- Artículos y Libros: Publicaciones académicas, artículos de investigación y libros escritos por docentes y estudiantes.
- Resultados de Investigación: Datos obtenidos de proyectos de investigación en diversas áreas del conocimiento.

Datos Administrativos

- Información de Estudiantes: Datos personales, calificaciones, historial académico y registros de inscripción.
- Información de Docentes y Empleados: Datos personales, contratos, historial laboral y evaluaciones de desempeño.
- Datos Financieros: Información sobre presupuestos, gastos, ingresos y otros aspectos financieros de la universidad.

Datos de Investigación

- Datos Científicos y Técnicos: Información recolectada durante investigaciones científicas y técnicas en diversas disciplinas.
- Datos de Proyectos Específicos: Información relacionada con proyectos específicos de investigación, incluyendo metodologías, resultados y conclusiones.

Datos de Recursos Educativos

- Materiales Didácticos: Libros de texto, guías de estudio, folletos y otros recursos educativos utilizados en las aulas.
- Recursos Digitales: Bibliografía digital, aulas virtuales, plataformas de aprendizaje en línea, entre otros.

Estos datos son esenciales para el funcionamiento y desarrollo de la UTMACH, y su protección y gestión adecuada son cruciales para mantener la confianza y la integridad académica.

3.2. Normativa de protección de datos de la Universidad Técnica de Machala

El Consejo Universitario de la UTMACH, mediante Resolución N° 0548-2024-CU-SO-30 de 28 de octubre 2024, aprobó la Política de Tratamiento de Datos Personales de la Universidad Técnica de Machala ("Política"). Este documento es el primero que emite la UTMACH en materia de protección de datos.

A fin de presentar una descripción detallada y fiel de los contenidos de la Política, se realiza citas textuales de sus acápites, acompañadas de breves comentarios al respecto.

0. Presentación de la política.

Se establece que contiene "los principios, responsabilidades y procedimientos que guiarán nuestras acciones en la recolección, uso, almacenamiento y protección de la

información personal de todos aquellos que interactúan con nuestra universidad, incluyendo estudiantes, profesores, colaboradores y terceros". Su objetivo es "garantizar que el tratamiento de los datos personales se realice en estricto cumplimiento con la normativa vigente, respetando los derechos de las personas y asegurando la integridad y confidencialidad de la información. Además, esta política refuerza nuestro compromiso con la ética y la responsabilidad social, pilares fundamentales de nuestra misión como institución educativa."

1. Introducción

> "La Universidad Técnica de Machala (UTMACH) está comprometida con la protección de los datos personales de todos los miembros de su comunidad universitaria y de aquellos que interactúan con la institución. En cumplimiento con la Ley Orgánica de Protección de Datos Personales del Ecuador, esta política establece los principios y directrices para el tratamiento y protección de datos personales recolectados y utilizados por la universidad."

En esta sección se describe el compromiso y responsabilidad de la UTMACH con la protección de datos y se establece que la Política se emite en cumplimiento de la LOPDP.

2. Responsable del tratamiento de los datos

UNIVERSIDAD TÉCNICA DE MACHALA
RUC: 0760001580001
Dirección: Av. Panamericana km 5 ½ Vía Pasaje
Correo electrónico: tramites@utmachala.edu.ec

La Política establece que el responsable del tratamiento de datos es la UTMACH y designa datos de identificación de la Universidad.

3. Alcance

> "Esta política se aplica a todos los procesos y actividades que involucren la recolección, almacenamiento, uso, divulgación, y eliminación de datos personales dentro de la UTMACH. Incluye a estudiantes, empleados, docentes, proveedores, y cualquier otra persona cuyos datos sean tratados por la universidad."

La Política determina que su alcance de la política abarca todos los procesos de tratamiento de datos provenientes de todas las personas cuyos datos se recopilan.

4. Definiciones

Se recogen definiciones sobre dato personal, dato sensible, titular del dato personal y tratamiento. Cabe señalar se ha preferido no referenciar estas definiciones porque son transcripciones de la ley.

5. Principios generales

- "Legalidad: Todos los datos personales serán tratados conforme a la Ley Orgánica de Protección de Datos Personales del Ecuador y demás normativas aplicables."
- "Transparencia: Los titulares de los datos serán informados de manera clara y precisa sobre el tratamiento de sus datos personales."
- "Finalidad: Los datos personales se recolectarán y tratarán solo para fines legítimos, específicos y explícitos."
- "Minimización de datos: Solo se recolectarán los datos personales necesarios para cumplir con la finalidad del tratamiento."
- "Exactitud: Los datos personales serán exactos y, cuando sea necesario, actualizados."
- "Seguridad: Se implementarán medidas técnicas y organizativas adecuadas para proteger los datos personales contra el acceso no autorizado, pérdida, destrucción o daño."

La Política reconoce principios de protección de datos personales tales como legalidad, transparencia, finalidad, minimización de datos, exactitud y seguridad. Al igual que las definiciones, también son extraídos de la LOPDP

6. Datos que se recolecta

"La UTMACH requerirá de los datos personales de: sus estudiantes, empleados, docentes, proveedores, postulantes a estudios, postulantes a empleos y cualquier otra persona que, de manera directa o indirecta, tenga relación con la institución. Podrá recopilar, agrupar, segmentar, organizar, estructurar, conservar, transferir, limitar y en general tratar los datos personales de los titulares conforme a lo establecido en la Ley Orgánica de Protección de datos personales y se podrá tratar en base a las siguientes categorías de datos:

- Información general
- Datos de nacimiento
- Domicilio
- Estudios secundarios
- Datos familiares
- Datos para ficha socioeconómica

Las categorías de datos serán determinados en cada caso dependiendo de las necesidades de la UTMACH, para el cumplimiento de sus objetivos."

En este acápite se menciona que la UTMACH, de acuerdo con la LOPDP, podrá tratar con los datos de sus estudiantes, empleados, docentes, proveedores, postulantes y otros, en función de seis categorías de datos, de acuerdo con las necesidades de la Universidad.

7. Finalidad del tratamiento de datos personales en la UTMACH

La Universidad Técnica de Machala (UTMACH) utiliza, recopila y administra la información personal que haya sido proporcionada por estudiantes, empleados, docentes, proveedores y cualquier otra persona cuyos datos sean tratados por la institución para mejorar el contenido, usabilidad y experiencia de los servicios académicos, administrativos, de investigación y vinculación.

Esto se realiza según la mejora continua de los procesos que permitan brindar servicios educativos de calidad, en el marco de cumplir la normativa legal vigente. La UTMACH realizará el tratamiento de los datos personales de acuerdo con las siguientes finalidades:

7.1 Para estudiantes / alumnis

- “Gestionar la relación académica, incluyendo la inscripción, matrícula, evaluación y emisión de títulos.
- Cumplir con las obligaciones legales, normativas y demás regulaciones educativas.
- Contar con una base de datos correspondiente a las características y perfiles de los titulares de datos personales, todo de acuerdo con lo dispuesto en la Ley.
- Prevenir el fraude y cualquier riesgo de conducta delictiva en el ámbito educativo.
- Realizar análisis de desempeño académico y seguimiento de la trayectoria estudiantil.
- Mejorar la atención y calidad de los servicios educativos: elaboración de perfiles académicos, ofertas laborales, ofertas de cursos y programas, generación y gestión de modelos de análisis.
- Cumplir con la entrega de información a autoridades educativas, como el Ministerio de Educación, el Consejo de Educación Superior (CES) y otras entidades competentes, CACES Y SENECYT.
- Conocer el comportamiento académico, disciplinario y cumplimiento de obligaciones legales de los estudiantes.
- Realizar las gestiones necesarias para confirmar y actualizar la información del estudiante para la prestación de servicios educativos contratados por la universidad.
- Gestionar información de contactos de emergencia de los estudiantes y/o tutores en los casos que aplique.
- Gestionar seguridad, salud y bienestar universitario.
- Proporcionar información sobre actividades académicas, bienestar universitario, de vinculación y de investigación relacionado con las carreras universitarias, de grado y/o programas de posgrados, becas, diplomados, cursos, talleres presenciales o virtuales.
- Expedir certificaciones de carácter académico como estudios y títulos obtenidos.
- Promocionar información sobre actividades relacionadas con descuentos empresariales, becas de educación continua entre otros relacionados con el bienestar de los graduados.
- Promover nuevos productos enfocados a las necesidades de los estudiantes y en pro de la calidad educativa, como ofertas laborales
- Cumplir con las obligaciones institucionales relacionadas al acceso a seguros de vida, otros beneficios y los que determine la ley.”

7.2. Para empleados y docentes

- “Gestionar actividades de recursos humanos para el registro de asistencia de empleados y docentes.
- Gestionar procesos de preselección y demás instancias de reclutamiento.
- Gestionar procesos de selección y otras instancias de la vinculación laboral.
- Contar con una base de datos correspondiente a las características y perfiles de los titulares de datos personales, todo de acuerdo con lo dispuesto en la Ley.
- Contar con la disponibilidad de la información para gestionar inducciones, capacitaciones, entrenamientos y atención de brechas.
- Gestionar evaluaciones del desempeño y clima laboral.
- Elaborar planes de carrera, promoción y rutas de crecimiento.
- Gestionar seguridad, salud y riesgo del trabajo.
- Habilitar mecanismos de seguridad física en las instalaciones de la universidad.
- Cumplir con las obligaciones legales, contractuales con empleados y docentes con respecto al pago de sus obligaciones contractuales, registro de gestión, nómina, económica, tributaria, contable y administrativa.
- Controlar el cumplimiento de códigos de ética, normativa nacional e internacional relacionada con el riesgo de conductas ilícitas.”

7.3. Para proveedores

- “Contar con información actualizada a fin de cumplir con las obligaciones
- legales, contractuales y normativa aplicable.
- Gestionar selección y calificación en procesos de contratación.
- Contar con una base de datos correspondiente a las características y perfiles de los titulares de datos personales, todo de acuerdo con lo dispuesto en la Ley.
- Instrumentar acuerdos: contratos, órdenes de compra, convenios, etc.
- Prevenir el lavado de activos, financiamiento de otros delitos, acciones de fraude, etc.
- Soportar incidencias para la gestión de la continuidad del negocio.
- Soportar incidencias para la gestión de la seguridad de la información.
- Soportar incidencias para la gestión de la protección de datos personales.

- Administrar y verificar antecedentes comerciales, de reputación, así como para la detección y/o prevención de fraude y otras actividades ilegales.
- Habilitar mecanismos de seguridad física en las instalaciones de la universidad.
- Gestionar la relación de confianza entre las partes permitiendo un mayor control en las obligaciones asumidas.

A fin de cumplir con las finalidades descritas, los datos personales tratados pueden:

- Ser agrupados, segmentados, organizados y recopilados en la base de datos de la Universidad Técnica de Machala y darles el uso lícito y correspondiente según lo establecido en la Ley Orgánica de Protección de Datos Personales y normativa vigentes.
- Proporcionarse o comunicarse a personas naturales o jurídicas, con las cuales la universidad tiene acuerdos, para poder ejecutar servicios en términos de lo contratado o solicitado por el titular. Estos servicios pueden incluir la gestión de mensajería, análisis de datos, procesos de debida diligencia, y otros servicios de apoyo a la gestión académica y administrativa.

La UTMACH se compromete a proteger la información personal de todos sus miembros y garantizar su tratamiento conforme a los más altos estándares de seguridad y confidencialidad."

En esta sección, que es la más amplia de toda la Política, se establecen los objetivos que tiene la Universidad para el tratamiento de datos personales de estudiantes, docentes y empleados y, proveedores. Respecto de cada grupo de titulares de derechos, se enlistas varios objetivos encaminados a la mejora de la protección, privacidad y mejora de procesos tanto de protección de datos como de otros procesos de la UTMACH. La sección finaliza con una breve descripción de la manera en la que serán tratados los datos recopilados para el logro de los objetivos planteados.

8. Derechos de los titulares de los datos

"Los titulares de los datos tienen los siguientes derechos:

- Acceso a la información: Conocer qué datos personales están siendo tratados y para qué fines, conforme a los principios de lealtad y transparencia, a través del acceso al Sistema Informático de la UTMACH.
- Rectificación: Solicitar la corrección de datos personales inexactos o incompletos.
- Cancelación: Solicitar la eliminación de datos personales cuando ya no sean necesarios para los fines para los cuales fueron recolectados.
- Oposición: Oponerse al tratamiento de sus datos personales por motivos legítimos.
- Portabilidad: Solicitar la transferencia de sus datos personales a otra entidad en un formato estructurado, de uso común y lectura mecánica."

A continuación, recoge varios derechos de los titulares de los datos, tales como: acceso a la información, rectificación, cancelación, oposición y portabilidad, cuyas definiciones son tomadas textualmente de la LOPDP.

9. Obligaciones de la Universidad

- "Recolección y uso: Recolectar y utilizar datos personales solo para los fines específicos y legítimos para los que se obtuvieron.
- Consentimiento: Obtener el consentimiento explícito de los titulares de los datos antes de recolectar y tratar sus datos personales, salvo en los casos previstos por la ley.
- Seguridad de los datos: Implementar y mantener medidas de seguridad adecuadas para proteger los datos personales.
- Confidencialidad: Asegurar que todas las personas que tengan acceso a los datos personales mantengan su confidencialidad.
- Respuesta a solicitudes: Atender y responder a las solicitudes de los titulares de los datos dentro de los plazos establecidos por la ley.

Los titulares de los datos tienen el derecho a revocar el consentimiento que se ha otorgado con respecto al tratamiento de sus datos personales en cualquier momento o cuando no se cumpla con la política de tratamiento de datos personales, de acuerdo con lo establecido en el Art. 8 de la Ley Orgánica de Protección de Datos Personales, esto siendo posible únicamente en las situaciones en las que no se impida una disposición legal o contractual.

> Para ello, la Universidad Técnica de Machala (UTMACH) cuenta con mecanismos para la revocación a través del siguiente medio: Formulario de Revocatoria de Tratamiento de Datos Personales de la página web institucional de la Universidad Técnica de Machala. La revocación del consentimiento puede darse solo en casos determinados, como fines publicitarios, bolsa de empleo y otros beneficios no obligatorios.
>
> La Universidad Técnica de Machala (UTMACH) en el ejercicio de sus funciones, mantendrá a salvo el tratamiento de datos personales para los fines universitarios, de conformidad con la autorización otorgada por el titular.
>
> Sin embargo, toda solicitud de supresión o revocatoria no procederán cuando el titular tenga un deber legal o contractual de permanecer en la base de datos.
>
> Para el cumplimiento del objeto de manera correcta y poder contar con los beneficios que ofrece la UTMACH, los titulares deberán entregar la información exacta y completa a la UTMACH."

Luego, establece que la UTMACH es responsable de la recolección y uso de datos, obtener el consentimiento, la seguridad de los datos, la confidencialidad, responder solicitudes y acoger la revocatoria de consentimiento conforme con la Ley. En cuanto a esto último, se afirma que la Universidad "cuenta con mecanismos para la revocación a través del siguiente medio: Formulario de Revocatoria de Tratamiento de Datos Personales de la página web institucional de la Universidad Técnica de Machala. La revocación del consentimiento puede darse solo en casos determinados, como fines publicitarios, bolsa de empleo y otros beneficios no obligatorios." La única excepción contemplada en la Política es cuando "el titular tenga un deber legal o contractual de permanecer en la base de datos".

10. Medidas de seguridad

> "La UTMACH implementará las siguientes medidas de seguridad:

- Control de acceso: Restringir el acceso a datos personales solo a aquellas personas autorizadas.
- Cifrado: Utilizar técnicas de cifrado para proteger los datos personales almacenados y transmitidos.
- Auditorías: Realizar auditorías periódicas para evaluar la efectividad de las medidas de seguridad implementadas.
- Capacitación: Proporcionar capacitación continua al personal sobre las mejores prácticas de protección de datos personales."

La Política contempla cuatro medidas de seguridad: control de acceso, cifrado, auditorías y capacitación.

11. Base legal

"La UTMACH fundamenta el tratamiento que da a los datos personales en estricto cumplimiento de la Ley Orgánica de Protección de datos personales con base en el Art. 7.- Tratamiento legítimo de datos personales:"

- "Por Consentimiento del titular para el tratamiento de sus datos personales, para una o varias finalidades específicas;"
- "Que el tratamiento de datos personales se sustente en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, derivados de una competencia atribuida por una norma con rango de ley, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta ley y a los criterios de legalidad, proporcionalidad y necesidad;"
- "Para tratamiento de datos personales que consten en bases de datos de acceso público;"
- "Para satisfacer un interés legítimo del responsable de tratamiento o de tercero, siempre que no prevalezca el interés o derechos fundamentales de los titulares al amparo de lo dispuesto en esta norma."

Este acápite tiene que ver con el contenido del artículo 7 de la LOPDP. Así, recopila algunas condiciones, constantes en el referido artículo, que debe cumplir el tratamiento de datos para ser considerado legítimo y lícito.

12. Transferencia de datos

> "transferencia de datos personales a terceros se realizará solo cuando sea necesario para cumplir con las finalidades para las que se recolectaron y si se garantiza un nivel adecuado de protección de datos personales."
> "La UTMACH podrá transferir datos personales a las instituciones nacionales o internacionales según los convenios establecidos y según lo estipulado en la Ley Orgánica de Protección de Datos Personales, contará con el consentimiento previo del titular del dato personal quien debe haber sido informado de forma suficiente sobre la finalidad del tratamiento de sus datos."
> "La UTMACH exigirá documentadamente el cumplimiento al responsable destinatario de la protección de los datos personales, para garantizar la aplicación de medidas de seguridad necesarias para garantizar la confidencialidad, integridad y disponibilidad de los datos personales."

En cuanto a la transferencia de datos, se determina que aquello ocurrirá solo cuando "sea necesario para cumplir con las finalidades para las que se recolectaron y si se garantiza un nivel adecuado de protección de datos personales." Así mismo, se establece que la transferencia ocurrirá en el marco de convenios que tenga la Universidad, según la Ley y el consentimiento del titular.

13. Conservación de datos a ser tratados

> "Los datos personales serán conservados durante el tiempo determinado por la UTMACH para efectos estadísticos, académicos e históricos, en base al principio de Conservación establecido en la Ley Orgánica de Protección de datos, por lo que el responsable del tratamiento de los datos se compromete a tomar las medidas de seguridad pertinentes."

Sobre el tiempo de conservación de los datos se afirma, en resumen, que serán conservados todo el tiempo que tengan alguna utilidad para la UTMACH.

14. Responsabilidades

- "Delegado de Protección de Datos: El delegado de Protección de Datos (DPD/DPO) según lo indica la Ley Orgánica de Protección de Datos Personales (LOPDP) es el responsable de supervisar el cumplimiento de esta política y de las normativas aplicables.
- Personal de la Universidad: Cumplir con las directrices establecidas en esta política y reportar cualquier incidente de seguridad relacionado con datos personales."

Luego, la Política recalca que el delegado de protección de datos tiene los deberes que le determina la ley y el personal de la Universidad debe reportar los incidentes de seguridad.

15. Modificaciones de la Política

> "La UTMACH se reserva el derecho de modificar esta política en cualquier momento. Las modificaciones serán publicadas en el sitio web de la universidad y notificadas a los titulares de los datos, cuando sea necesario."

La política establece que la Universidad se reserva el derecho de modificar la Política, es decir, puede hacerlo en el momento y las veces que las considere necesarias en cumplimiento de la normativa vigente.

16. Contacto

> "a cualquier consulta, solicitud o ejercicio de derechos relacionados con la protección de datos personales, los titulares pueden contactar al delegado de Protección de Datos de la UTMACH a través del correo electrónico protecciondatos@utmachala.edu.ec.
> En cualquier caso, las consultas se atenderán en los quince días hábiles contados a partir de su recibo, según lo establecido en el Ley Orgánica de Protección de Datos Personales."

Antes de terminar, la Política establece un correo electrónico como contacto para absolución de dudas y acoge lo establecido en la LOPDP para la absolución de consultas.

17. Glosario de términos

A fin de no extender más allá de lo necesario la presente sección, es suficiente con afirmar que la Política finaliza con un glosario de algunos términos extraídos de la LOPDP. Aquellos son: datos personales, datos sensibles, tratamiento de datos, responsable del tratamiento, encargado del tratamiento, consentimiento, transferencia de datos, derechos ARCO, medidas de seguridad, violación de datos, delegado de protección de datos y base legal.

CAPITULO 4

Evaluación y aportes de perfeccionamiento de la Política de la Universidad Técnica de Machala

4.1. Evaluación de la Política

En primer lugar, se debe resaltar el compromiso que demuestra la UTMACH al haber emitido la Política. Como se indicó en líneas anteriores, la Universidad se encuentra en una etapa temprana de desarrollo normativo en lo relativo a la protección de datos por lo quex se advierte que los aspectos de incumplimiento o de posibilidad de mejora serán más notorios.

Así, de manera general, la Política recoge aspectos fundamentales de la protección de datos tales como la determinación de los datos que recolecta, las finalidades del tratamiento de datos según se trate de estudiantes, empleados y docentes o proveedores, los parámetros generales de seguridad, la transferencia de datos y responsabilidades de la Universidad. A continuación, la evaluación se realiza la evaluación de las secciones de la Política que requieren de mayor atención.

1. Introducción. Si bien no es algo que exija la LOPDP, se podría incluir un preámbulo tanto normativo como fáctico que explique la pertinencia de la emisión de la Política. Aquí, la UTMACH tiene la oportunidad de fortalecer su Política, considerando tanto normativa vigente como fundamentarse en su realidad fáctica. Así, para la elaboración de una mejor introducción, se podrían elaborar trabajos previos que determinen la situación actual de la Universidad en cuanto a protección de datos personales.

2. Definiciones, principios generales y glosario. No es común como práctica legislativa que se incluyan definiciones, sin embargo, en Ecuador se acostumbra a incluir dentro del articulado de sus cuerpos normativos amplios artículos que recogen definiciones de palabras técnicas, principios y otros términos que se consideran imprescindibles para expedir una ley. La Política, a nuestro parecer cae en este vicio de legislación por partida doble: porque, por un lado, incluye estos apartados cuya ausencia no afectarían su objeto y, porque, en todo caso, los términos que acoge no serían los suficientes para los objetivos del documento. Así, bien se podría, con miras a que el documento sea leído por los titulares de los datos, prescindir de una transcripción de definiciones de la ley en favor de una sistematización, no de definiciones, sino de lineamientos generales e imprescindibles que rigen la protección de datos en la Universidad.

3. Datos que se recolecta: la Política enlista seis categorías de datos que no serían los adecuados para determinar los datos que recopila la Universidad. En virtud del principio de responsabilidad proactiva, no es recomendable incluir una categoría como “información general”, pues es un criterio demasiado amplio, lo cual genera riesgos en la indeterminación de los datos que se recolecta. Así mismo, esta sección únicamente parece enfocarse en los

datos de estudiantes, dejando de lado a profesores, personal administrativo y proveedores. En consecuencia, la Política debe ser más específica en determinar los datos que recolecta distinguiendo los titulares cuyos datos se recolecta. Es necesario que la Universidad enfatice en la política el aspecto normativo que garantiza la protección de los datos personales de todos los titulares que forman parte de la comunidad universitaria, especificando los datos personales recolectados por estamento y proveedor y el tratamiento que se darán a los mismos.

4. Finalidad del tratamiento. Este apartado se divide en tres: para estudiantes, docentes y empleados y para proveedores. En general, podemos decir que, si bien que este acápite es el más desarrollado de la Política, no deja de ser un poco escueto. Comprendemos que el objetivo de esta sección es brindar una lista más bien amplia de finalidades del tratamiento de datos según los titulares, sin embargo, a criterio de los investigadores, la Política debería incluir más que solamente objetivos. Era deseable que la Universidad cuente con procedimientos claros de recolección, tratamiento y protección de datos. Por lo que esta sección es por demás insuficiente para cumplir con la protección de datos. Si bien no se requiere un documento exhaustivo, sí se merecía un detalle más pormenorizado de procedimientos a fin de que los titulares tengan mejor información sobre el tratamiento de sus datos. Sin perjuicio de lo anterior, se puede afirmar que la Universidad tiene una enorme oportunidad de desarrollas sus finalidades, a través de procesos y lineamientos claros que les permita cumplir con lo propuesto.

5. Derechos de los titulares. De manera semejante, esta sección es insuficiente por ser algo escueta (sólo contiene cuatro derechos) y por ser mayormente descriptiva. Lo óptimo

sería que, sin ser exhaustivos, se incluya más que los derechos de los titulares, al menos, indicios de procedimientos para hacer ejercer sus derechos. Es importante también que la Universidad considere ampliar los derechos de los titulares descritos en la Política puesto que existe datos de carácter sensibles y que no están siendo considerados en la política vigente en la institución.

6. Obligaciones de la Universidad. En este apartado la Universidad tenía una clara oportunidad para desarrollar de manera más exacta las responsabilidades del tratamiento de datos personales. Así, el apartado se presta para desarrollar los fines de recolección de datos, la manera en que se conseguirá el consentimiento, más detalle sobre las políticas y procedimientos de seguridad, especificaciones sobre qué información se considera confidencial y algún protocolo al respecto, desarrollar una lista tentativa de solicitudes que permitan ejercer los derechos a los titulares, etc. Así mismo, la Política debe contemplar mecanismos de información dirigidos a los titulares de los datos que abarquen todos los momentos en que se traten sus datos.

7. Medidas de seguridad. De manera semejante, este acápite es bastante laxo en determinar las medidas de seguridad. Consideramos que se debe diferenciar los mecanismos de recolección de datos, pues no aplica la misma seguridad si es información almacenada en formato físico o digital. Así, se debe hacer la distinción mencionada y especificar las medidas de seguridad para cada una, considerando además que la Universidad puede optar por mecanismos de automatización y digitalización en la recolección y tratamiento de datos.

8. Transferencia de datos. Si bien este es uno de los criterios más desarrollados, se refiere a la facultad que tiene la Universidad para transferir datos a otras instituciones. En

virtud del principio de responsabilidad proactiva y de transparencia, consideramos que se debería explicitar o al menos mencionar, motivos más exactos que justificarían la transferencia, pues solamente decir que esto puede ocurrir en función de convenios o de disposiciones de la ley, no parece ser lo suficientemente claro. Así mismo, se debería detallar el procedimiento para recabar el consentimiento informado del titular en este supuesto.

9. Conservación de los datos. Según la Política, no se determina un tiempo exacto de conservación, sino que queda a discreción de la misma Universidad. Es decir, no establece un tiempo de acuerdo con los datos que se trata. La Universidad debería definir plazos específicos de conservación según cada categoría de datos, en función de sus finalidades.

La política menciona fines como "mejorar la experiencia de servicios académicos" y "promover nuevos productos", que son propósitos amplios y poco específicos.

10. Delegado de Protección de Datos. Se lo describe, pero sin proveer detalles operativos como la manera de contactarlo ni su campo de actuación. Al respecto, se debería describir funciones específicas del delegado, datos de contacto y el procedimiento para gestionar incidentes.

Sin perjuicio de todo lo anterior, y para una mejor presentación, conviene esquematizar la evaluación realizada, a través del siguiente cuadro:

Sección de la Política	Evaluación	Relación con la LOPDP	Resultado
1. Introducción	La UTMACH muestra un firme compromiso con el tratamiento y protección de los datos personales, alineándose con la Ley	No existe una norma que obligue a la UTMACH a presentar una introducción.	Corresponde a una sección que puede mejorar. Para ello, convendría incluir una exposición de motivos

	Orgánica de Protección de Datos Personales del Ecuador.		que incluya un marco normativo nacional y de la Universidad, así como criterios fácticos que evidencien la pertinencia de la emisión de la Política.
2. Responsable del tratamiento de los datos	La UTMACH se limita a identificarse como responsable y designa su RUC, dirección y un correo electrónico. No contiene una definición. No expone sus obligaciones.	El artículo 4 define esta figura.	Corresponde a una falencia de la Política, más que no incluir una definición, las obligaciones que tiene la UTMACH como responsable del tratamiento de datos. Esta información se recoge recién en el acápite 9 de la Política. Por lo que demuestra una deficiente técnica legislativa que puede mejorar.
3. Alcance	Expone un ámbito de aplicación circunscrito a las actividades que realiza la Universidad	Los artículos 2 y 3 determinan los ámbitos de aplicación material y territorial de la Ley.	Esta sección corresponde a una que puede fortalecerse. Así, se pueden ampliar, como lo hace la LOPDP, los supuestos de aplicación de la Política.
4. Definiciones	Replica las definiciones contenidas en la LOPDP sobre dato personal, datos sensibles, titular y tratamiento	El artículo 4 contiene una amplia lista de términos y definiciones	La LOPDP no obliga a contener una lista más o menos exhaustiva de términos y definiciones, por lo que esta sección corresponde a una de las que se puede mejorar. Así se debe incluir términos que se utilizan

			en la Política y que sirvan para una mejor comprensión del texto, especialmente de aquellos términos que sean técnicos en la materia.
5. Principios generales	Reproduce las definiciones que tiene la LOPDP de los principios de legalidad, transparencia, finalidad, minimización de datos, exactitud y seguridad.	El artículo 10 contiene una lista exhaustiva de principios	Al igual que la anterior, esta sección es de las que se puede mejorar. Así, conviene no dejar de lado principios importantísimos en la protección de datos como el de responsabilidad proactiva, confidencialidad y conservación.
6. Datos que se colecta	Identifica seis categorías: información general, datos de nacimiento, domicilio, estudios secundarios, datos familiares, datos para ficha socioeconómica. Se deja abierta la determinación de categorías según las necesidades de la UTMACH	El artículo 4 contiene la definición de dato personal y el capítulo IV regula las categorías especiales de datos	Esta sección no cumple con lo determinado por la LOPDP. Se confunde categoría de datos con dato personal. No se considera que la Universidad trata datos no solo de estudiantes, sino de empleados, profesores, proveedores y otros. La lista que contiene la Política está enfocada principalmente para estudiantes, pero deja de lado los demás titulares. Tampoco contiene una clara determinación de categorías de datos sensibles que trate la Universidad. Esto es

			relevante porque se cuenta con procedimientos en caminados a proteger datos especiales que trate la UTMACH.
7. Finalidad del Tratamiento	La finalidad general se enfoca a mejorar el servicio brindado por la UTMACH. En este sentido, expone una lista de finalidades para estudiantes, empelados y docentes, y proveedores.	El artículo 1, establece la finalidad de la ley.	Esta sección no corresponde con lo determinado por la LOPDP. Los fines del tratamiento en la Política están enfocados a mejorar procesos internos con la intensión de que el trabajo en la Universidad sea más amigable con sus usuarios e incluso la prevención de delitos no necesariamente relacionados con la protección de datos. Sin embargo, no se encuentran finalidades encaminadas a la protección de datos de estudiantes, empleados, profesores, proveedores y otros. Esta sección podría ser mucho más corta, como lo es su contraparte de la LOPDP, y explicitar que el fin de la Política es "garantizar el ejercicio del derecho a la protección de datos personales" con los matices que requiera su

			aplicación en al UTMACH.
8. Derechos de los titulares	Se recogen los derechos al acceso de la información, rectificación, cancelación, oposición y portabilidad.	El capítulo III contiene los derechos de los titulares	La política no cumple con establecer todos los derechos de los titulares, conforme lo establece la LOPDP. Así, no se incluye, por ejemplo, el derecho a la eliminación, a la suspensión del tratamiento, entre otros, como tampoco se consideran excepciones del ejercicio de tales derechos. Por otro lado, la Política se limita a brindar una definición de cada derecho, pero no establece reglas de ejercicio de cada uno. Es decir, debe contener más que una definición de cada derecho, parámetros más concretos que viabilicen su aplicación en la UTMACH.
9. Obligaciones de la Universidad	Se establecen cinco obligaciones: Recolectar y usar la información para los fines específicos y legítimos de la UTMACJ, obtener el consentimiento explícito de los titulares, implementar y mantener medidas de seguridad, guardar confidencialidad	El artículo 47 contiene las obligaciones del responsable del tratamiento de datos personales.	La Política es insuficiente al establecer, a penas, cinco obligaciones del responsable del tratamiento. Esta sección debería abordar de manera amplia y detallada las obligaciones de la UTMACH, como

	de los datos, atender y responder a solicitudes de los titulares. Además, se reconoce que los titulares pueden solicitar la supresión o revocatoria del consentimiento y se regula de manera general este procedimiento		responsable del tratamiento. Por otro lado, no es conveniente que en esta misma sección se aborde el ejercicio del derecho a supresión o revocatoria del consentimiento porque no guarda armonía con la cuestión de obligaciones de la UTMACH, así como este asunto debería ser abordado en un acápite especial y con mayor detalle que permita identificar de manera clara los supuestos en los que corresponde o no ejercer este derecho y un procedimiento explícito para tal efecto.
10. Medidas de seguridad	La UTMACH contempla: control de acceso a datos a personas autorizadas, utilizar técnicas de cifrado, realización de auditorías periódicas y capacitar continuamente a su personal.	Artículo 4 literal j. Se reconoce el principio de seguridad de datos personales y el capítulo VI.	Así, este acápite deviene en insuficiente, pues, la determinación de medidas de seguridad supone la determinación clara de los tipos de datos que se trata y de los mecanismos de recopilación y almacenamiento de estos. Así, no existe certeza de que las medidas contempladas sean las adecuadas para la protección de datos en el contexto de UTMACH.

			En específico, las medidas están orientadas a la protección de bases de datos digitales, pero no se ha mencionado antes las formas de almacenamiento de la información con la que cuenta la Universidad, así, podrían quedar desprotegidos datos que no estén respaldados de manera digital. Por otro lado, únicamente se consideran medidas tecnológicas que protegen las formas de almacenamiento, pero no se consideran medidas de protección en cuanto al acceso de la información, como la anonimización, protocolos en el flujo del tratamiento de datos, entre otros.
11. Base legal	Se refiere al tratamiento legítimo de los datos y se transcribe el artículo 7 de la LOPDP	El artículo 7 determina las condiciones para que el tratamiento de datos sea legítimo.	Consideramos que al ser una transcripción del artículo 7 de la LOPDP, se podría concluir que no existe una deficiencia al respecto. Salvo que el título conferido a esta sección no es el adecuado y puede ser objeto de confusión.
12. Transferencia de datos	La transferencia de datos a terceros se realizará en	Capítulo V	Consideramos que esta es una sección que debe ser

	cumplimiento de las finalidades de su recolección y en observancia de las medidas de seguridad. Se remite a la LOPDP para la transferencia nacional o internacional y establece que, para ello, se requiere el consentimiento informado del titular. Establece la responsabilidad del tercero de informar sobre el cumplimiento de medidas de seguridad en el tratamiento de datos		perfeccionada por la UTMACH, puesto que es una actividad que debe realizar con cierta frecuencia. Así, considerando que el criterio fundamental en este caso es el consentimiento informado de los titulares, se debe explicitar las condiciones del ejercicio de este derecho en este supuesto específico, así también, la LOPDP sugiere que se incluyan excepciones a la necesidad de contar con el consentimiento y la determinación de responsabilidades y rango de actuación de los terceros a quienes se transfiere los datos.
13. Conservación de datos	Se afirma que se conservarán los datos recopilados durante el tiempo que la UTMACH lo considere necesario para el cumplimiento de su fin.	Art. 4 literal i Art. 12 numeral 4 Art. 15 numeral 4	La política no cumple con el principio de conservación de datos, pues no es adecuado no limitar en su Política el tiempo de conservación de los datos. Si bien se identifican fines de tipo estadístico, académico e histórico, se debería establecer un tiempo de conservación de acuerdo con cada fin identificado. Así, se cumple también

			con el principio de transparencia y de responsabilidad proactiva. La determinación del tiempo de conservación, además, permite el ejercicio de otros derechos como el de información o de eliminación de datos.
14. Responsabilidades	Se menciona al delegado de protección de datos y al personal de la Universidad como responsables del cumplimiento de la normativa vigente, en el ámbito de sus competencias.	Art. 48 sobre el delegado de protección de datos.	La Política se limita a afirmar que contará con un delegado de acuerdo con la LOPDP, pero no se establecen sus funciones y obligaciones. Es decir, no cumple con regular esta figura de manera suficiente. Además, se habla de delegado, pero no de encargado. Así, la Política no incluye una figura importante para la protección de datos, lo cual debe ser observado en su futura normativa. Además, si bien todo el personal de la Universidad tiene un deber de proteger datos, no es adecuado ponerlo a la par del delegado de protección de datos.
15. Modificaciones a la Política	La UTMACH puede modificar la Política en cualquier momento. Las	Artículo 47 literal 4	Este acápite está de acuerdo con la facultad contemplada por la

	modificaciones serán publicadas por canales oficiales.		LOPDP para que los responsables de protección de datos implementen políticas en la materia.
16. Contacto	Se designa un correo electrónico de contacto y presentación de consultas	No se establece el deber de señalar un canal de contacto	Es adecuado que la UTMACH defina un canal de contacto para dudas y consultas.

Tabla 3: *Esquema de la evaluación realizada*

Elaborada por Astrid Salazar, Diego Huiracocha, Darwin Quinche, Josué Alvear y María Peña

En consecuencia, de todo lo abordado en las páginas previas, se puede observar que la Política de la UTMACH no cumple con todos los criterios que determina la LOPDP para protección de datos personales. Esto, como ya se afirmó, se debe a que la Universidad está en una etapa temprana de implementación de políticas en la materia. Así, la Política no cumple con la gran mayoría de criterios normativos que serían adecuados o suficientes para sentar una base sobre la cual se articule su sistema de protección de datos.

4.2. Aportes de perfeccionamiento de la Política de la Universidad Técnica de Machala

Ahora bien, todo lo anterior son las cuestiones en las que la Política de la Universidad Técnica de Machala tendría una normativa insuficiente. Sin embargo, consideramos que existen cuestiones que no fueron consideradas por la Política y que deberían serlo. A continuación, se detallan algunas de las más importantes.

1. Capacitación y Concienciación: Implementar programas de capacitación continúa dirigidos a estudiantes, docentes y personal administrativo sobre la importancia de la

protección de datos personales. Estos programas deben incluir temas como el manejo adecuado de la información sensible, las políticas de privacidad vigentes, el uso seguro de herramientas digitales y la identificación de posibles riesgos relacionados con la ciberseguridad. La capacitación constante tiene un impacto directo en la conciencia colectiva acerca de la relevancia de la protección de datos. Un personal y alumnado bien informado estará mejor preparado para cumplir con las políticas de tratamiento de datos personales, reduciendo el riesgo de incidentes de seguridad y asegurando el cumplimiento de normativas locales e internacionales, como la Ley de Protección de Datos Personales. Para esto se considera oportuno que los estudiantes reciban una capación una semana antes del inicio de clases la misma que puede regirse bajo el siguiente cronograma:

CRONOGRAMA DE CAPACITACIÓN DE PROTECCIÓN DE DATOS PERSONALES A LOS ESTUDIANTES DE LA UNIVERSIDAD TECNICA DE MACHALA.

Día	Actividad	Duración	Modalidad
1	Taller introductorio sobre la protección de datos personales, conceptos básicos e importancia de la privacidad.	1 hora	Presencial o virtual (dependiendo de la modalidad de estudio del estudiante, así como de lo que la universidad considere como mejor opción de modalidad)
2	Taller sobre amenazas virtuales, con la intención de identificar correos o enlaces sospechosos, así	2 horas	Presencial o Virtual

	como consejos para prevenir ser víctimas de un ciber ataque.		
3	Taller sobre el uso de contrase**ñas, sistemas de autentificación y seguridad de la nube.**	1 hora	Presencial o virtual
4	Simulacro de ciber ataque, con la finalidad de analizar y reforzar los conocimientos adquiridos por los estudiantes.	2 horas	Presencial o virtual

Tabla 4: *Sugerencia de cronograma de capacitación*

Elaborada por Astrid Salazar, Diego Huiracocha, Darwin Quinche, Josué Alvear y María Peña

Con respecto al personal docente y administrativo al contar manejar ellos una mayor cantidad de datos, se considera oportuno contar con un cronograma más extenso, por lo que se sugiere el siguiente cronograma:

CRONOGRAMA DE CAPACITACIÓN DE PROTECCIÓN DE DATOS PERSONALES A LOS DOCENTES Y PERSONAL ADMINISTRATIVO DE LA DE LA UNIVERSIDAD TÉCNICA DE MACHALA.

Día	Actividad	Duración	Modalidad
1	Taller introductorio sobre la protección de datos personales, conceptos básicos e importancia de la privacidad.	1 hora	Presencial
2	Taller sobre amenazas virtuales, con la intención de identificar correos o enlaces sospechosos, así como consejos para prevenir ser víctimas de un ciber ataque.	2 horas	Presencial o Virtual
3	Taller sobre el manejo seguro de datos en las Bases administrativas, conocimiento sobre los protocoles de respaldo de datos, así como de acceso a estos, procedimiento en	2 horas	Presencial

	caso de existir brechas de seguridad.		
4	Taller sobre riesgos existentes por la utilización de redes públicas y las reglas sobre el uso de los dispositivos tanto personales como los pertenecientes a la universidad	1 hora	Presencial
5	Taller sobre el uso de contrase**ñas, sistemas de autentificación y manejo correcto de la nube, así como la seguridad de la nube.**	1 hora	Presencial
6	Taller de análisis ético del manejo de datos personales de la universidad, así como recomendaciones para resguardar la información.	2 horas	Presencial o virtual
7	Simulacro de ciber ataque, con la finalidad de analizar y reforzar los conocimientos adquiridos	2 horas	Presencial

***Tabla 5**: Sugerencia de Cronograma de Capacitación para docentes y personal administrativo*

Elaborada por Astrid Salazar, Diego Huiracocha, Darwin Quinche, Josué Alvear y María Peña

Para reducir costos se considera oportuno que estas capacitaciones sean realizadas por los docentes de la carrera de Tecnologías de la información en conjunto con los docentes de la carrera de derecho que se encuentren especializados en el área de derecho penal y derecho digital.

2. Actualización de Infraestructura Tecnológica: Este parámetro es sumamente importante al considerar que entre los riesgos que podrían estar vinculados con una /infraestructura insuficiente o inadecuada podemos citar los siguientes:

Ausencia de seguridad: Los sistemas anticuados o configurados de forma equivocada son propensos a ataques informáticos, como el hacking, el ransomware o el phishing. Esto puede causar la desaparición, hurto o divulgación de información personal delicada.

Accesos no autorizados: Sin protocolos apropiados de control de acceso, individuos sin permiso pueden ingresar a bases de datos o sistemas que albergan datos sensibles, lo que favorece el uso indebido de la información.

Pérdida de datos: Este representa un peligro posible ya que, al tener una infraestructura insuficiente, existe el riesgo de que esta no disponga de sistemas apropiados de respaldo o recuperación de datos frente a incidentes como errores técnicos, catástrofes naturales o fallos humanos. Por lo tanto, también podría tener una capacidad restringida para el almacenamiento de datos.

Ausencia de cifrado: Una infraestructura deficiente puede mostrar la falta de herramientas de cifrado, lo que amenaza la información durante su transmisión.

Considerando los aspectos previamente mencionados se sugiere las siguientes soluciones:

Como punto de partida se debe realizar una autoría tecnológica, esto con la intención de poder identificar de mejor manera las vulnerabilidades en los sistemas de almacenamiento, así como en el hardware y software, para posteriormente invertir en la actualización y mejora continua de la infraestructura tecnológica de la universidad es crucial esto con el objetivo de reforzar la protección de los datos personales almacenados y gestionados en sus sistemas. Esto incluye la renovación de servidores, la implementación de soluciones avanzadas de encriptación de datos, el uso de sistemas de autenticación y el fortalecimiento de las políticas de acceso a la información sensible. La tecnología es un pilar fundamental en la protección de datos personales, por lo que contar con una infraestructura robusta y actualizada mejora significativamente la capacidad de la universidad para defenderse de las amenazas cibernéticas. Además, la actualización constante de los sistemas es crucial para cumplir con

los estándares de seguridad internacionales y garantizar la confidencialidad, integridad y disponibilidad de los datos. Se sugiere a la universidad contar con redes de internet seguras, estableciendo redes privadas virtuales, conocidas como VPN para poder proteger los sistemas y los datos de las conexiones externas.

3. Evaluaciones Periódicas de Seguridad: Realizar evaluaciones periódicas y exhaustivas de seguridad de la información, con el fin de identificar y mitigar posibles vulnerabilidades o riesgos asociados al tratamiento de datos personales. Estas evaluaciones deben incluir pruebas de penetración, análisis de vulnerabilidades, auditorías de acceso y revisión de los sistemas de protección implementados. Además, se sugiere la contratación de expertos externos para llevar a cabo auditorías independientes que proporcionen una visión objetiva de la situación actual de la seguridad en la universidad. Las evaluaciones periódicas son esenciales para mantener la seguridad de los datos frente a amenazas cada vez más sofisticadas. Estas auditorías permiten detectar debilidades en los sistemas antes de que sean explotados, asegurando la protección de la información a lo largo del tiempo.

4. Mejora de los Procedimientos de Gestión de Datos Sensibles: Revisar y mejorar los procedimientos existentes para el manejo, almacenamiento y tratamiento de datos sensibles, implementando medidas adicionales de seguridad para garantizar su protección. Esto incluye la actualización de políticas internas que regulan el acceso a este tipo de datos, así como la implementación de medidas de seguridad más estrictas, como la encriptación de la información, controles de acceso más rigurosos y la adopción de protocolos de manejo seguro. Mejorar los procedimientos de gestión de estos datos reduce significativamente el

riesgo de brechas de seguridad, como accesos no autorizados o divulgación involuntaria de información confidencial.

5. Implementación de Tecnologías Avanzadas: Considerar la implementación de tecnologías avanzadas, como el aprendizaje automático (machine learning) y la inteligencia artificial (IA), para mejorar la seguridad de los datos personales gestionados por la universidad. Estas tecnologías pueden ser implementadas para monitorear continuamente las bases de datos y sistemas, identificando patrones inusuales o potenciales amenazas de seguridad de manera más eficaz que los métodos tradicionales.

6. Revisión y Actualización de Políticas: Realizar una revisión y actualización periódica de las políticas relacionadas con el tratamiento de datos personales en la universidad, con el fin de garantizar que sigan siendo relevantes, efectivas y alineadas con los avances tecnológicos y las normativas legales vigentes. También se debe evaluar la efectividad de las políticas implementadas mediante la retroalimentación de los usuarios y la auditoría interna de los procesos. Las políticas de protección de datos deben evolucionar constantemente para mantenerse alineadas con las mejores prácticas, las normativas actuales y los avances tecnológicos en ciberseguridad. La revisión periódica de las políticas asegura que la universidad esté en cumplimiento con la legislación de protección de datos, como la Ley de Protección de Datos Personales, y que se adapte a las nuevas amenazas que puedan surgir.

Capítulo 5

Conclusiones

El presente trabajo pudo corroborar que la Universidad Técnica de Machala, en cuanto a protección de datos personales ha tenido un avance que, si bien puede ser calificado como inicial, no deja de ser importante para los objetivos que se plantearon en esta investigación. Aquí se procuró, a partir de un marco teórico y normativo suficiente en cuanto a protección de datos personales, analizar y evaluar las políticas o mecanismos de protección de datos personales que haya implementado la Universidad Técnica de Machala.

En consecuencia y como primera conclusión, se puede determinar que los referidos análisis y evaluación fueron posibles en la medida en la que la Universidad cuenta con un primer documento emitido en el mes de octubre del año 2024, denominado Política de Tratamiento de Datos Personales de la Universidad Técnica de Machala. Es decir, la Universidad cuenta con un documento primigenio que hizo factible la presente investigación.

Así pues, la referida Política contiene lineamientos generales que procuran guiar una futura elaboración de normativa sobre protección de datos personales en la Universidad. La Política, entonces, contiene una definición de su alcance y objetivos generales, que se pueden resumir en lo siguiente: la Política es un documento inicial sobre protección de datos, sobre lo cual la Universidad seguirá estableciendo normativa sobre protección de datos.

Posteriormente, recoge la figura del responsable del tratamiento de datos, mayormente describiendo de manera general su labor y responsabilidad. De manera semejante, la Política incluye una mención de algunas definiciones de términos propios de la materia extraídos de la Ley. A continuación, tiene una lista preliminar de categorías de datos que va a tratar y pasa a

establecer la finalidad de su tratamiento, que se sintetiza en criterios de optimización de los procedimientos de protección de datos y procesos propios de la Universidad.

Posteriormente, la Política establece, en una de sus partes más desarrolladas, los fines del tratamiento de datos según se trate de estudiantes, de empleados y profesores y de proveedores. Seguido de lo cual se recogen varios derechos de los titulares de los datos y luego, se determina que la Universidad cuenta con mecanismos para la revocación del consentimiento. Así también, la Política contiene una mención general de las medidas de seguridad orientadas al ámbito digital.

A continuación, se determinan lineamientos generales sobre la transferencia de datos con terceros, en donde se dice que los titulares estarán informados y podrán consentir al respecto y de acuerdo con parámetros que serán establecidos por la Universidad y sus contratos con terceros.

En cuanto al tiempo de conservación de los datos se afirma de manera general que serán conservados mientas sean útiles para la Universidad. Y termina reafirmando que las responsabilidades del delegado de protección de datos son conforme a la ley y normativa vigente, a la vez que recoge un glosario de términos.

En virtud de lo anterior, se evaluó la Política de la Universidad y se verificó que, aunque la política incluye elementos fundamentales como la recolección de datos, finalidades del tratamiento y medidas de seguridad, presenta algunas deficiencias y aspectos que deben ser perfeccionados. En primer lugar, se debe anotar que las falencias encontradas en la Política se deben justamente a que no se trata de un documento exhaustivo o definitivo sino a un primer documento en la materia de protección de datos. Por lo cual se pudo advertir que la Universidad

tiene una importante tarea posterior en cuanto a desarrollar la normativa en torno a la protección de datos personales, lo que se traduce en una enorme oportunidad de seguirlo haciendo conforme a la normativa legal vigente. Así, se verificó que la Política presenta, como puntos positivos, el compromiso de la Universidad con la protección de datos personales y una buena aprehensión de la normativa que debe observar en el futuro.

Sin embargo, y como aspectos a mejorar no solo en la Política sino en posteriores desarrollos normativos de la Universidad, se deben tomar muy en cuenta los siguientes aspectos:

- Una redacción organizada en cuanto temas. Si bien la Política se divide en diferentes acápites, no es prolijo que se encuentre un glosario de términos al final, o los derechos de los titulares de los datos por la mitad del documento. Una estructura que comience por cuestiones teóricas, conceptuales o terminológicas, seguida de cuestiones de fondo organizadas con secuencia lógica por temas, es por demás relevante.
- Si bien no es imprescindible contar con definiciones, principios, derechos y otras cuestiones teóricas y conceptuales, en caso de incluirlo dentro de la normativa se debe procurar su precisión, claridad y relevancia para ser incluidas. Así, se debe fortalecer la redacción de los aspectos mencionados a fin de que realmente sean un aporte a la normativa emitida por la Universidad que permita una mejor comprensión de sus contenidos y no una mera enunciación de términos que luego no se mencionan en el documento.
- No existe especificidad en cuanto a los datos recolectados, pues la Política se refiere de manera general a los datos que recolecta y luego trata. Únicamente contiene un apartado

en donde fija los objetivos del tratamiento de datos según se trate de estudiantes, profesores y empleados y, proveedores, sin embargo, esto no es suficiente porque no explicita los datos que se recolecta respecto de cada uno, la manera de almacenamiento, el uso que se dará a los datos, etc.

- De manera semejante, la Política es escaza en procedimientos relativos a la recolección, tratamiento y protección de datos, así como directrices sobre el ejercicio de los derechos de los titulares. Una vez más, consideramos que esto se debe a la naturaleza del documento analizado, con lo cual la Universidad tiene una tarea ardua en normar estos aspectos que son los más relevantes para la protección de datos.
- En cuanto al establecimiento de medidas de seguridad, la Política no prescribe un sistema de seguridad que se adecue a la trascendencia de los datos que trata, sino que mayormente contiene enunciados de fin, es decir, normas que guiarán el establecimiento posterior de procedimientos más detallados para establecer medidas y protocolos de seguridad, lo cual inequívocamente debe incluir un análisis de peligros y amenazas de vulneración de sus bases de datos y de sus procedimientos.
- Otro punto importante que llamó nuestra atención fue que se puso énfasis en la transferencia de datos personales, sin embargo, notamos que este procedimiento carece de justificaciones y protocolos explícitos, sobre todo, que permitan a los titulares la decisión sobre la transferencia de sus datos.
- Uno de los aspectos cruciales en la protección de datos es el tiempo de conservación, por lo cual nos generó preocupación que no se establezca tiempos claros y justificados para la conservación de datos.

- Finalmente, consideramos que el rol del delegado de protección de datos no contiene una descripción suficiente en cuanto a sus responsabilidades y atribuciones.

En consecuencia, consideramos que la Universidad tiene, como ya se anotó antes, una enorme oportunidad y responsabilidad de normar, básicamente, todos los aspectos de protección de datos de conformidad con la normativa inherente a la materia en mención.

BIBLIOGRAFÍA

Arellano López, C. A. (2020). El derecho de protección de datos personales. *Biolex*, *12*(23), 163-174.

Universidad Técnica de Machala. (2024), Política de tratamiento de datos personales de la Universidad de Machala. https://n9.cl/htvs7

Polo Roca, A. (2020). El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado. *Revista de Derecho Político*, *1*(108), 165–194. https://doi.org/10.5944/rdp.108.2020.27998

Ley Orgánica de Protección de Datos de Ecuador, Registro Oficial Suplemento 747 (2021). Ley Orgánica de Protección de Datos de Ecuador. https://www.funcionjudicial.gob.ec/web/jurisprudencia/-/ley-organica-de-proteccion-de-datos-de-ecuador.

Constitución de la República del Ecuador (2008). Constitución de la República del Ecuador. https://www.asambleanacional.gob.ec/sites/default/files/documents/2023-04/constitucion_republica_ecuador_2008.pdf.

Lima, D. D. (2023). Transparencia y protección de datos personales en el ámbito universitario:¿ avance o retroceso?. Revista española de la transparencia, (17), 8.

Universidad de las Américas (2020) Cálamo, Revista de Estudios Jurídicos.

Conde, P. y Cazurro, V. (2017). El cumplimiento de la normativa de protección de datos personales y su impacto en la Universidad. En J. C. Gómez, M.C. Pérez y L. Nieto (2017). Investigaciones de Economía de la Educación(pp. 103-112). Asociación Economía de la Educación.

Hernández, R. (2014). La investigación cualitativa desde la perspectiva de los participantes en un ambiente natural y en relación con su contexto. Alhambra