

**UNIVERSIDAD ESTATAL
PENÍNSULA DE SANTA ELENA**

**FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD
CARRERA DE DERECHO**

**TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL
TÍTULO DE ABOGADO**

**TÍTULO:
PRINCIPIO DE FINALIDAD EN LA PROTECCIÓN DE DATOS PERSONALES:
CASO ESTUDIANTES DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE
SANTA ELENA, 2024**

AUTORES:

**NATHALY VALENTINA TORRES HERRERA
CARLOS LUIS VERA YAGUAL**

**TUTORA:
AB. BRENDA REYES TOMALÁ, Mgt.**

**LA LIBERTAD – ECUADOR
2025**

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

**FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD CARRERA DE
DERECHO**

**TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL
TÍTULO DE ABOGADO**

TÍTULO:

**PRINCIPIO DE FINALIDAD EN LA PROTECCIÓN DE DATOS PERSONALES:
CASO ESTUDIANTES DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA
ELENA, 2024**

AUTORES:

NATHALY VALENTINA TORRES HERRERA

CARLOS LUIS VERA YAGUAL

TUTORA:

AB. BRENDA REYES TOMALÁ, Mgt.

LA LIBERTAD – ECUADOR

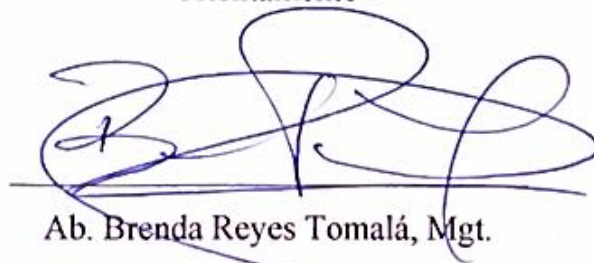
2025

APROBACIÓN DE LA TUTORA

CERTIFICO

Que analizado el trabajo de investigación curricular de título **“PRINCIPIO DE FINALIDAD EN LA PROTECCIÓN DE DATOS PERSONALES: CASO ESTUDIANTES DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA, 2024”** presentado por los estudiantes **NATHALY VALENTINA TORRES HERRERA** y **CARLOS LUIS VERA YAGUAL**, portadores de las cédulas de ciudadanía No. 0706402054 y No. 2450315516 respectivamente, como requisito previo a optar por el título de ABOGADOS, declaro que luego de haber orientado científica y metodológicamente su desarrollo, el referido proyecto de investigación se encuentra concluido en todas sus partes cumpliendo así con el proceso de acompañamiento determinado en la norma interna, recomendando que se inicien los procesos de evaluación que corresponden.

Atentamente

A handwritten signature in blue ink, consisting of several loops and flourishes, positioned above a horizontal line.

Ab. Brenda Reyes Tomalá, Mgt.

TUTORA

CERTIFICACIÓN ANTIPLAGIO

En mi calidad de Tutora del Trabajo de Integración Curricular: **“PRINCIPIO DE FINALIDAD EN LA PROTECCIÓN DE DATOS PERSONALES: CASO ESTUDIANTES DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA, 2024”**, cuya autoría corresponde a los estudiantes **NATHALY VALENTINA TORRES HERRERA** y **CARLOS LUIS VERA YAGUAL**, de la carrera de Derecho, CERTIFICO, que el contenido de dicho trabajo ha sido sometido a la validación en el software antiplagio COMPILATIO, obteniendo un porcentaje de similitud del 3%, cumpliendo así con los parámetros técnicos requeridos para este tipo de trabajos académicos.

 **CERTIFICADO DE ANÁLISIS**
magister

**NATHALY TORRES - CARLOS VERA
2024-2 FINAL**

3%
Textos sospechosos

3% Similitudes
< 1% similitudes entre comillas
0% entre las fuentes mencionadas

< 1% Idiomas no reconocidos

17% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: NATHALY TORRES - CARLOS VERA 2024-2 FINAL.docx	Depositante: BRENDA AMPARITO REYES TOMALÁ	Número de palabras: 22.957
ID del documento: 48364d19ef8e0032200e434f2cab858c1780fe4d	Fecha de depósito: 2/6/2025	Número de caracteres: 150.222
Tamaño del documento original: 1,34 MB	Tipo de carga: interface	fecha de fin de análisis: 2/6/2025

Ubicación de las similitudes en el documento:



Atentamente



Ab. Brenda Reyes Tomalá, Mgt.

TUTORA

CERTIFICACIÓN GRAMATICAL Y ORTOGRAFÍA

CERTIFICO:

Que, he revisado la redacción y ortografía del trabajo de Integración Curricular de título: **"PRINCIPIO DE FINALIDAD EN LA PROTECCIÓN DE DATOS PERSONALES: CASO ESTUDIANTES DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA, 2024"** elaborado por los estudiantes de la Carrera de Derecho de la Universidad Estatal Península de Santa Elena: **NATHALY VALENTINA TORRES HERRERA** y **CARLOS LUIS VERA YAGUAL**, previo a la obtención del título de Abogado.

Que, he realizado las observaciones pertinentes, mismas que han sido acogidas proactivamente por los mencionados jóvenes, corroborando así, que han sido introducidos los ajustes correspondientes en el trabajo en mención.

Por lo expuesto, autorizo al peticionario, hacer uso de este certificado como a bien convenga.

Atentamente,



YOLANDA ELVIRA BARZOLA SEGOVIA

**LICENCIADA EN CIENCIAS DE LA EDUCACIÓN ESPECIALIZACIÓN
LITERATURA Y CASTELLANO**

MAGÍSTER EN DISEÑO Y EVALUACIÓN DE MODELOS EDUCATIVOS

C.I: 0904075140

Registro SENESCYT: 1050-12-86029391

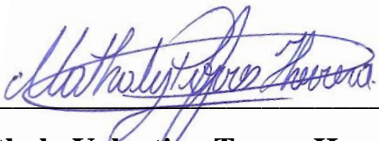
Teléfono: 0969973579

La Libertad, a los 03 días del mes de junio de 2025

DECLARACIÓN DE AUTORÍA

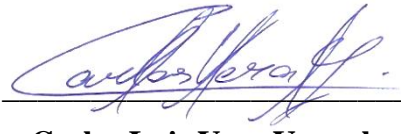
Nosotros Torres Herrera Nathaly Valentina y Vera Yagual Carlos Luis, estudiantes del séptimo semestre de la carrera de Derecho de la Universidad Estatal Península de Santa Elena, habiendo cursado la asignatura Unidad de Integración Curricular I, declaramos la autoría de la presente propuesta de investigación, de título: Principio De Finalidad en la Protección de Datos Personales: Caso Estudiante de la Universidad Estatal Península de Santa Elena, 2024, desarrollada en todas sus partes por las suscritas estudiantes con apego a los requerimientos de la ciencia del derecho, la metodología de la investigación y las normas que regulan los procesos de titulación de la UPSE.

Atentamente



Nathaly Valentina Torres Herrera

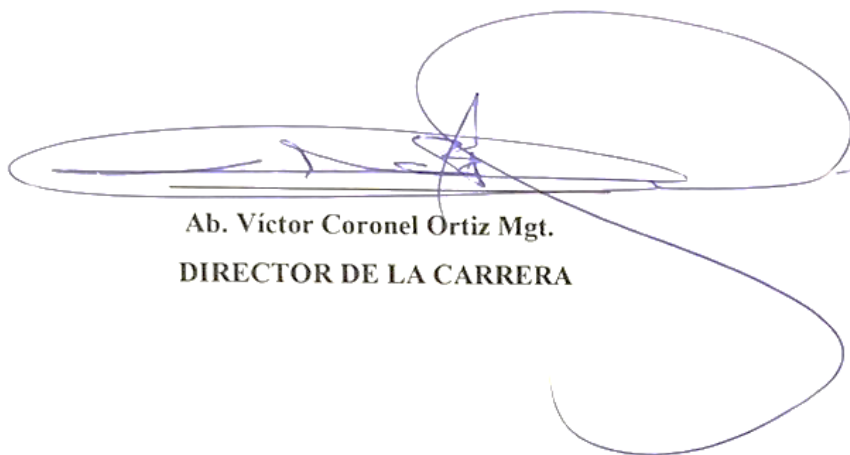
CC. 0706402054



Carlos Luis Vera Yagual

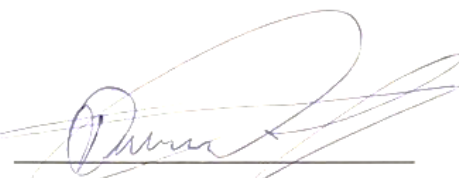
CC. 2450315516

APROBACIÓN DEL TRIBUNAL DE GRADO




A large, stylized handwritten signature in blue ink, consisting of several loops and a long horizontal stroke.

**Ab. Victor Coronel Ortiz Mgt.
DIRECTOR DE LA CARRERA**



A handwritten signature in blue ink, featuring a prominent loop and a long horizontal stroke.

**Ab. Daniel Procel Contreras Mgt.
DOCENTE ESPECIALISTA**



A handwritten signature in blue ink, with multiple overlapping loops and a long horizontal stroke.

**AB. Brenda Reyes Tomalá Mgt.
DOCENTE UIC**



A handwritten signature in blue ink, similar to the previous one, with multiple overlapping loops and a long horizontal stroke.

**AB. Brenda Reyes Tomalá Mgt.
TUTORA**

DEDICATORIA

Dedico este trabajo primeramente a Dios, por ser mi guía y mi fortaleza en cada momento de este camino.

A mis padres, Jhonny Torres y Soraya Herrera, por su amor incondicional, por cada palabra de aliento, por cada sacrificio silencioso y por enseñarme con el ejemplo que la constancia y la fe abren todas las puertas. Esta meta es tan suya como mía.

A mi hermano Heyder por su compañía sincera y por ser una fuente constante de ánimo y apoyo.

Con gratitud infinita, les dedico este logro que marca un paso más en mi crecimiento personal y profesional.

- Nathaly Torres Herrera

A mi mamá Blanca Yagual, quien ha sido el pilar fundamental que me ha sostenido en cada paso a lo largo de mi vida, siempre estando a mi lado, brindándome el consejo, el apoyo y el aliento que tanto he necesitado. Le debo todo lo que soy y lo que llegaré a ser, tanto en lo profesional como en lo personal, porque en cada uno de mis logros ella siempre será mi fuente de inspiración.

A mi papá, mi hermano y mis tías porque sin su apoyo constante nunca habría podido llegar hasta donde estoy ahora. Ellos han sido una parte fundamental en mi formación como persona, guiándome y acompañándome durante toda mi vida.

Finalmente, a mis ángeles, mis abuelitos que desde el cielo sé que siempre me han cuidado y protegido como lo hicieron en vida, este logro también es de todos ustedes.

- Carlos Vera Yagual

AGRADECIMIENTO

A la Universidad Estatal Península de Santa Elena, expresamos nuestra más profunda gratitud por habernos acogido como estudiantes y por habernos brindado una formación académica integral a lo largo de nuestra carrera universitaria. Esta casa de estudios ha sido el espacio donde sembramos nuestros sueños y hoy cosechamos sus frutos con orgullo y compromiso profesional.

A la Dra. Brenda Reyes, quien asumió la tutoría de este trabajo de investigación, le extendemos nuestro más sincero agradecimiento por su guía permanente, sus observaciones oportunas y su acompañamiento riguroso durante todo el proceso investigativo, su apoyo ha sido fundamental para alcanzar los objetivos propuestos.

A la Dra. Nicolasa Panchana, Dra. Karen Díaz y la Dra. Isabel Gallegos, docentes de la universidad, expresamos nuestro más profundo agradecimiento por la dedicación, el compromiso y la excelencia con los que guiaron nuestra formación académica, sus enseñanzas nos dejaron valiosas lecciones que han contribuido significativamente a nuestro crecimiento profesional y humano, gracias por inspirarnos a ejercer el Derecho con responsabilidad, disciplina y ética.

Al Ab. Víctor Manuel Coronel Ortiz, docente y director de la carrera de Derecho, le extendemos un especial reconocimiento por el acompañamiento brindado durante nuestra formación académica, su claridad en la enseñanza del derecho y su compromiso dejó una huella imborrable en nuestra preparación.

De igual manera, agradecemos a los departamentos institucionales, autoridades y profesionales de la Universidad Estatal Península de Santa Elena que nos brindaron su colaboración para la recolección de información a través de entrevistas, y cuya disposición fue clave para el desarrollo de esta investigación, su apertura y contribuciones han enriquecido profundamente nuestro trabajo.

A todos quienes han sido parte de este proceso, muchas gracias por habernos acompañado en este camino académico.

- Nathaly Torres Herrera y Carlos Vera Yagual

ÍNDICE

PORTADA	I
CONTRAPORTADA	II
APROBACIÓN DEL TUTOR	III
CERTIFICACIÓN ANTIPLAGIO	IV
CERTIFICACIÓN GRAMATICAL Y ORTOGRAFÍA	V
DECLARACIÓN DE AUTORÍA	VI
APROBACIÓN DEL TRIBUNAL DE GRADO	VII
DEDICATORIA	VIII
AGRADECIMIENTO	IX
ÍNDICE GENERAL	X
ÍNDICE DE CUADROS	XII
ÍNDICE DE GRÁFICOS	XII
ÍNDICE DE ILUSTRACIONES	XIII
ÍNDICE DE ANEXOS	XIII
RESUMEN	XIV
ABSTRACT	XV
INTRODUCCIÓN	1
CAPÍTULO I	3
1. PROBLEMA DE LA INVESTIGACIÓN.....	3
1.1 Planteamiento del problema	3
1.2 Formulación del problema.....	6
1.3 Objetivos.....	6
1.4 Justificación	7
1.5 Variable de investigación e Idea a Defender	8
CAPÍTULO II	9
2. MARCO REFERENCIAL	9
2.1 Marco teórico.....	9
2.1.1 Generalidades de la Protección de Datos.....	9
2.1.2 La protección de Datos Personales en el Ecuador	12
2.1.3 La Protección de Datos como Derecho de cuarta generación	14
2.1.4 Derecho a la protección de datos	15

2.1.5 Derecho a Ser Informados	16
2.1.6 Consentimiento Informado	19
2.1.7 Obligación de Notificación	21
2.1.8 Derechos sobre Contenidos Emitidos, Transmitidos, Retransmitidos y Comunicados Públicamente.....	23
2.1.9 Impacto de la Violación del Principio de Finalidad.....	24
2.1.10 Abuso de la Información.....	26
2.1.11 Gestión de los Datos Personales en el Sistema Educativo Ecuatoriano	28
2.1.12 Universidad Estatal Península de Santa Elena.....	33
2.2 Marco Legal.....	36
2.3 Marco Conceptual.....	53
CAPÍTULO III	55
3. MARCO METODOLÓGICO	55
3.1 Diseño y tipo de Investigación.....	55
3.2 Recolección de la Información	56
3.3 Tratamiento de la Información	62
3.4 Operacionalización de variables	64
CAPÍTULO IV	68
4 RESULTADOS Y DISCUSIÓN	68
4.1 Análisis, interpretación y discusión de resultados	68
4.2 Verificación de la Idea a Defender	91
CONCLUSIONES	92
RECOMENDACIONES	93
BIBLIOGRAFÍA	93
ANEXOS	96

ÍNDICE DE CUADROS

CUADRO 1 POBLACIÓN	56
CUADRO 2 MUESTRA	58
CUADRO 3 PREGUNTA 1	68
CUADRO 4 PREGUNTA 2	69
CUADRO 5 PREGUNTA 3	70
CUADRO 6 PREGUNTA 4	71
CUADRO 7 PREGUNTA 5	72
CUADRO 8 PREGUNTA 6	73
CUADRO 9 PREGUNTA 7	74
CUADRO 10 PREGUNTA 8	75
CUADRO 11 PREGUNTA 9	76
CUADRO 12 PREGUNTA 10	77

ÍNDICE DE GRÁFICOS

GRAFICO 1 PRINCIPIOS FUNDAMENTALES DEL DERECHO A LA PROTECCIÓN DE DATOS	16
GRÁFICO 2 TIPOS DE ABUSO DE LA INFORMACIÓN.....	27
GRÁFICO 3 PREGUNTA 1	68
GRÁFICO 4 PREGUNTA 2	69
GRÁFICO 5 PREGUNTA 3	70
GRÁFICO 6 PREGUNTA 4	71
GRÁFICO 7 PREGUNTA 5	72
GRÁFICO 8 PREGUNTA 6	73
GRÁFICO 9 PREGUNTA 7	74
GRÁFICO 10 PREGUNTA 8	75
GRÁFICO 11 PREGUNTA 9	76
GRÁFICO 12 PREGUNTA 10	77

ÍNDICE DE ILUSTRACIONES

ILUSTRACIÓN 1 Entrevista, Ing. Fabricio Ramos Mgt. Director de Departamento De Tic	96
ILUSTRACIÓN 2 Entrevista, Lcda. Gisella Paula Chica, PhD. Vicerrectora de la Universidad Estatal Península de Santa Elena	96
ILUSTRACIÓN 3 Entrevista, Lic. Marlon Novillo, Mgt. Director de Departamento de Bienestar Estudiantil.....	97
ILUSTRACIÓN 4 Entrevista, Abg. María Rivera González, Mgt. Secretaria General	97

ÍNDICE DE ANEXOS

ANEXO 1 Evidencias Fotográficas.....	96
ANEXO 2 CUESTIONARIO APLICADO A ESTUDIANTES DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA	98
ANEXO 3 ENTREVISTA AL DEPARTAMENTO DE TIC DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA	100
ANEXO 4 ENTREVISTA A LA VICERECTORA DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA	101
ANEXO 5 ENTREVISTA AL DEPARTAMENTO DE BIENESTAR ESTUDIANTIL DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA.....	102
ANEXO 6 ENTREVISTA A LA SECRETARIA GENERAL DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA	103

**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD
CARRERA DE DERECHO**

**PRINCIPIO DE FINALIDAD EN LA PROTECCIÓN DE DATOS
PERSONALES: CASO ESTUDIANTES DE LA UNIVERSIDAD
ESTATAL PENÍNSULA DE SANTA ELENA, 2024**

Autores: Nathaly Torres
Carlos Vera

Tutora: Ab. Brenda Reyes

RESUMEN

Esta investigación radica en demostrar los protocolos basados en el consentimiento informado para la recolección de la información de los datos sensibles de los estudiantes, contemplando el principio de finalidad estipulado en el artículo 10 inciso d) de la Ley Orgánica de Protección de Datos Personales, mediante el estudio realizado se destaca que la Universidad Estatal Península de Santa Elena consta con la falta de mecanismos y protocolización en la recolección de los datos sensibles de su comunidad universitaria, lo cual se vuelve preocupante en torno a la posible vulneración de los derechos a la privacidad de dicha información, esto debido a la gran cantidad de estudiantes que alberga y toda la información que recauda durante cada periodo académico. Aunque la universidad comprende la importancia de la protección de datos, su falta de base normativa, mecanismos para su correcto manejo y su falta del desarrollo de una estructura normativa interna que garantice el manejo adecuado de estos datos puede llegar a generar riesgos legales y éticos. Es así que la falta de consentimiento informado e inexistencia de procedimientos formales para su tratamiento constituyen una seria vulneración de los derechos a la privacidad y protección de datos personales, especialmente en el marco de la LOPDP. El presente trabajo investigativo nos permite llegar a la conclusión de que la falta de protocolos y políticas institucionales dentro de la universidad no sólo evidencia una debilidad administrativa, sino también un incumplimiento de obligaciones legales y riesgos a los derechos fundamentales de los estudiantes, en este caso es necesario que la universidad desarrolle y aplique políticas claras de protección de datos, capacitando a su personal, estableciendo procedimientos específicos para la recolección, tratamiento, almacenamiento y eventual eliminación de la información sensible, sólo así se podrá garantizar el respeto a la privacidad de su comunidad y alinearse con la legislación vigente en el país.

Palabras clave: Consentimiento, informado, datos, sensibles, protección.

ABSTRACT

The basis of this research is to demonstrate the protocols based on informed consent for the collection of sensitive student data, considering the principle of purpose stipulated in Article 10, paragraph d) of the Organic Law on Personal Data Protection. The study highlights that the Peninsula State University of Santa Elena lacks mechanisms and protocols for the collection of sensitive data from its university community. This is a concern regarding the potential violation of the right to privacy regarding such information, due to the large number of students it houses and all the information it collects during each academic period. Although the university understands the importance of data protection, its lack of a regulatory basis, mechanisms for its correct management, and its failure to develop an internal regulatory structure to guarantee the proper handling of this data can generate legal and ethical risks. Thus, the lack of informed consent and formal procedures for processing it constitute a serious violation of the rights to privacy and personal data protection, especially within the framework of the LOPDP (Lectoral and Data Protection Act). This research allows us to conclude that the lack of institutional protocols and policies within the university not only demonstrates administrative weakness, but also a failure to comply with legal obligations and poses risks to students' fundamental rights. In this case, it is necessary for the university to develop and implement clear data protection policies, training its staff, and establishing specific procedures for the collection, processing, storage, and eventual disposal of sensitive information. Only then can it guarantee respect for the privacy of its community and align itself with current national legislation.

Keywords: Consent, informed, data, sensitive, protection.

INTRODUCCIÓN

La protección de los datos personales representa hoy en día una garantía esencial para el respeto de la privacidad y la dignidad humana, es por ello que en el presente trabajo de investigación de naturaleza jurídica tiene como finalidad examinar la aplicación del principio de finalidad en el tratamiento de los datos personales de los estudiantes por parte de la Universidad Estatal Península de Santa Elena, en el marco de lo establecido en la Ley Orgánica de Protección de Datos Personales. Esta investigación surge ante la necesidad de determinar si la recolección, almacenamiento y uso de los datos personales dentro del entorno universitario se ajusta al fin específico, legítimo y explícito que exige la normativa vigente, garantizando a su vez el respeto al consentimiento informado del titular de los datos.

La problemática identificada radica en la posible falta de mecanismos claros y formalizados dentro de la UPSE para informar adecuadamente a los estudiantes sobre los fines para los cuales serán utilizados sus datos y, en consecuencia, obtener de ellos un consentimiento libre, informado e inequívoco, tal como lo exige el artículo 10 de la LOPDP. El estudio se orienta a analizar el tratamiento actual que la universidad otorga a los datos personales, evaluar el conocimiento que poseen los estudiantes sobre el uso de su información, y determinar el grado de cumplimiento del principio de finalidad, a partir de ello, se busca proponer recomendaciones que permitan fortalecer las políticas internas de protección de datos personales.

En el Capítulo I se aborda el problema de investigación, definiendo su contexto, delimitación, objetivos y justificación, se establece la idea a defender sobre la necesidad de implementar

mecanismos de consentimiento informado que garanticen el cumplimiento del principio de finalidad en el tratamiento de datos personales por parte de la UPSE.

El Capítulo II, correspondiente al marco referencial, contiene un análisis teórico, legal y conceptual de los elementos que sustentan la investigación, se exploran los fundamentos doctrinarios y jurídicos del derecho a la protección de datos personales, el consentimiento informado, el principio de finalidad y su implicación en el ámbito educativo, así como el análisis de la normativa aplicable, incluyendo la Constitución del Ecuador, la LOPDP y los instrumentos internacionales en materia de derechos humanos.

El Capítulo III lleva por título Marco Metodológico, donde se detalla el tipo de investigación, aquí se estructuró el enfoque metodológico y los instrumentos utilizados para la recolección de datos, la investigación se apoya en técnicas cualitativas y cuantitativas incluyendo encuestas dirigidas a los estudiantes y entrevistas a funcionarios de áreas específicas de recolección de datos de la universidad en donde gestionan información personal.

Finalmente, el Capítulo IV sujeta el análisis, interpretación y discusión de los resultados obtenidos, confrontando la normativa con la práctica institucional, lo cual permite verificar la hipótesis planteada, se sustenta la necesidad de fortalecer los procesos de gestión de datos personales de la UPSE, promoviendo un tratamiento transparente con los derechos de los estudiantes, conforme a los principios establecidos en la LOPDP. De este modo, se generan conclusiones y recomendaciones jurídicas orientadas a contribuir con la consolidación de una cultura de protección de datos en el ámbito universitario.

CAPÍTULO I

1. PROBLEMA DE LA INVESTIGACIÓN

1.1 Planteamiento del problema

La pandemia Covid-19 se constituyó en periodo de crisis sanitaria que transformó las tradicionales prácticas de comunicación, educativas de intercambio de bienes y servicios entre otros aspectos en los que la tecnología impulsó la celeridad de los procesos, tomando como base y fundamento la recolección de datos personales, sin que a esa fecha hayan existido reglas claras para el tratamiento de estos, generando múltiples situaciones de inadecuado incluso malicioso manejo o procesamiento de datos sensibles. En este contexto, nace La Ley Orgánica de Protección de Datos Personales del Ecuador, de ahora en adelante LOPDP, que entró en vigor en Ecuador el 26 de mayo de 2021, esta ley marcó un hito en el manejo y tratamiento de la información personal. Esta legislación tiene como objetivo garantizar la protección de los datos personales de las personas, promoviendo una cultura de respeto a la dignidad humana y la integridad de los individuos, además, la ley busca fomentar un entorno digital seguro en donde las organizaciones, independientemente de su tamaño, puedan gestionar los datos de manera adecuada, conforme a los principios establecidos en la normativa, uno de los pilares fundamentales de esta ley es el principio de finalidad, que regula cómo deben ser recogidos, tratados y utilizados los datos personales.

El principio de finalidad, conforme lo establece el artículo 10, inciso d) de la LOPDP, indica que los datos personales deben ser recolectados y tratados únicamente para fines específicos, explícitos y legítimos, esta prohíbe que dichos datos se utilicen para fines distintos sin el consentimiento previo y expreso del titular. Esta disposición subraya la importancia de informar a los titulares de los datos sobre el propósito para el cual se solicita su información y obtener su consentimiento informado, con el fin de asegurar un tratamiento adecuado y transparente de los datos, evitando cualquier tipo de mal manejo en base al uso irresponsables de los datos sensibles de las personas.

En la Universidad Estatal Península de Santa Elena, de ahora en adelante UPSE, se recolectan y tratan diariamente datos personales de los estudiantes para diversos fines administrativos y académicos, los datos que generalmente se solicitan incluyen nombres, apellidos, número de cédula, dirección, correo electrónico, números telefónicos y otros datos académicos relacionados con su desempeño, inscripción en materias, asistencia a clases, calificaciones, entre otros. Estos datos son indispensables para gestionar los servicios que la universidad ofrece a los estudiantes, contando también con el registro en asignaturas, la emisión de certificados y la administración de becas y beneficios.

No obstante, el proceso de recolección y tratamiento de datos en la UPSE requiere ser analizado en cuanto a la forma en que se garantiza el consentimiento informado y la claridad sobre los fines específicos para los que se utilizará la información de los estudiantes. En muchos casos, los estudiantes no son plenamente conscientes de cómo se utilizarán sus datos más allá de los propósitos administrativos, ni se les solicita formalmente su consentimiento para otros usos que pudieran derivarse de su información personal, esto plantea un problema significativo en cuanto a la protección de los derechos de los estudiantes, ya que podría dar lugar a un uso inadecuado de la información, vulnerando su privacidad y autonomía.

El consentimiento informado es un elemento clave para la legitimidad en el tratamiento de datos personales. Según la LOPDP, dicho consentimiento debe ser libre, informado, específico y explícito. Sin embargo, en la UPSE, el consentimiento no siempre se solicita de manera adecuada, ni se informa a los estudiantes de forma clara y transparente sobre el uso que se dará a sus datos, y esta situación crea un ambiente de incertidumbre que podría afectar no solo la confianza de los estudiantes en la institución, sino también su percepción de seguridad y privacidad en el manejo de su información personal.

De acuerdo con Thiel (2020), "el respeto al principio de finalidad es esencial para mantener la confianza del titular de los datos en las instituciones que los recolectan, especialmente en un contexto donde la transparencia y la protección de la privacidad son fundamentales para garantizar que el manejo de datos personales no derive en usos indebidos" (p. 78). Esta afirmación pone de manifiesto la importancia de garantizar que los datos personales sean

utilizados exclusivamente para los fines que fueron comunicados, y que cualquier uso adicional deba ser previamente autorizado por el titular de los datos. Por otro lado, Vázquez Requena resalta que:

“La violación del principio de finalidad puede conllevar serias repercusiones legales, incluidas sanciones para la entidad responsable del tratamiento de datos, además de consecuencias éticas, dado que se vulnera el control que el titular debe tener sobre su propia información” (2019, pág. 132).

A nivel universitario, el manejo de datos personales es especialmente delicado, ya que los estudiantes depositan en la institución una confianza implícita sobre el tratamiento seguro de su información. En palabras de Solove y Schwartz (2020), “en el entorno educativo, donde se maneja un volumen considerable de datos sensibles, es vital que las políticas de privacidad sean claras y que los estudiantes sean conscientes de cómo se utilizará su información” (p. 214). Esto sugiere que la falta de claridad y transparencia en las políticas de manejo de datos no solo podría llevar a un mal manejo de la información, sino que también podría vulnerar gravemente la privacidad de los estudiantes, exponiéndolos a posibles riesgos de filtración o uso indebido de sus datos.

En este sentido, la situación en la UPSE presenta un claro desafío para el cumplimiento del principio de finalidad, a pesar de que los datos personales recolectados pueden ser esenciales para la operación y administración de los servicios universitarios, la ausencia de mecanismos claros para informar a los estudiantes sobre los fines específicos para los cuales se utilizarán sus datos y la carencia de un proceso adecuado para obtener su consentimiento informado podrían traducirse en incumplimientos de la LOPDP. Esto no solo genera riesgos legales para la universidad, sino también una vulnerabilidad para los estudiantes, quienes podrían ver comprometida su privacidad sin estar plenamente conscientes de los usos de su información.

Por tanto, el presente estudio se enfocará en analizar el cumplimiento del principio de finalidad en la recolección y tratamiento de datos personales de los estudiantes en la UPSE, y cómo la falta de consentimiento informado puede afectar a la transparencia y la confianza en el manejo de los datos. Se busca identificar prácticas actuales de la universidad en relación con la protección de datos, examinar si los estudiantes son informados adecuadamente sobre

el propósito del uso de su información personal y evaluar si se garantiza un consentimiento informado adecuado conforme a lo que establece la normativa vigente.

La protección de los datos personales en el ámbito universitario es un tema de vital importancia, ya que, como señala Solove (2008), "la falta de claridad y comunicación en el tratamiento de datos puede llevar a vulneraciones significativas de la privacidad y la seguridad de la información" (p. 103). En este sentido, la UPSE debe adoptar medidas correctivas que le permitan alinear sus procedimientos con lo establecido por la LOPDP, garantizando no solo el cumplimiento legal, sino también el respeto a los derechos fundamentales de los estudiantes y el mantenimiento de la confianza de la comunidad universitaria.

1.2 Formulación del problema

¿De qué manera afecta la falta de implementación del principio de finalidad en el manejo de los datos personales de los estudiantes de la Universidad Estatal Península de Santa Elena?

1.3 Objetivos

Objetivo General

Analizar el tratamiento de los datos personales de los estudiantes por parte de la Universidad Estatal Península de Santa Elena, mediante un enfoque general estudiantil en base al conocimiento que poseen sobre la recolección de sus datos personales, el estudio jurídico del principio de finalidad y los componentes del consentimiento, a fin de que se permita la valoración del tratamiento de datos personales, asimismo recomendar ajustes a los estándares institucionales, legales y éticos de los elementos de consentimiento establecidos en la normativa de la protección de datos personales dentro del ámbito universitario.

Objetivo específico

- ❖ Evaluar las prácticas actuales de la Universidad Estatal Península de Santa Elena en la recolección y uso de los datos personales de los estudiantes, identificando posibles

incumplimientos con el principio de finalidad.

- ❖ Examinar el nivel de conocimiento y la percepción de los estudiantes sobre el uso de sus datos personales por parte de la universidad, y si han sido adecuadamente informados sobre el propósito de dicha recolección.
- ❖ Proponer recomendaciones para el mejoramiento en el manejo de los datos sensibles por parte de la universidad, asegurando el cumplimiento del principio de finalidad según como se lo estipula en la Ley Orgánica de Protección de Datos Personales.

1.4 Justificación

En el presente trabajo investigativo, se aborda el tratamiento de los datos personales de los estudiantes en la Universidad Estatal Península de Santa Elena (UPSE), con especial atención al Principio de Finalidad estipulado en la Ley Orgánica de Protección de Datos Personales. Este principio establece que los datos deben ser conseguidos y tratados con propósitos específicos y legítimos, garantizando que su uso no se desvíe de dichos fines específicos sin el consentimiento expreso del titular, a través de este estudio, se busca analizar cómo se aplica este principio en el entorno educativo, evaluando si las prácticas actuales aseguran el apropiado cumplimiento de las normativas vigentes.

Desde el punto de vista teórico, este estudio beneficiará al ámbito académico al profundizar en el análisis jurídico del Principio de Finalidad y su aplicación en instituciones de educación superior en Ecuador. Se espera generar un cuerpo teórico sólido que sirva como base para futuros trabajos de investigación, proporcionando una mejor comprensión de la normativa sobre la protección de datos y su relevancia en la defensa de derechos fundamentales en argumentos educativos.

En el ámbito metodológico, la investigación propondrá un enfoque práctico para evaluar la aplicación del Principio de Finalidad, a través de un análisis crítico de las políticas de protección de datos de la UPSE, de esta manera, se espera que los resultados ofrezcan herramientas que puedan ser replicadas o adaptadas por otras universidades interesadas en revisar sus propias prácticas en relación con la protección de la información de sus

estudiantes.

Finalmente, desde una perspectiva práctica, los resultados de la investigación contribuirán al fortalecimiento de la gestión de datos personales de los estudiantes en la UPSE. Esto abrirá la posibilidad de mejorar las políticas internas, garantizar el respeto de los derechos de los estudiantes y asegurar un manejo ético de su información, los hallazgos podrán ser utilizados por las autoridades universitarias y entidades regulatorias para implementar medidas que refuercen el cumplimiento de las obligaciones legales en materia de protección de datos, incrementando la confianza de la comunidad educativa en el manejo de su información.

1.5 Variable de investigación e Idea a Defender

Variables de investigación

V1: Principio de finalidad. VD

V2: Protección de Datos Personales de los estudiantes de la Universidad Estatal Península de Santa Elena. VI

Idea a defender

La recepción de datos sensibles no se sujeta a mecanismos que garantiza el consentimiento informado en la recolección de datos personales de los estudiantes de la Universidad Estatal Península de Santa Elena, lo que vulnera el principio de finalidad, al no establecerse de forma clara y específica los propósitos para los cuales dichos datos son recopilados.

CAPÍTULO II

2. MARCO REFERENCIAL

2.1 Marco teórico

2.1.1 Generalidades de la Protección de Datos

La protección de datos personales era considerado como un mecanismo para proteger el derecho a la vida privada, a partir de finales de los años de 1970 en países europeos como Francia y Alemania, la Unión Europea se convirtió en el ejemplo a seguir en el área, a partir de la directiva 95-46-CE la cual fue promulgada en octubre de 1995, catalogada como una directiva de la misma organización, que regulaba el procesamiento de los datos personales y la libre circulación de datos dentro de dicha asociación, debido a problemas de homogeneización entre los países miembros por la falta de mecanismos que permitan lograr su cumplimiento, surge el Reglamento General de Protección de Datos, de ahora en adelante RGPD, ley que entra en aplicación el 25 de mayo de 2018. La RGPD es la reglamentación jurídica más importante en materia de protección del derecho a la seguridad de la información, debido a que se los considera como el instrumento del derecho más proactivo con más impacto en la historia dentro de la materia, esto, fundamentado en la gestión de riesgos, puesto que ha cambiado radicalmente la manera de procesar datos personales en el mundo, por lo que gracias a ello la mayoría de países latinoamericanos se encuentran en procesos de reforma de sus leyes de protección de datos para seguir acorde a lo estipulado en el RGPD, estableciendo que las sanciones llegan hasta el 4% de la facturación anual de una institución pública o privada, aunque la realidad es que todavía existe mucha incertidumbre en base a su gestión. En el año 2018 en Estados Unidos, se promulga la California Consumer Privacy Act, en adelante CCPA, entra en vigor el 1 de enero de 2020, fusionando de manera armoniosa la visión estadounidense sobre el derecho a la privacidad de la información

personal de las personas, con un marco alto en protección parecido al del Reglamento General de Protección de Datos, estableciendo que las organizaciones deben proporcionar un aviso claro y obtener permiso explícito para recopilar datos confidenciales, implementar medidas razonables para proteger los datos de los consumidores, es por ello que según la CCPA:

“La información personal se define como cualquier dato que identifique, se relacione, describa o pueda vincularse razonablemente como un consumidor u hogar específico de California” (2020).

En el ámbito latinoamericano, el 4 de octubre del 2000 en Argentina se crea la primera Ley de Protección de Datos Personales 25.326 cuyas siglas son PDPA, ley que siguió el modelo de la directiva 95-46-CE de la Unión Europea, sin embargo, en la actualidad ya se encuentra en reforma debido a que fue considerada bajo el título de obsoleta, considerando el nuevo estándar internacional establecido por el RGPD de la Unión Europea. En esta misma línea, en el año 2011 Perú aprueba la Ley Peruana de Protección de Datos la cual resultó ser bastante eficiente en cuanto a sus derechos, principios y sanciones, aun siendo de la era pre-RGPD por lo que también fue sometida a un proceso de reforma, sin embargo, es necesario resaltar que fue la primera ley de protección de datos de la Comunidad Andina de Naciones CAN. Por su parte en 2012, Colombia promulgó la Ley Estatutaria 1581, cuyo propósito era desarrollar el derecho constitucional de todas las personas a conocer, actualizar y rectificar la información que se haya recopilado sobre ellas en bases de datos o archivos, así como garantizar otros derechos, libertades y garantías constitucionales. A pesar de ello, por seguir el modelo de la directiva 95-46-CE de la Unión Europea, también se consideró que era necesario una actualización bajo los parámetros normativos establecidos por el Reglamento General de Protección de Datos.

Con estos precedentes dentro del territorio latinoamericano, Ecuador aprueba su Ley Orgánica de Protección de Datos en mayo del 2021, con muchas similitudes a lo dispuesto en el Reglamento General de la Protección de Datos, con la aplicación de dicha ley se establece que todas las instituciones tanto públicas y privadas deben estar preparadas de conformidad a lo que se estipule en la normativa, es por ello que se vuelve fundamental que todas las organizaciones, identifiquen los datos personales que manejan, los soportes donde

se encuentran estos datos y, en general revisen el tratamiento que le están otorgando, con el fin de qué se verifique si el tratamiento cumple con lo determinado en la ley y con los principios que la misma contempla, asimismo es necesario que cada organización adopte su tratamiento a su infraestructura y giro de negocio, esto con el objetivo de establecer una hoja de ruta apropiada para la implementación de esta normativa de una manera adecuada. La definición de una hoja de ruta es la consecuencia de un diagnóstico previo de la organización que permite tener un panorama más esclarecido en base a su situación actual respecto a los datos personales que en la misma manera, no sólo es el cumplimiento legal, sino también desde la seguridad que brinda el tratamiento de estos datos sensibles, entendiendo que no solo radica en un asunto de materia jurídica sino en un trabajo más de gestión sobre el manejo de estos datos sensibles.

El desarrollo de la protección de datos personales no solo se limita a la implementación de leyes, sino también a la evolución de principios fundamentales que rigen esta materia, entre estos principios destacan el de finalidad, el consentimiento informado, la transparencia y responsabilidad proactiva, estos conceptos, han sido adaptados en diferentes contextos nacionales, reflejando las necesidades y particularidades de cada región, en este sentido, el RGPD ha sido una herramienta clave para establecer un lenguaje común que permita armonizar los esfuerzos globales en torno a la privacidad y la protección de datos.

En el ámbito tecnológico, los avances en inteligencia artificial, big data y blockchain han planteado nuevos desafíos para la protección de datos personales, estas tecnologías, aunque prometen mejorar la eficiencia y la toma de decisiones, también incrementan los riesgos asociados al tratamiento masivo de información, países como Brasil, con la Ley General de Protección de Datos, de ahora en adelante LGPD, han adoptado marcos normativos que no solo regulan el uso de estas tecnologías, sino que también fomentan el desarrollo de estándares técnicos que aseguren el cumplimiento de los principios de privacidad, este enfoque preventivo ha sido determinante para fortalecer la confianza en el uso de datos en entornos digitales.

La protección de datos personales ha tenido un impacto significativo en la manera en que las

empresas operan y gestionan la información de sus clientes, la implementación de programas de cumplimiento normativo, auditorías internas y capacitaciones ha llevado a las organizaciones a adoptar un enfoque más ético y transparente en el tratamiento de los datos y esto no solo mejora su reputación corporativa, sino que también les permite evitar sanciones económicas y legales, este proceso de transformación ha sido particularmente relevante para sectores como el financiero, el sanitario y el de comercio electrónico, donde la confianza del usuario juega un papel fundamental en la sostenibilidad del negocio.

Por último, el reconocimiento del derecho a la protección de datos como un derecho humano ha impulsado su inclusión en instrumentos internacionales y constituciones nacionales, este enfoque ha permitido consolidar su relación con otros derechos fundamentales, como la libertad de expresión, la igualdad y la no discriminación, en Ecuador, la Constitución de 2008 ya reconocía la importancia de la protección de datos dentro del marco de los derechos digitales, estableciendo las bases para la posterior promulgación de la Ley Orgánica de Protección de Datos Personales, este marco normativo refuerza el compromiso del país con la protección de la privacidad y la promoción de un entorno seguro para el desarrollo de la sociedad de la información.

2.1.2 La protección de Datos Personales en el Ecuador

Ante el vertiginoso desarrollo de las tecnologías de la información y la comunicación, el derecho a la protección de datos personales ha emergido como una necesidad impostergable dentro de los Estados constitucionales, en el caso ecuatoriano, la promulgación de la Ley Orgánica de Protección de Datos Personales en mayo de 2021 representa un hito normativo que responde a los desafíos que impone la sociedad digital contemporánea, donde el uso masivo de datos se ha vuelto moneda corriente en casi todas las esferas sociales, educativas y económicas.

Desde una perspectiva constitucional, el derecho a la protección de datos se enlaza con la garantía de la dignidad humana, entendida no solo como un principio del ordenamiento jurídico, sino como el núcleo del constitucionalismo moderno, como señala Luigi Ferrajoli (2001), "la dignidad es el presupuesto axiológico de todos los derechos fundamentales y exige que el ser humano no sea tratado como un medio, sino siempre como un fin en sí

mismo", bajo esta premisa, el tratamiento de datos personales debe realizarse con respeto al consentimiento, la autodeterminación informativa y la privacidad.

En el plano teórico, esta necesidad de control sobre los propios datos personales se vincula también con la noción de autonomía de la voluntad, piedra angular del constitucionalismo contemporáneo, autores como Jürgen Habermas han subrayado que la libertad individual, en contextos altamente tecnologizados, solo puede ejercerse plenamente si las personas conservan control sobre la información que las identifica, por tanto, el manejo inadecuado o arbitrario de datos personales puede traducirse en una forma moderna de dominación o exclusión.

A esto se suma la teoría del “mosaico de datos” desarrollada por Daniel J. Solove, que plantea cómo pequeños fragmentos de información, aparentemente inofensivos por separado, pueden al combinarse revelar aspectos profundamente sensibles sobre la vida privada del titular, en este sentido, lo que está en juego no es simplemente la posesión de un dato aislado, sino el poder de perfilar y predecir comportamientos, preferencias y decisiones futuras, el riesgo no radica solo en la recolección, sino en el uso inteligente y potencialmente invasivo que pueden hacer terceros de esa información.

Además, autores como Stefano Rodotà han aportado una perspectiva ética y jurídica sobre el tratamiento de los datos personales como una extensión del propio cuerpo, y, por tanto, parte de la identidad individual. En su obra *Tecnopolítica. La democracia y las nuevas tecnologías de la comunicación* (2007), Rodotà sostiene que “los datos personales no son cosas, son expresión de la personalidad de los sujetos, por lo que su tratamiento debe estar siempre bajo el control de quien los genera” (p. 122).

La necesidad de proteger los datos personales cobra especial relevancia en ámbitos como el educativo, donde los estudiantes deben confiar su información personal a instituciones que muchas veces no tienen protocolos claros ni una cultura de transparencia en el tratamiento de la información, ello plantea una tensión entre los principios constitucionales y las prácticas institucionales. Como afirma Gregorio Peces-Barba, “el respeto a los derechos fundamentales no solo requiere leyes que los reconozcan, sino estructuras sociales e institucionales que los hagan posibles” (2005, p. 46), por tanto, la protección de datos personales no debe verse únicamente como una respuesta jurídica al avance tecnológico, sino

como un compromiso constitucional con la libertad, la intimidad y el respeto por la persona humana.

2.1.3 La Protección de Datos como Derecho de cuarta generación

Los derechos de cuarta generación, se los establece como un conjunto de derechos humanos los cuales se han desarrollado dentro del contexto de las nuevas tecnologías de la información y la comunicación (TIC) sustentados en la necesidad de asegurar el acceso a las mismas, dentro de estos derechos se manifiestan los derechos generacionales es una caracterización de los Derechos Humanos que identifican diversas oleadas o generaciones de reconocimiento histórico de los mismos, la división en generaciones de los Derechos Humanos para su estudio es una creación del checoslovaco ex director de la División de Derechos humanos y Paz de la UNESCO, Karel Vašák (1929), quien fue el que introdujo el concepto con su conferencia en el Instituto Internacional de los Derechos Humanos, en Estrasburgo, inspirado en el lema de la República Francesa denominado: libertad, igualdad y fraternidad, esta última siendo sustituida por, solidaridad, tiempos después. Las tres primeras generaciones de derechos humanos son fundamentalmente producto de la evolución política de las sociedades nacionales e internacionales.

En los derechos de cuarta generación se manifiestan las innovaciones tecnológicas y la globalización, aquí se encuentran los derechos de acceso a la tecnología y medios de comunicación, estos mismos surgiendo a finales del siglo XX e inicios del siglo XXI con la escalada de creación de tecnología y globalización que experimentó el mundo. Tal como lo menciona la revista Derechos Fundamentales y Justicia:

“Los derechos de cuarta generación son a la democracia, a la información y al pluralismo como reflejo de la globalización política y el ánimo de asegurar el futuro de la ciudadanía y la libertad de todos los pueblos” (Bonavides, 2008).

Con este pensamiento se puede entender que los derechos de cuarta generación son mecanismos legales que buscan responder a los retos y desafíos que surgen dentro de la globalización con la tecnología y su avance en el tiempo, protegiendo y respetando todo acceso a la información, la privacidad y al pluralismo; en cierto aspecto, gracias a esta cuarta

generación de derechos la democracia toma una forma más compacta dentro de la sociedad, debido a que permite una ciudadanía mejor informada, con mayor participación y promoviendo un entorno donde diferentes culturas pueden coexistir, esto siendo fundamental ya que nos encontramos en un mundo que cada vez está más conectado a través de la tecnología.

Actualmente, a los derechos de cuarta generación se los ve como una necesidad básica interdependiente para el cumplimiento de los demás derechos, por lo que estos derechos buscan asegurar un futuro en donde la libertad y el bienestar de todas las personas no sean vulnerados bajo ningún medio; el ciberespacio, junto a las nuevas tecnologías se presentan como un nuevo mundo omnipresente en el cual surgen nuevos derechos y a su vez los derechos tradicionales toman una nueva dimensión, haciendo referencia al derecho de la tecnología, la libertad de expresión en redes y el derecho a la libre distribución de información.

2.1.4 Derecho a la protección de datos

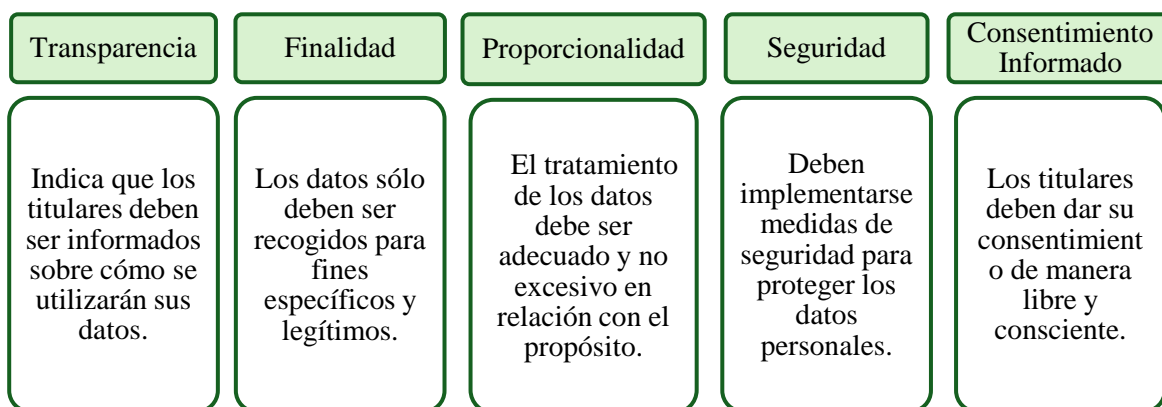
Desde la perspectiva constitucional, el derecho a la protección de datos personales se deriva directamente del principio de dignidad humana y del derecho a la intimidad, ambos reconocidos como pilares fundamentales del ordenamiento jurídico, este derecho garantiza la autonomía personal frente al poder del Estado y de actores privados, asegurando que cada individuo conserve el control sobre su información, en este sentido, el constitucionalismo moderno reconoce que el libre desarrollo de la personalidad exige no solo la protección física y moral del individuo, sino también el resguardo de su identidad informacional. Como señala Luigi Ferrajoli (2001), “los derechos fundamentales imponen límites al poder en todas sus formas y garantizan la inviolabilidad de la esfera personal”, siendo el derecho a la protección de datos una expresión concreta de ese límite en la era digital.

El derecho a la protección de datos personales es considerado un derecho fundamental que permite a los individuos controlar su información personal y como esta es tratada por terceros, este derecho se ha fortalecido a nivel global a la creciente digitalización y al uso intensivo de datos, desde el comercio electrónico hasta la administración pública. Según la

Declaración Universal de Derechos Humanos, "toda persona tiene derecho a la protección de la ley contra injerencias arbitrarias en su vida privada, su familia, su domicilio y su correspondencia" (ONU, 1948).

Para facilitar la comprensión de los conceptos esenciales que rigen el derecho a la protección de datos, se presenta a continuación un gráfico que ilustra los principios fundamentales establecidos en la legislación ecuatoriana. Esta representación visual ayuda a resaltar cómo cada uno de estos principios contribuye a la salvaguarda de la privacidad y la dignidad de los titulares de datos personales:

GRAFICO 1
PRINCIPIOS FUNDAMENTALES DEL DERECHO A LA PROTECCIÓN DE DATOS



Elaborado por: Nathaly Torres y Carlos Vera

Fuente: Ley Orgánica de Protección de Datos Personales

La implementación segura del derecho a la protección de datos no solo protege a las personas, sino que también fomenta la confianza en las instituciones ya sean públicas o privadas que manejan información personal, dentro de un entorno donde los datos son considerados un activo valioso, la protección adecuada de estos derechos es esencial para promover la transparencia y la responsabilidad.

2.1.5 Derecho a Ser Informados

El derecho a ser informados se configura como una manifestación del principio de dignidad humana y del libre desarrollo de la personalidad, en la actualidad, este derecho se rige como una garantía fundamental dentro del tratamiento de datos personales, ya que otorga a los

individuos la posibilidad de conocer, de manera clara, precisa y perceptible, el cómo, por qué y para qué se recogen y utilizan sus datos, su reconocimiento es esencial en un entorno dominado por tecnologías digitales o comercio electrónico, donde los flujos de datos se multiplican y su tratamiento tiene impactos directos sobre los derechos y decisiones de las personas.

La transparencia se presenta como un principio estructural para la protección de datos, ya que permite que los titulares de la información comprendan los procesos a los que sus datos serán sometidos, facilitando una toma de decisiones consciente, como ha señalado la doctrina constitucional, el consentimiento válido solo puede existir cuando está precedido de una información clara, suficiente y accesible. La simple aceptación formal no equivale a un consentimiento legítimo si la persona no ha comprendido realmente el uso que se dará a su información personal, esta situación ha sido especialmente señalada por autores como Bertoni (2020), quien sostiene que “la falta de comprensión sobre el uso de los datos personales es una de las mayores barreras para la efectiva protección de la privacidad en el entorno digital” (p. 105).

El derecho a ser informados se convierte, por tanto, en un elemento habilitante de otros derechos asociados al tratamiento de datos, como el acceso, la rectificación, la oposición o la cancelación, en el caso específico del comercio electrónico, por ejemplo, la transparencia en el uso de los datos es un requisito indispensable para generar confianza entre los consumidores y las plataformas digitales. Las personas suelen proporcionar información altamente sensible al momento de realizar compras o contratar servicios en línea, como datos de contacto, información financiera o historial de navegación, si no se les informa adecuadamente sobre el destino y el uso de esta información, no solo se vulnera su privacidad, sino que también se expone al usuario a posibles riesgos como el robo de identidad, fraudes o manipulación de sus preferencias de consumo.

Aun más complejo es el escenario que plantea el desarrollo de tecnologías basadas en inteligencia artificial, los sistemas de IA pueden procesar enormes volúmenes de datos, realizar análisis predictivos y tomar decisiones automatizadas que afectan directamente a los usuarios, en estos casos, la transparencia no solo debe limitarse a informar que se utiliza inteligencia artificial, sino que debe incluir explicaciones claras sobre el funcionamiento

general del sistema, los criterios utilizados en los algoritmos y los impactos que puede tener en la vida de las personas, esto es especialmente relevante cuando dichas decisiones inciden en ámbitos sensibles como el acceso al crédito, la contratación laboral, los servicios de salud o la educación.

Tal como afirma Bertoni (2020), “la transparencia es una garantía básica para que los titulares mantengan el control sobre sus datos en un mundo cada vez más automatizado” (p. 98). En este sentido, la información que se proporcione al titular debe ser clara, accesible, libre de tecnicismos jurídicos o tecnológicos, y adaptada a distintos niveles de comprensión. Esto es particularmente importante en el entorno educativo, donde los estudiantes al igual que otros usuarios se encuentran en una posición de desventaja frente al poder institucional en cuanto al conocimiento y control del tratamiento de su información personal.

El derecho a ser informados cobra especial relevancia en los contextos donde se manejan datos personales sensibles, como aquellos de naturaleza académica, socioeconómica, médica o psicológica, las entidades que recopilan esta información, especialmente en entornos institucionales, suelen establecer vínculos con plataformas tecnológicas, proveedores de servicios y organismos públicos, lo que amplía los riesgos asociados al tratamiento de datos si no se comunica adecuadamente a los titulares el flujo de esta información hacia terceros, por ello, es indispensable que las personas sean informadas no solo sobre las políticas internas de tratamiento de datos, sino también sobre las condiciones bajo las cuales su información será compartida, quiénes tendrán acceso a ella y con qué finalidades será utilizada.

Una implementación adecuada del derecho a ser informados en estos entornos implica el desarrollo de mecanismos comprensibles y efectivos para comunicar toda la información relevante, un ejemplo de buena práctica es la habilitación de plataformas digitales donde los titulares puedan consultar permanentemente cómo se gestionan sus datos, en qué se emplean y qué derechos pueden ejercer, estas herramientas deben estar diseñadas con un lenguaje claro, de modo que cualquier persona, sin conocimientos jurídicos o tecnológicos avanzados, pueda comprender la información ofrecida, en donde deberían permitir a los titulares gestionar directamente sus derechos, como acceder a su información, solicitar correcciones o ejercer su derecho de oposición.

Igualmente, es esencial que las instituciones informen a los titulares sobre cualquier

modificación que se realice en las políticas de privacidad o en los procesos de tratamiento de datos, especialmente cuando dichas modificaciones implican nuevos fines o encargados del tratamiento, este tipo de comunicación no solo fortalece el principio de transparencia, sino que también garantiza el respeto a la legalidad, a la lealtad en el tratamiento de datos y a la autonomía del titular, quien puede decidir si continúa autorizando el uso de su información o si prefiere limitarlo.

La transparencia en el tratamiento de datos personales no debe entenderse como un mero requisito legal, sino como un valor fundamental que fortalece la confianza entre las partes y promueve una cultura institucional de respeto a los derechos fundamentales, las buenas prácticas informativas fomentan la corresponsabilidad y empoderan a los titulares, quienes, al comprender claramente cómo se maneja su información, pueden actuar con mayor conciencia y vigilancia sobre su propia privacidad, en definitiva, el derecho a ser informados no solo permite conocer el destino de los datos personales, sino que habilita a cada persona a participar activamente en la defensa de su identidad digital y su autodeterminación informativa.

2.1.6 Consentimiento Informado

La Segunda Guerra Mundial se constituyó en una época de grave conmoción a nivel mundial, la historia da cuenta de que en Alemania y otros países ocupados por la legión nazi, se ejecutaron experimentos médicos criminales a gran escala sobre ciudadanos no alemanes, tanto prisioneros de guerra como civiles, incluidos judíos y personas para entonces denominadas asociales, tales experimentos no fueron acciones aisladas o casuales del equipo médico o científico que trabajaba para los nazi, sino que fueron el resultado de la normativa y planteamiento coordinado al más alto nivel del gobierno, del ejército y del partido nazi, practicado como parte del esfuerzo de guerra total.

Con estos antecedentes nace el código de Nuremberg el cual es un conjunto de principios éticos para la experimentación humana que se desarrolló como resultado de los juicios de Nuremberg tras la Segunda Guerra Mundial, se crea para la protección de los sujetos de experimentación médica y asegurar que los experimentos sean éticos e ilegales, el código

establece, entre otros principios, la importancia el consentimiento voluntario y la necesidad de un propósito benéfico para la sociedad, estableciendo al principio como el consentimiento voluntario del sujeto humano es absolutamente esencial, esto quiere decir que la persona afectada deberá tener la capacidad legal para consentir; deberá estar en situación tal que puede ejercer plena libertad de elección sin impedimento alguno de fuerza, fraude, engaño, intimidación, promesa o cualquier otra forma de coacción o amenaza; y deberá tener información y conocimiento suficiente de los elementos del correspondiente experimento y/o tratamiento, de modo que puede entender lo que decida.

El consentimiento informado es esencial dentro de la ética y la bioética, debido a que se basa en el respeto de la autonomía y la dignidad de las personas, asegurando que previo a la toma de decisiones el titular de derecho sea correctamente informado, dentro de muchas ramas profesionales se lo considera en como la expresión práctica del principio de autonomía, en base a ello Beauchamp y Childress definen al principio de autonomía como:

“La obligación de respetar los valores y opciones personales de cada individuo en aquellas decisiones básicas que le atañen vitalmente. Supone incluso el derecho a equivocarse a la hora de hacer uno mismo su propia decisión” (1999).

Entendiendo que, es primordial que exista el respeto sobre la autonomía humana en relación a la decisión que cada persona tome sobre sus acciones y sus derechos, es así que con el consentimiento informado, como un requisito legal, se le otorga la oportunidad ejercer un acto voluntario y consciente al titular del derecho, en función de que se le brinde una información clara y precisa sobre el tipo de procedimiento que se vaya a realizar con la información recolectada, reflejando así la ética dentro del respeto por la dignidad y la libertad de cada persona.

El consentimiento informado se convierte en un pilar fundamental en la protección de los derechos del titular de los datos, ya que la finalidad de esta manifestación es legitimar el tratamiento de los datos personales, como señalan Bedrossian y Fernández (2001), “el consentimiento es un proceso que requiere proporcionar al titular toda la información relevante sobre los fines y alcances del tratamiento, para que pueda decidir de manera consciente”. Por ello el titular de los datos siempre debe estar en busca del equilibrio entre

mantener un ámbito íntimo y no privado de aquellos datos que ser conocido públicamente. En muchas ocasiones el tratamiento de datos va más allá del propósito con el fin de qué se lo recolectó y que por ende el titular no ha dado consentimiento de ello, es por lo que debe existir una relación directa de los datos personales recogidos y la finalidad con la que se la obtuvo, siendo así la finalidad y el consentimiento los pilares fundamentales del contenido esencial dentro de este derecho a la protección de datos, mediante el cual se limita el manejo de ellos y la facultad del titular para decidir acerca de sus datos personales.

Cada persona tiene el derecho de revocar su consentimiento en cualquier momento sin que ello afecte la calidad del servicio académico que reciben, esto refuerza la importancia de que la autorización para el tratamiento de sus datos personales sea realmente libre y sin coacción, en donde se otorgue un periodo adecuado para que el titular reflexione antes de dar su consentimiento, evitando así que este se convierta en un simple trámite.

Finalmente, debe recordarse que el consentimiento no es una exoneración de responsabilidad por parte del responsable del tratamiento. Si no se cumple con el deber de informar de manera adecuada y suficiente, el consentimiento pierde validez. La información debe ser comprensible y ajustarse a las características del titular, para garantizar que comprenda completamente los fines del tratamiento de sus datos. Aun cuando se hable el mismo idioma, es común que surjan malentendidos, por lo que la claridad en la comunicación es fundamental para proteger la voluntad libre e informada del titular.

2.1.7 Obligación de Notificación

La obligación de notificar es un principio fundamental en la protección de datos personales, que garantiza a los titulares la información privada sobre el tratamiento de sus datos, esta obligación se basa en la premisa de que las personas tienen derecho a conocer cómo se están utilizando sus datos, quién los está manejando y para qué fines serán destinados, lo que contribuye a la transparencia y a la confianza en el manejo de la información, esto asegura que los titulares estén informados antes de dar su consentimiento para el tratamiento de sus datos personales.

La notificación debe realizarse en un lenguaje claro y accesible, evitando tecnicismos que puedan dificultar la comprensión del mensaje por parte del titular, de acuerdo con Cañete (2012), "la claridad y la precisión en la información proporcionada son concluyentes para que el consentimiento sea considerado válido y efectivo". Esto implica que la información proporcionada debe incluir detalles sobre la finalidad del tratamiento de los datos personales, especificando el por qué se están recolectando los datos y cómo se utilizarán, es de menester proporcionar la identidad del responsable, es decir, el nombre y la información de contacto del responsable del tratamiento, asegurando que los titulares sepan a quién dirigirse en caso de dudas o preocupaciones.

Dentro de los derechos que tienen los titulares, es fundamental informar sobre el derecho a acceder, rectificar, cancelar y oponerse al tratamiento de sus datos personales, detallar de igual manera los procedimientos que los titulares deben seguir para ejercer sus derechos, incluyendo la forma y los plazos para presentar solicitudes. La obligación de notificación no solo es un deber legal, sino que también es un componente esencial de la ética en el tratamiento de datos. Al informar adecuadamente a los titulares, se fomenta un ambiente de confianza y respeto hacia sus derechos. Como señala Bedrossian (2001), "la información adecuada empodera a los titulares, permitiéndoles tomar decisiones informadas sobre el uso de sus datos".

La notificación a los titulares de los datos es aquel derecho de cada persona a ser informado sobre la manera en que serán procesados sus datos personales, abarcando dentro de los mismo darle a conocer el propósito con el cual es recolectada su información, el tratamiento que se les dará, la persona que será la encargada del manejo de sus datos y tener el pleno conocimiento de sus derechos en base a su información personal. "Una notificación efectiva permite que el titular comprenda su situación y pueda tomar decisiones informadas sobre el tratamiento de sus datos" (Cañete, 2012). Este principio destaca la importancia de la notificación a los titulares de datos personales en el ámbito de la protección de datos, dentro del tratamiento la notificación no solo es un requisito legal, sino que también es esencial para fomentar la transparencia y la confianza entre los responsables del tratamiento y los titulares de los datos.

La comunicación continua y efectiva es vital para fomentar un entorno de confianza y respeto mutuo. Como señala Bedrossian (2001), "la comunicación continua y efectiva es fundamental para fomentar un entorno de confianza y respeto mutuo entre el responsable del tratamiento y titulares". Así, la notificación a los titulares de datos no solo cumple con una obligación legal, sino que también es un elemento clave para garantizar la protección de los derechos de los individuos.

2.1.8 Derechos sobre Contenidos Emitidos, Transmitidos, Retransmitidos y Comunicados Públicamente

La digitalización y el uso intensivo de las tecnologías de la información han transformado las dinámicas de protección de datos personales, especialmente en los derechos sobre contenidos emitidos, transmitidos, retransmitidos y comunicados públicamente, los titulares de los datos tienen el derecho de controlar el uso de su información personal, lo cual implica que cualquier forma de emisión o transmisión de datos que los involucre, ya que se debe contar con su consentimiento explícito, y este debe ser informado, específico y libre de coerción, lo que permite a los titulares comprender cómo se utilizarán sus datos y las discrepancias de su divulgación.

La Comisión Europea (2018) establece que "el consentimiento debe ser otorgado de manera clara, específica y mediante una acción afirmativa que indique la aceptación", lo que resalta la necesidad de un consentimiento activo y plenamente informado. En este sentido, el consentimiento se convierte en el mecanismo de control por parte de los titulares de los datos sobre su información personal, asegurando que cualquier tratamiento o uso de estos sea legítimo y conforme con sus expectativas, es de importancia saber que los responsables del tratamiento de datos proporcionen información clara y accesible sobre el uso que se dará a los contenidos emitidos o comunicados públicamente, esta información debe ser transparente, abarcando el principio de la finalidad del tratamiento, la identidad del responsable y los derechos que asisten a los titulares, no solo facilita el ejercicio de los derechos por parte de los individuos, sino que también fomenta la confianza en las entidades que gestionan la información.

La protección de la imagen y la reputación de las personas sobre sus datos es un componente

esencial dentro de este marco de derechos, la utilización no autorizada de contenidos que involucren a personas puede dar lugar a violaciones de derechos, afectando la dignidad y el honor de los individuos, es necesario que los titulares de los datos cuenten con mecanismos claros para revocar el consentimiento previamente otorgado y exigir la eliminación de contenidos difundidos sin su autorización. En palabras de Paul Bernal:

“la protección de la privacidad y la autonomía digital está íntimamente ligada a la posibilidad de los individuos de controlar sus datos personales y su imagen en la esfera pública” (2017).

Esta cita resalta un aspecto central de la discusión sobre los derechos de los titulares sobre los contenidos emitidos, la privacidad no solo se refiere a la información personal directa, sino también a la proyección pública de los individuos y el control sobre cómo se expone esa información en los medios, la emisión pública de contenido relacionado con una persona, sin su consentimiento, puede tener efectos devastadores en su vida personal y profesional, lo que subraya la importancia de que los derechos sobre esos contenidos sean claros y defendidos por la legislación.

La legislación sobre protección de datos no debe limitarse a regular la recolección y tratamiento de información, sino que debe abordar de manera integral el respeto por los derechos humanos y la dignidad de las personas, esta debe incluir derechos sobre los contenidos emitidos, transmitidos, retransmitidos y comunicados, asegurando que la privacidad de los individuos sea protegida en todas las fases del tratamiento de sus datos. Tal como lo apunta Nissenbaum (2010), “la privacidad, en el contexto de la interconexión digital, no debe ser entendida como la protección de los datos en sí, sino como la capacidad de los individuos para controlar la divulgación y el uso de su información en el espacio público y digital”.

2.1.9 Impacto de la Violación del Principio de Finalidad

El principio de finalidad es uno de los pilares fundamentales en la protección de datos personales, ya que establece que la recolección y el tratamiento de datos deben tener un propósito legítimo, específico y claramente definido. La Ley Orgánica de Protección de Datos Personales de Ecuador, resalta que el tratamiento de datos debe realizarse con base en una finalidad previamente establecida, lo que garantiza que los derechos de los titulares sean

respetados, la violación de este principio puede tener consecuencias tanto para los individuos como para las organizaciones responsables del tratamiento de datos.

Una de las principales consecuencias de la violación del principio de finalidad es la erosión de la confianza del público en las instituciones que manejan datos personales. Cuando los titulares de datos perciben que su información está siendo utilizada para fines no autorizados, su confianza se ve comprometida. Según un estudio de la Comisión Interamericana de Derechos Humanos, "la confianza de los ciudadanos en el uso de sus datos personales es importante para el desarrollo de sociedades democráticas y justas" (CIDH, 2016). Cuando no existe confianza, los individuos pueden optar por restringir el uso de servicios digitales, lo que podría limitar su acceso a beneficios en un mundo cada vez más digitalizado.

Otro impacto es el riesgo de daño a la dignidad y la privacidad de los individuos, la utilización de datos personales para el cual fueron recopilados puede resultar en situaciones de vulnerabilidad o discriminación. Por ejemplo, el uso indebido de información personal en el ámbito laboral puede llevar a prácticas discriminatorias en la contratación o promoción de empleados. Según la Autoridad Nacional de Protección de Datos Personales de España, "la falta de respeto por el principio de finalidad puede tener repercusiones graves en la vida de los afectados, afectando su autonomía" (AEPD, 2020).

Desde una perspectiva legal y organizativa, la violación del principio de finalidad puede acarrear sanciones severas para las instituciones responsables, esto pone de manifiesto la necesidad de que las organizaciones implementen políticas y procedimientos adecuados para asegurar el cumplimiento de este principio.

El impacto de violación en el principio de finalidad trasciende la esfera individual y puede afectar a la reputación de las organizaciones involucradas, las denuncias de mal manejo de datos pueden resultar en pérdida de clientes, deterioro de la imagen corporativa y repercusiones financieras a largo plazo. La Comisión Europea señala que "las organizaciones deben ser proactivas en la gestión de sus obligaciones de protección de datos, para así evitar consecuencias negativas que puedan afectar su desempeño" (Comisión Europea, 2018).

Este enfoque subraya la necesidad de que las empresas no solo cumplan con la normativa de protección de datos por obligación legal, sino como una estrategia esencial para mantener la confianza de los consumidores, un mal manejo de la información puede generar sanciones graves, y la falta de una respuesta proactiva puede llevar a un daño reputacional irreparable, cuyas consecuencias se extienden más allá de la simple multa, afectando la sostenibilidad a largo plazo de cualquier organización.

2.1.10 Abuso de la Información

La utilización indebida de datos personales es un abuso de la información, donde se refiere a las formas que comprometen la privacidad y los derechos de los titulares, este abuso se ha vuelto cada vez más relevante en un entorno digital donde la recolección, el almacenamiento y el procesamiento de datos se realiza a gran escala.

El abuso de la información puede manifestarse de diversas maneras, un ejemplo es la utilización de datos personales con fines diferentes a aquellos para los cuales fueron originalmente recopilados, aquí no solo infringe el principio de finalidad, sino que también puede llevar a situaciones de discriminación, explotación y vulneración de la privacidad de los individuos. La Comisión Interamericana de Derechos Humanos señala que "el uso indebido de datos personales puede resultar en violaciones graves de derechos humanos, afectando la dignidad de las personas" (CIDH, 2016). Este pronunciamiento pone de manifiesto que el abuso de la información no se limita a una simple cuestión administrativa o legal, su impacto se extiende al ámbito de los derechos humanos fundamentales, ya que no solo pone en riesgo la privacidad, sino que también puede facilitar situaciones de exclusión social o incluso persecución en ámbitos políticos o laborales.

El impacto del abuso de la información no se limita a las repercusiones individuales, también puede tener consecuencias significativas para las organizaciones que manejan datos, las violaciones a la normativa de protección de datos pueden resultar en sanciones legales, pérdida de confianza de los consumidores y daño a la reputación corporativa. Según la Autoridad Nacional de Protección de Datos Personales de España, "la falta de cumplimiento con las obligaciones de protección de datos puede acarrear no solo consecuencias financieras,

sino también un deterioro en la imagen y confianza en la organización" (AEPD, 2020). Esta indicación refleja que las infracciones relacionadas con el manejo de datos pueden desencadenar una pérdida de legitimidad en el mercado, afectando la credibilidad de la empresa ante los clientes y socios comerciales que son los titulares de dicha información.

Para mitigar el riesgo de abuso de la información, es fundamental que las organizaciones implementen políticas robustas de protección de datos y fomenten una cultura de transparencia y responsabilidad. Esto incluye la capacitación del personal sobre la importancia de la protección de datos, la implementación de medidas técnicas y organizativas adecuadas, y la promoción de prácticas de tratamiento que respeten los derechos de los titulares, los titulares de datos deben ser empoderados para ejercer sus derechos, incluyendo el derecho a acceder, rectificar y eliminar la información personal.

Antes de profundizar en los distintos tipos de abuso de la información, es importante reconocer que la violación de los derechos de los titulares puede manifestarse de múltiples formas, a continuación, se presenta una tabla que detalla los principales tipos de abuso de la información, con el objetivo de ilustrar su impacto y frecuencia en el tratamiento de datos.

GRÁFICO 2
TIPOS DE ABUSO DE LA INFORMACIÓN

TIPOS DE ABUSOS	DESCRIPCIÓN	PORCENTAJE ESTIMADO
Uso no autorizado de datos	Venta o tratamiento de información sin el consentimiento	30%
Discriminación basada en datos personales	Negación de servicios o trato desigual por información	25%
Explotación comercial	Uso de datos para marketing agresivo o engañoso	20%
Violaciones a la privacidad	Monitoreo o recopilación de datos sin consentimiento	15%
Otras violaciones	Filtraciones de datos o mal uso de información	10%

Elaborado por: Nathaly Torres y Carlos Vera

Fuente: José Martínez Vilchis

La tabla anterior ilustra como el abuso de la información puede presentarse en diversas formas, afectando directamente los derechos de los titulares y el cumplimiento del principio de finalidad en el tratamiento de datos personales. Cada tipo de abuso descrito plantea una amenaza a la confianza pública en las instituciones que manejan esta información, es fundamental que las organizaciones implementen mecanismos de control y supervisión que aseguren que los datos sean utilizados exclusivamente para los fines previstos por los titulares, dentro de la creciente digitalización de los procesos y servicios hace aún más relevante este enfoque preventivo, dado que un mal manejo de la información puede acarrear sanciones legales, pérdida de reputación y, lo más crítico, el detrimento de los derechos fundamentales de las personas.

2.1.11 Gestión de los Datos Personales en el Sistema Educativo Ecuatoriano

El derecho a la educación se encuentra consagrado en el artículo 26 de la Constitución de la República del Ecuador, el cual establece que el acceso a la educación es un derecho humano fundamental, no obstante, gracias a la transformación digital este derecho implica el manejo constante de los datos personales, ya que el progreso tecnológico y la adaptación de nuevas modalidades educativas requieren del tratamiento especializado cuando se trata de información sensible, por otra parte, el sistema educativo nacional, independientemente de cualquier tipo de nivel educativo, incluye dentro de sus políticas la promoción de la educación digital, este enfoque no sólo favorece los estudiantes, brindándoles herramientas para el desarrollo académico dentro de esta nueva era digital, sino también a los docentes, los cuales deben informarse de estas nuevas tecnologías como parte de su formación profesional; es importante mencionar que los datos personales manejados en estas plataformas incluyen información clave que permite identificar a cada individuo, información que se constituye: en nombres, apellidos, dirección, número de teléfono y correo electrónicos. Por ello es menester que las instituciones educativas mantengan un registro adecuado y detallado de todas las actividades relacionadas con el tratamiento de datos personales, esto implica que cada institución debe desarrollar y documentar protocolos que reflejen claramente qué tipo de datos están recolectando, con qué propósito y bajo qué justificación se solicita dicha información sensible, dichos protocolos deben incluir los

formularios del consentimiento de los estudiantes, describiendo el uso que se le dará a estos datos y las entidades o proveedores externos a los que se les puede delegar su tratamiento. Además, es primordial asegurar que estos datos se publiquen de manera adecuada y que se garantice su confidencialidad a través de un sistema de seguridad, todas estas prácticas son parte de la responsabilidad proactiva que es la sumir en cada institución educativa, asegurando así el correcto tratamiento de los datos personales de sus estudiantes.

Es crucial que se identifique y se estacionen los riesgos relacionados con la pérdida, distribución o alteración de los datos personales, así como el acceso no autorizado a esta información, no sólo dentro de las instituciones educativas sino dentro de toda empresa que maneje este tipo de información sensible, debido a que si no se implementan estas medidas de prevención y monitoreo se estaría vulnerando la protección de datos sensibles, exponiendo a los estudiantes y a la comunidad educativa a situaciones en las que terceros podrían acceder y manipular su información, creando así escenarios de vulnerabilidad, por lo que es imprescindible que las instituciones mantengan un control constante sobre el manejo de los datos personales, en los últimos años, el sistema educativo ha sido uno de los sectores más impactados por los constantes cambios tecnológicos y sociales, esta afectación ha sido notable debido a la necesidad de uso constante de herramientas tecnológicas, plataformas digitales y sistemas de educación que permitan mantener en marcha las actividades institucionales.

En el ámbito de la educación superior, la constitución del 2008 consagra la autonomía universitaria, la que implica también una mayor responsabilidad en base a la gestión y uso de los datos sensibles, debido a ello se genera una necesidad mayor de gobernanza para la gestión de información y una mejora en la calidad de la educación. Con estos antecedentes nace La Ley de la Educación Superior del 2010 sentando los principios y bases legales para ejercitar el derecho para la educación superior, incluyendo la participación de diversos actores dentro de la toma decisiones, además de la creación de la Secretaría de Educación Superior, Ciencias, Tecnología e Innovación en el año 2011, siendo este último un punto de inflexión en la forma en que se gestiona los datos en estas instituciones.

Dentro del caso de las instituciones de educación superior en Ecuador, la gobernanza de datos implica establecer estructuras organizativas específicas, como la figura del delegado de protección de datos, este rol es fundamental para supervisar que las políticas internas estén alineadas con la Ley Orgánica de Protección de Datos Personales y que las prácticas diarias cumplan con los estándares de seguridad y privacidad requeridos, aquí el delegado actúa como un enlace entre la institución, los titulares de datos y las autoridades reguladoras, promoviendo una cultura de cumplimiento y transparencia.

La gobernanza de datos está dirigida a la gestión y recopilación de datos para las instituciones de educación superior, en donde se gestionan grandes cantidades de datos de diversas fuentes, como registros estudiantiles, investigación del profesorado y sistemas administrativos, la implementación de políticas y mejores prácticas para la gobernanza de datos ayuda a garantizar la consistencia, la precisión y seguridad de los datos sensibles. Tal como lo menciona en una entrevista con Masanalytics, el especialista en gobierno de datos en el sector de la educación, Sergio Bocaz:

“La gobernanza de datos no sólo garantiza la integridad, disponibilidad y seguridad de los datos en el ambiente educativo, también permite las instituciones maximizar su valor al facilitar la toma de decisiones informadas con alta calidad, innovar en las enseñanzas y adaptarse a las demandas y tendencias actuales” (2024).

La gobernanza de datos en el entorno universitario va más allá de cumplir con los requisitos legales, representa una oportunidad para optimizar la gestión de la información y fortalecer la confianza institucional, este concepto abarca la implementación de políticas, la asignación de responsabilidades y la utilización de tecnologías seguras que permitan un manejo eficiente de los datos personales, en un ámbito donde los datos se han convertido en un recurso estratégico, aquí la gobernanza adecuada contribuye al cumplimiento de los objetivos académicos y administrativos.

El uso de herramientas tecnológicas avanzadas para garantizar la seguridad de la información, incluyen la implementación de sistemas de encriptación, controles de acceso y auditorías periódicas que permitan identificar y mitigar riesgos potenciales, en el ámbito educativo, donde los datos personales pueden incluir información académica, financiera y de salud, estas medidas son esenciales para prevenir filtraciones o accesos no autorizados que

puedan comprometer la privacidad de los estudiantes.

La seguridad de los datos personales es un principio esencial en la recolección de datos personales en las instituciones de educación superior, debido a que busca proteger la información contra accesos no autorizados, pérdida, alteración o destrucción, este principio adquiere especial relevancia debido al manejo de grandes volúmenes de información sensible de estudiantes, docentes y personal administrativo, los datos académicos, financieros y de salud son los más vulnerables, y cualquier brecha en la seguridad puede tener consecuencias graves tanto para los titulares como para la institución, por ello, es imprescindible implementar medidas que garanticen su confidencialidad.

El codificar datos es otra medida clave para garantizar la seguridad en el ámbito universitario, este proceso permite que los datos se almacenen y transmitan en un formato accesible únicamente mediante claves específicas, de esta manera, incluso si la información es interceptada, no puede ser comprendida ni utilizada sin la clave correspondiente, es especialmente relevante en la transmisión de datos a través de plataformas digitales, como sistemas de gestión académica o correos electrónicos institucionales, las auditorías regulares son fundamentales para identificar y corregir vulnerabilidades en los sistemas de seguridad.

La capacitación del personal es un pilar indispensable en la estrategia de seguridad de datos, los empleados que manejan información personal deben estar conscientes de las implicaciones legales y éticas de sus acciones, así como de los procedimientos adecuados para garantizar la seguridad de los datos, esto incluye reconocer amenazas comunes, como el phishing o el acceso no autorizado, y actuar de manera proactiva para prevenir incidentes, una fuerza laboral bien capacitada es clave para mitigar riesgos y fomentar una cultura de privacidad y seguridad, tomando en cuenta uso creciente de plataformas digitales en el ámbito educativo planteando nuevos retos en cuanto a la seguridad de los datos.

Las universidades que adoptan herramientas tecnológicas deben asegurarse de que estas cumplen con los estándares de seguridad y protección de datos, esto implica realizar evaluaciones de impacto previas, firmar acuerdos claros con los proveedores tecnológicos y supervisar continuamente el funcionamiento de estas plataformas para prevenir

vulneraciones, la seguridad de la información ve el diseño de los procesos y sistemas, y dentro de las universidades no solo protegen a sus estudiantes y empleados, sino que también refuerzan su reputación como instituciones confiables, éticas y comprometidas con la protección de derechos fundamentales.

Los estudiantes toman un rol importante dentro de la recolección de información, como titulares de sus datos personales, contando con derechos fundamentales que buscan proteger la integridad de su información y garantizar que esta sea tratada de manera adecuada siendo reconocida por la constitución del 2008, como un derecho humano fundamental, sentando sus principios y fines generales en la Ley Orgánica de Educación Intercultural, así como también se reconocen sus deberes y derechos en la Ley Orgánica de Educación Superior,

Por ello el derecho a la información es uno de los pilares fundamentales en la protección de los datos personales, debido a que desprende los derechos a los cuales los estudiantes tienen potestad de elegir qué hacer con su información, siendo el principal el derecho a la acceso de los datos, ya que les permite conocer qué información se ha recopilado, quien la utiliza y el por qué se ha recolectado, junto a este, el derecho de rectificación le da la posibilidad de corregir datos inexactos o desactualizados, garantizando así la calidad de la información evitando cualquier tipo de problemas que puedan suscitarse. El derecho de cancelación o supresión permite solicitar la eliminación de los datos cuando ya no sean necesarios o cuando su tratamiento no cumple con la normativa vigente, por su parte, el derecho a la portabilidad facilita que los estudiantes obtengan una copia de sus datos dentro de un formato estructurado, lo que les permite trasladarlos a otras instituciones, asimismo, el derecho de oposición les brinda la facultad de poder rechazar el tratamiento de sus datos por motivos legítimos, especialmente si el titular considera que se está afectando su privacidad, finalmente el derecho a la limitación del tratamiento ofrece una protección adicional al permitir que se restrinja cualquier tipo de uso de los datos que se hayan recolectados dentro de determinados circunstancias, como cuando se cuestiona su exactitud o legalidad, así que todos estos derechos son componentes esenciales los cuales permiten que exista una correcta gestión basada en la responsabilidad, transparencia y el respeto de toda la información personal que se ha recolectado dentro del ámbito educativo.

2.1.12 Universidad Estatal Península de Santa Elena

Dentro de la provincia de Santa Elena con el paso de los años a través de varias instituciones y de los ciudadanos peninsulares, realizó una serie de acciones y actividades para conseguir el funcionamiento de un centro de educación superior en Santa Elena.

Desde 1984 a 1994 las municipalidades de Salinas, Santa Elena y diversas instituciones cívicas realizaron gestiones en procura de institucionalizar la Educación Superior dentro de la Península de Santa Elena, consiguiendo así un funcionamiento de la extensión de la Universidad de Guayaquil, pero solo en áreas específicas, como la de Ingeniería Industrial, Filosofía y Letras, Ingeniería Comercial e Idiomas; en agosto de 1997 con la Junta Cívica de Salinas mediante la Asamblea Peninsular Interinstitucional con la participación de la Junta Cívica de La Libertad, Santa Elena y más instituciones peninsulares, resolviéndose, insistir en el trámite de creación de la Universidad del Pacífico y volver a presentar el proyecto de ley que fuera vetado un año antes. El 6 de noviembre de 1997 se presenta nuevamente el proyecto, siendo aprobado por el congreso nacional el 1 y 2 de julio de 1998, con algunas reformas tales como la disminución de facultades académicas, participación de la Universidad de Guayaquil en la organización inicial de la universidad creada y lo más sobresaliente el cambio de nombre que contaba en el proyecto original como Universidad del Pacífico en la Península de Santa Elena, por el de Universidad Estatal Península de Santa Elena, es así que finalmente el 17 de julio de 1998, el Dr. Fabián Alarcón presidente interino de la República del Ecuador firma el ejecútese de la ley No. 110 y que se promulga en el suplemento del registro oficial #366 del 22 de julio de 1998, se convirtiéndose así en el pilar fundamental para el desarrollo académico y social de la región. Actualmente la Universidad estatal península de Santa Elena, conocida por su acrónimo UPSE, es una universidad pública localizada en el cantón de la libertad, provincia de Santa Elena, se encuentra acreditada dentro del sistema de educación superior, ubicándose en la categoría C, de acuerdo a la evaluación realizada por el consejo de evaluación, acreditación y aseguramiento de la calidad de la educación superior.

Como toda universidad, la UPSE contaba con su sistema educativo presencial, pero dentro de su modelo educativo del 2015, aprobado por el Honorable Consejo Superior Universitario,

mediante resolución RCS-SO-0311-2014 el 18 de diciembre del 2014, establece que como consecuencia del desarrollo inesperado del conocimiento científico y tecnológico, así como del papel determinante de la electrónica asigna un valor económico al conocimiento, diferente al que tuvo en los siglos anteriores, entendiendo de esa manera el avance exponencial de las tecnologías dentro de los sistemas educativos, resaltando la importancia para su implementación dentro del modelo educativo que se imparte dentro de la institución, si bien hasta ese momento la tecnología solo se enfocaba mayormente en el ámbito administrativo ya se evidencia un cambio radical en la estructura de la educación superior, sin embargo, es en el año del 2020 donde comienza la era digital a nivel global, debido a la pandemia del COVID-19 y el confinamiento, tanto empresas como instituciones se vieron obligadas a revolucionar sus sistemas operacionales, en el ámbito de cómo se iba a impartir la educación, así como también de qué manera se iba a realizar el trabajo que por años había mantenido una estructura sólida y mecanizada, es ahí donde surge la tecnología como una medida viable en respuesta a la problemática que azotaba al mundo, surgiendo métodos como el teletrabajo, las clases en línea y la recaudación de los datos personales de cada persona que ingresaban estudiar a la universidad, si bien al inicio no fue fácil adaptarse este nuevo método de trabajo, enseñanza y gestión de información, con el paso de los años se ha ido perfeccionando, observando que, mantuvo su funcionamiento mientras duró el confinamiento, sino que se lo adaptó hasta el punto que se volvió imprescindible para el sistema educativo dentro del universidad para el tratamiento de la información que se maneje.

En el ámbito de la educación superior se logran identificar las 4 funciones principales en la UPSE, siendo éstas, la docencia que va enfocada a la formación académica y profesional de sus estudiantes, mediante programas de pregrado, posgrado y educación continua, la investigación, tanto científica y tecnológica, que permita generar conocimientos y soluciones a problemas que surjan dentro de la sociedad, vinculación con la sociedad en donde se compromete a la interacción directa con la comunidad, con el objetivo de obtener un beneficio mutuo y el desarrollo social dentro de la provincia y por último la gestión, que se enfoca más en la administración de sus recursos y la realización de actividades eficientes y transparentes para garantizar el buen funcionamiento de la institución educativa,

determinando que si estas funciones se logran entrelazar de una manera adecuada permitirán así la formación integral de los estudiantes y el desarrollo de la comunidad.

Ante la emergencia mundial del COVID-19 y dando con el cumplimiento de las medidas de bioseguridad, la UPSE se vio obligada a cambiar la modalidad presencial por la virtual, involucrando el uso de las tecnologías a tiempo completo dentro de la educación, mediante la rendición de cuentas realizada en el año 2020, el total de estudiantes de pregrado que lograron matricularse fue de 7494, aun así, con una nueva modalidad en marcha.

En el ámbito de la titulación, en dicho periodo, la Universidad Estatal Península de Santa Elena, contó con un total de 1130 graduados, de los cuales el 74,1% obtuvieron su título mediante Examen de Grado o de fin de Carrera de Carácter Complexivo, el 21,77% con Proyectos de Investigación y el 4,14% restantes con Análisis de casos, Proyectos Integradores, Propuestas Tecnológicas y Tesis de Grado, entendiendo que a lo largo de sus 26 años de historia ha tenido un número significativo de graduados, sin embargo desde el 2021 hasta la fecha, la oferta de grado de la UPSE pasó de 18 a 34 carreras y sus programa de maestrías crecieron de 16 a 26, junto con una comunidad actual que oscila entre más de 20.000 estudiantes en modalidad presencial, híbrida y en línea. Asimismo, los profesores investigadores han tenido que adaptar sus actividades académicas a las restricciones provocadas por la pandemia del COVID-19, esto en base a las formas en las que realizan la investigación, su recolección, el análisis, el diseño y la forma en la que se comunicará científicamente los proyectos que vayan a realizar.

A raíz del 2020, los proyectos de investigación tributan a los siguientes dominios académico: 47% recursos naturales, producción y ambiente, el 42% al desarrollo económico, productivo, educación, comunicación, cultura y sociedad ingeniería, 11% de tecnología, infraestructura y sistemas constructivos, pero dentro de este tópico también se debe resaltar la importancia de la protección de datos de los maestrantes, debido a que ellos son la fuente que genera y busca información por parte de la institución educativa, esto también siendo fundamental ya que con la avance exponencial de la universidad a raíz de sus convenios internacionales, dichos datos sensibles se encuentran más cerca de ser vulnerados en caso de existir una mala

gestión y tratamiento. La recolección de datos no sólo se encuentra enfocada dentro de la universidad, debido a que gracias a la vinculación con la sociedad, los estudiantes, si bien realizan un trabajo más íntegro con distintos sectores dentro de la provincia, las actividades que los mismos desarrollan están dirigidas al fortalecimiento de un entorno integral dentro de toda la provincia, y que para su realización muchas veces recurren a la recolección de datos, lo cual muchas veces las personas que otorgan su información no son conscientes de lo que están realizando, es por ello que tanto dentro de la institución educativa, como en sus actividades extracurriculares, que son primordiales según sus funciones, es necesario que se otorgue un consentimiento informado, sobre el objetivo por el cual se recolecta dicha información sensible, es por ellos que se logra evidenciar que la UPSE en los últimos años ha tenido un crecimiento significativo, pero dicha evolución no solo se logra observar en la cantidad de estudiantes que alberga, sino en su propuesta académica, infraestructura y proyección a futuro, en la misma medida crecen las necesidades de ampliar las seguridades, protocolos y un marco normativo interno que brinde garantías en la gestión de datos.

2.2 Marco Legal

Constitución de la Republica del Ecuador

La Constitución del 2008 en el Ecuador se le establece como la norma jurídica de mayor jerarquía dentro del ordenamiento jurídico ecuatoriano, de tal manera que esta supremacía obliga a todas las nuevas normas infra constitucionales a que sean rectas en concordancia los derechos y garantías establecidas en el texto constitucional, denominándola también como garantista dentro de la tendencia neoconstitucionalista, cambiando el modelo estatal de estado social ha estado constitucional de derechos y justicia, en ella también se establecen los derechos y deberes de los ecuatorianos, la organización del Estado y los valores que orientan la vida en el país, en ella se incorpora a los principios del buen vivir, los cuales promueven el bienestar colectivo de la sociedad en armonía con la naturaleza.

A continuación, se detallan los artículos de la Constitución del Ecuador que son vinculantes al tema:

TÍTULO II

Principios de aplicación de los derechos

Art. 11.- el ejercicio de los derechos se regirá por los siguientes principios:

1. Los derechos se podrán ejercer, promover y exigir de forma individual o colectiva ante las autoridades competentes; esta autoridad garantizará su cumplimiento.
2. Todas las personas son iguales y gozarán de los mismos derechos, deberes y oportunidades.
3. Los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos serán de directa e inmediata aplicación y por y ante cualquier servidora o servidor público, administrativo o judicial, de oficio o a petición de parte
4. Ninguna norma jurídica podrá restringir el contenido de los derechos ni de las garantías constitucionales
5. En materia de derechos y garantías constitucionales, las servidoras y servidores públicos administrativos o judiciales, deberán aplicar la norma y la interpretación que más favorezca su efectiva vigencia
6. Todos los principios de los derechos son inalienables, irrenunciables, indivisibles, interdependientes y de igual jerarquía
7. El reconocimiento de los derechos y garantías establecidas en la Constitución y en los instrumentos internacionales de derechos humanos, no excluir a los demás derechos derivados de la dignidad de las personas, comunidades, pueblos y nacionalidades, que sean necesarios para su pleno desenvolvimiento
8. El contenido de los derechos se desarrollará de manera progresiva a través de las normas, la jurisprudencia y las políticas públicas. El Estado generará y garantizará las condiciones necesarias para su pleno reconocimiento y ejercicio
9. El más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en la Constitución

Dentro de este articulado se establece el reconocimiento de todos los derechos inherentes de cada persona, constatando que será deber y obligación del Estado que todos estos derechos mencionados no se vean vulnerados de ninguna manera, respetando también todos los precedentes internacionales que desembocaron la creación y protección de estos derechos, es decir qué se busca una sociedad en donde se respete a cada miembro que la conforma evitando cualquier tipo de discriminación y así de esa manera buscar un orden público bajo el respeto de los derechos de cada persona.

Se reconoce explícitamente la importancia de la protección de datos personales como un derecho fundamental, estableciendo que el Estado debe mantener la confidencialidad de los datos personales que se encuentran en los archivos de cada institución que esté en el país, esto implica que ninguna entidad pública o privada puede hacer uso de la información

personal sin contar con el consentimiento expreso de su titular, esta disposición fortalece la autonomía individual y garantiza que el manejo de los datos se realice conforme a principios de transparencia y legalidad.

CAPÍTULO SEXTO

Derechos de libertad

Art. 66.- Se reconoce y garantizará a las personas:

19) 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.

El artículo destaca la importancia del consentimiento informado como una herramienta esencial para el respeto de los derechos de los ciudadanos, sin embargo, en la práctica, pueden existir desafíos en la implementación de este principio, especialmente en contextos donde las personas no tienen acceso suficiente a información clara sobre el tratamiento de sus datos.

Establece el derecho de todas las personas a la protección de sus datos personales, lo que incluye el acceso y la decisión sobre su información, así como su correspondiente protección. Para garantizar este derecho, la norma exige que la recolección, archivo, procesamiento y difusión de datos personales requieran la autorización del titular o el mandato de la ley, este principio está alineado con el concepto de consentimiento informado, el cual permite a los ciudadanos decidir sobre el uso de su información y refuerza su privacidad y autonomía.

Declaración Universal de los Derechos Humanos

La declaración universal de los derechos humanos tiene su génesis en el año 1948, fue promulgada el 10 de diciembre por la Asamblea General de las Naciones Unidas en París, esta declaración se la precisa como un documento el cual marca un hito histórico de los derechos humanos, elaborado por representantes de todas las regiones del mundo con diferentes antecedentes jurídicos y culturales, con un ideal común para todos los pueblos y naciones, sentada bajo las bases del texto de la declaración de derechos del hombre y del ciudadano del año 1789, y de las experiencias vividas en la Segunda Guerra Mundial.

La declaración universal de los derechos humanos (DUDH) es una respuesta a todos los

conflictos que se suscitaron en dicha época, en el ámbito sociales, políticos e internacionales de interés propio, siendo este último uno de los más relevantes debido a todo lo suscitado en la Segunda Guerra Mundial, hecho histórico el cual se evidenciaba como se violaban masivamente los derechos humanos, por lo que surge la necesidad de que exista un órgano normativo que vele por la protección de los derechos de las personas, naciendo de esa manera un nuevo orden mundial denominada como Organización de las Naciones Unidas (ONU), con ello los líderes del mundo decidieron complementar la carta de las Naciones Unidas con una hoja de ruta para que otorgándole la responsabilidad de salvaguardar y garantizar los derechos de cada ser humano en cualquier lugar y en todo momento; además de que con su creación se reconoce que todas las personas nacen libres e iguales en dignidad y derechos, describiendo los derechos y libertades esenciales e inherentes de cada persona como el derecho a la vida, la libertad, la educación y la cultura, estas normas se encuentran fundamentadas internacionalmente en función a que se respete a los derechos humanos, inspirando el trabajo para garantizar que todas las personas pueden tener libertad, igualdad y dignidad, volviéndose esencial para que vivamos en una sociedad justa, equitativa, tolerante y respetuosa ante los derechos que representan la dignidad humana.

A continuación, se detalla el artículo de la Declaración Universal de los Derechos Humanos, que es vinculante al tema.

LA ASAMBLEA GENERAL

Art. 12.- nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tal es injerencias o ataques.

El presente articulado establece que ninguna persona será objeto de violación a su vida privada, otorgándole la posibilidad de tener una vía legal para que se respete el derecho a su información, asimismo evitando ataques contra su honra y su reputación, enfatizando el recepto a la privacidad de las personas en sus vidas, es decir que la persona tiene total libertad sobre la decisión de lo que quiera mantener privado o público en base a su vida o información que considere importante, delimitando así una barrera entre dichos ámbitos, a la que ninguna persona tendrá la posibilidad de tener acceso mediante injerencia a dicha información de carácter confidencial. Es así que, este articulado busca que se respete la autonomía y vida

digna de la persona en relación a cualquier tipo de información que sea de índole personal del titular del derecho, evitando que exista algún tipo de violencia psicológica o física que busque dañar tanto a la persona como a su familia, teniendo su enfoque en salvaguardar la integridad personal y el derecho de la vida privada de cada individuo.

Pacto Internacional de Derechos Civiles y Políticos

Entrando en vigor el 23 de marzo de 1976, sí llegó a considerar que, conforme a los principios que se enmarcan dentro de la carta de las Naciones Unidas, en donde la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad inherente a todos los miembros de la familia humana y sus derechos iguales e inalienables, reconociendo de esa manera que estos derechos se derivan de la dignidad inherente de cada persona, por lo que se reconoce que, con el arreglo de la declaración universal de los derechos humanos, no se puede realizar el ideal del ser humano libre en el disfrute de las libertades civiles y políticas, A menos de qué se creen condiciones que permitan a cada persona gozar de dichos derechos Y además en sus derechos económicos, sociales y culturales.

Es por ello que la carta de las Naciones Unidas impone a los estados la obligación de promover el respeto universal y efectivo de los derechos y libertades humanas, comprendiendo así que el individuo, por tener deberes respecto de otros individuos y de la comunidad a quien pertenece, tiene la obligación de esforzarse por la consecución y la observancia de los derechos reconocidos dentro de este pacto.

A continuación, se detallan los artículos del Pacto Internacional de Derechos Civiles y Políticos, que son vinculantes al tema.

Parte III

Art. 17.

- 1.- Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación
- 2.- Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques

Este articulado dentro de sus numeral 1, rectifica la protección de la vida privada del titular

del derecho, relacionando también a cualquier tipo de injerencia arbitraria que busque dañar a su familia, domicilio o su correspondencia de manera ilegal e injustificada, en base a cualquier tipo de delito que atente contra la vida privada del individuo, en concordancia, dentro del numeral 2 se estipula que existe un mecanismo legal ante cualquier acción que violente este derecho, buscando de esa manera salvaguardar el derecho a la integridad personal de cada ser humano, es así que toda acto que sobrepase los límites impuestos en relación a lo que el titular del derecho considere como su vida pública o privada constará con una protección legal ante cualquier tipo de hechos que traten de vulnerar la integridad personal de cada individuo.

Parte III

Art. 19.

2.- Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir información e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

Dentro de este articulado se establece que toda persona es libre de expresarse ante cualquier tipo de hecho sobre el cual busque opinar, otorgando así la libertad de poder realizarlo de distintas maneras, es primordial destacar que todas las opiniones deberán de respetarse y las personas que las emitan no deberán ser juzgados por las mismas, es menester resaltar que, cada opinión se deberá realizar bajo el respeto, la prudencia y de conformidad a como se lo manifieste en la ley, evitando cualquier tipo de discriminación, falacias, calumnias u otro tipo de opiniones que busquen dañar u ofender a otras personas, buscando de esa manera que exista una sociedad libre regida bajo el respeto y el orden.

Ley Orgánica de Protección de Datos Personales del Ecuador

La Ley Orgánica de Protección de Datos Personales (LOPDP) fue promulgada en el año 2021 con el fin de regular el tratamiento de la información personal y establecer garantías que eviten su uso indebido. Su creación fue impulsada, entre otros factores, por la filtración masiva de datos en 2019 que puso en riesgo la privacidad de millones de ecuatorianos.

La norma impone una responsabilidad directa a los responsables del tratamiento de datos

para que demuestren que el consentimiento fue obtenido de manera adecuada. Esta medida es esencial para evitar prácticas abusivas y garantizar que la recolección de datos se realice conforme a la normativa vigente.

A pesar de estas disposiciones, persiste el desafío de asegurar su correcta aplicación. Muchas organizaciones aún carecen de mecanismos adecuados para documentar el consentimiento, lo que puede generar conflictos en la protección de datos. Es crucial que las entidades encargadas del cumplimiento de la normativa supervisen de manera efectiva estas prácticas y promuevan una cultura de protección de datos en todos los sectores.

CAPÍTULO I

Generalidades

Art. 5.- De la recogida del consentimiento. - El responsable de datos personales deberá obtener el consentimiento del titular de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales.

En todos los casos en los que de conformidad con la Ley se requiera el consentimiento explícito del titular para el tratamiento de sus datos, el responsable deberá informar previa y detalladamente los tipos de tratamiento, finalidades, el tiempo de conservación, las medidas de protección a adoptarse, las consecuencias de su entrega, entre otros aspectos determinados en la Ley, lo cual deberá ser consentido inequívocamente por el titular.

El consentimiento del titular deberá reflejar de manera indubitada la aceptación de éste en relación con el tratamiento de LEXIS S.A. sus datos personales a través de una declaración, pronunciamiento para darse de baja o clara acción afirmativa. El consentimiento otorgado por el titular deberá ser demostrado por el responsable que lo obtiene, cuando así sea requerido por la autoridad competente.

Cuando los datos personales recogidos pertenecen a un incapaz, bastará con el consentimiento del representante legal debidamente acreditado ante el responsable, en los términos señalados en el presente artículo. El consentimiento de niñas, niños y adolescentes y, en general, de personas incapaces, se obtendrá a través de sus representantes legales y curadores, según lo dispuesto en la Ley Orgánica de Protección de Datos Personales y el Código Civil.

El silencio o la inacción, por sí solos, no presumen el consentimiento del titular.

Dentro de este articulado del reglamento establece que el consentimiento para el tratamiento de datos personales debe obtenerse de manera explícita e informada. La información proporcionada al titular debe incluir detalles sobre el tipo de tratamiento, su finalidad, el tiempo de conservación, las medidas de protección adoptadas y las consecuencias de la entrega de datos. El consentimiento también debe reflejarse a través de una acción afirmativa clara, y el responsable del tratamiento debe ser capaz de demostrar su obtención en caso de

requerimiento por parte de la autoridad.

El derecho a revocar el consentimiento es otro elemento clave dentro de este marco normativo, esto significa que los ciudadanos pueden retirar su autorización en cualquier momento sin que ello afecte la legalidad del tratamiento previo. Este mecanismo refuerza la autodeterminación informativa y protege a los titulares de situaciones donde su información podría ser utilizada en contra de su voluntad.

Sin embargo, en la práctica, el cumplimiento de esta norma puede enfrentar desafíos debido a la falta de conocimiento del ciudadano sobre sus derechos y a la resistencia de algunas instituciones a implementar mecanismos de revocación efectivos y accesibles. Es fundamental que se fortalezcan los procesos de educación y sensibilización sobre la importancia del consentimiento informado.

CAPÍTULO I

Ámbito De Aplicación Integral

Art. 8.-Consentimiento. -Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo. El consentimiento será válido, cuando la manifestación de la voluntad sea:

- 1) Libre, es decir, cuando se encuentre exenta de vicios del consentimiento;
- 2) Específica, en cuanto a la determinación concreta de los medios y fines del tratamiento;
- 3) Informada, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia,
- 4) Inequívoca, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular.

El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación, para lo cual el responsable del tratamiento de datos personales establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento sencillo, similar al proceder con el cual recabó el consentimiento.

El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos.

Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste que dicho consentimiento se otorga para todas ellas.

El articulado plantea que el tratamiento de datos personales solo podrá realizarse bajo el consentimiento del titular, este consentimiento debe cumplir con cuatro requisitos fundamentales: debe ser libre (sin presión o vicios del consentimiento), específico

(definiendo claramente los propósitos del tratamiento), informado (con plena transparencia sobre el uso de los datos) e inequívoco (sin ambigüedades sobre la voluntad del titular). Además, la norma permite la revocación del consentimiento en cualquier momento, garantizando que el usuario mantenga el control sobre su información.

CAPÍTULO II

Principios

Art. 10.-Principios. - Sin perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras son jurídicas, la presente ley se regirá por los principios de:

- a) Juridicidad.-Los datos personales deben tratarse con estricto apego y cumplimiento de los principios, derechos y obligaciones establecidos en la Constitución, los instrumentos internacionales, la presente ley, su reglamento y las demás normativas y jurisprudencia aplicable.
- b) Lealtad.-El tratamiento de datos personales deberá ser leal, por lo que para los titulares debe quedar claro que se están recogiendo, Utilizando, consultando o tratando de otra manera, datos personales que le conciernen, así como a las formas que en dichos datos son o serán tratados.
- c) 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.
- d) Finalidad.-Las finalidades del tratamiento deberán ser determinadas, explícitas, legítimas y comunicadas al titular: no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley.
- e) Pertinencia y minimización de datos personales.-Los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento.
- f) Proporcionalidad del tratamiento.-El tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo con relación a las finalidades para las cuales hayan sido recogidos o a la naturaleza misma, de las categorías especiales de datos.
- g) 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.
- h) Calidad y exactitud.-Los datos personales que sean objeto de tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros; y, de ser el caso, debidamente actualizados; de tal forma que no se altere su veracidad. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

En caso de tratamiento por parte de un encargado, la calidad y exactitud será obligación del responsable del tratamiento de datos personales.

Siempre que el responsable del tratamiento haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, no le será imputable la inexactitud de los datos personales,

con respecto a los fines para los que se tratan, cuando los datos inexactos:

- a) Hubiesen sido obtenidos por el responsable directamente del titular.
- b) Hubiesen sido obtenidos por el responsable de un intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario que recoja en nombre propio los datos de los afectados para su transmisión al responsable.
- c) Fuesen obtenidos de un registro público por el responsable.
- i) Conservación.-Los datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento.
- j) Seguridad de datos personales.-Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole, para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto.
- k) Responsabilidad proactiva y demostrada.-El responsable del tratamiento de datos personales deberá acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la presente Ley, para lo cual, además de lo establecido en la normativa aplicable, podrá valerse de estándares, mejores prácticas, esquemas de auto y coregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento.
- l) Aplicación favorable al titular.-En caso de duda sobre el alcance de las disposiciones del ordenamiento jurídico o contractuales, aplicables a la protección de datos personales, los funcionarios judiciales y administrativos las interpretarán y aplicarán en el sentido más favorable al titular de dichos datos.
- m) Independencia del control.-Para el efectivo ejercicio del derecho a la protección de datos personales, y en cumplimiento de las obligaciones de protección de los derechos que tiene el Estado, la Autoridad de Protección de Datos deberá ejercer un control independiente, imparcial y autónomo, así como llevar a cabo las respectivas acciones de prevención, investigación y sanción.

En el presente artículo se establecen principios que buscan garantizar un tratamiento de datos personales lícito, seguro y respetuoso de los derechos fundamentales del titular, priorizando su autodeterminación informativa. asimismo, se asegura que los datos se utilicen únicamente para fines legítimos y previamente autorizados, imponiendo obligaciones al responsable mediante los principios de proporcionalidad, pertenencia y minimización, con el fin de evitar excesos en la recolección y tratamiento de dicha información sensible.

Ley Orgánica de Educación Superior

La ley Orgánica de Educación Superior, en adelante LOES, es aquella ley que se encarga de garantizar el derecho a la educación superior de buena calidad y promover la excelencia de la misma, expedida el 12 de octubre de 2010. Esta ley también regula los principios y el

funcionamiento de las diferentes instituciones que conforman el sistema educación superior y los organismos que la rigen, la presente ley es considerada de carácter humanista, cultural y científico, además de propender por el derecho de las personas a contribuir con el bien público y social.

Dentro de todos sus derechos se encuentra la igualdad de oportunidades, con el fin de que las y los individuos que ingresen a la educación superior puedan tener la oportunidad de acceder a una formación académica profesional de excelencia, es así que toda la ciudadanía constituida por las comunidades, pueblos y personas en general tienen el derecho de pertenecer y participar en el proceso educación superior a través de los mecanismos que sean establecidos por la LOES.

CAPÍTULO 2

Fines De La Educación Superior

Art. 5.- Derecho De Las Y Los Estudiantes. – Son Derechos De Las Y Los Estudiantes Los Siguietes:

- a) todos los estudiantes tendrán el derecho a acceder, movilizarse, regresar y titularse sin que sean discriminados en consideración a sus méritos académicos.
- b) los y las estudiantes tendrán educación superior de calidad y pertinente
- c) todos los estudiantes podrán contar y acceder con los medios y los recursos que sean necesarios y pertinentes para su formación
- d) los y las estudiantes tendrán el derecho de participar en el proceso de evaluación y acreditación de la carrera que estén cursando
- f) podrán elegir y ser elegidos para las representaciones estudiantiles
- g) cada uno de los estudiantes podrá ejercer la libertad de asociarse y expresarse bajo la libertad de cátedra
- h) los y las estudiantes podrán participar de los diferentes procesos de construcción, difusión y aplicación del conocimiento.
- i) tendrán derecho a recibir una educación superior laica, intercultural, democrática, que ayuda impulsar la equidad de género, la justicia y la paz.
- j) todos los estudiantes tendrán el derecho de recibir, atrás de sus méritos académicos diferentes ayudas económicas que les garanticen oportunidades educativas.

Dentro del presente articulado se establecen los derechos con los que gozarán las personas que accedan a la educación superior, es así que el sistema educativo esta direccionado hacia el respeto de los derechos y normas constitucionales de cada estudiantes, ponderando que la educación superior sea para todos, es decir no aceptará ningún tipo de discriminación, ya sean estas de raza, etnia, discapacidad, orientación sexual o cualquiera actitud o acción que

violente el derecho de las personas que decidan ingresar a la educación superior, otorgándole la posibilidad de participar en cualquier actividad académica que se lleva a cabo dentro de cualquier institución, menciona también que la educación superior debe regirse y ser impartida bajo la excelencia y una buena calidad, sin que existan inconvenientes de ningún tipo que tergiversen la educación del individuo, con esto se logrará que las personas que se encuentren dentro de la educación superior tengan un mejor rendimiento dentro de su proceso educativo y hacia la obtención de su título profesional, contando con que se remunerara el buen desempeño del estudiante bajo becas, créditos o distintos apoyos económicos el cual logre garantizar una igualdad en las oportunidades para cada persona.

En el contexto universitario, los docentes y profesionales de la investigación no solo ejercen derechos, sino que también tienen deberes fundamentales con la comunidad académica. Estos deberes incluyen el respeto por los derechos y garantías de los estudiantes, así como la obligación de promover una educación de calidad, en donde el tratamiento de datos personales debe observar principios legales como la finalidad, proporcionalidad y consentimiento

CAPÍTULO 2

Fines De La Educación Superior

Art. 6.1.- Deberes de las y los profesores e investigadores: Son deberes de las y los profesores e investigadores de conformidad con la Constitución y esta Ley los siguientes:

- a) Cumplir actividades de docencia, investigación y vinculación de acuerdo a las normas de calidad y normativas de los organismos que rigen el sistema y las de sus propias instituciones;
- b) Ejercer su derecho a la libertad de cátedra respetando los derechos y garantías constitucionales y legales del sistema y de sus propias instituciones;
- c) Promover los derechos consagrados en la Constitución y leyes vigentes;
- d) Mantener un proceso permanente de formación y capacitación para una constante actualización de la cátedra y consecución del principio de calidad;
- e) Someterse periódicamente a los procesos de evaluación; y,
- f) Cumplir con la normativa vigente, así como con las disposiciones internas de la institución de educación superior a la que pertenecen.

Este artículo recalca que el ejercicio docente debe enmarcarse en el respeto de las normas y garantías constitucionales, lo que incluye la protección de los derechos de los estudiantes en el entorno académico. En el caso de la protección de datos personales, este deber se traduce en una responsabilidad ética y legal para manejar la información de los estudiantes conforme

al principio de finalidad, es decir, utilizar los datos exclusivamente para los fines académicos legítimos previamente informados. Además, al promover los derechos constitucionales, los docentes se convierten en agentes claves para garantizar que el entorno educativo respete la privacidad, dignidad e integridad de cada estudiante.

La educación superior en el Ecuador está concebida como un proceso integral que persigue no solo la formación técnica o profesional de las personas, sino también el desarrollo de valores éticos, culturales, sociales y científicos que contribuyan al progreso del país, para ello, la Ley Orgánica de Educación Superior establece una serie de fines que deben guiar el funcionamiento de las instituciones de educación superior, dentro de los cuales se enmarca también el respeto a los derechos fundamentales de las y los estudiantes, como el manejo adecuado de su información personal conforme al principio de finalidad.

CAPÍTULO 2

Fines De La Educación Superior

Art. 8.- Fines de la Educación Superior. - La educación superior tendrá los siguientes fines:

- a) Aportar al desarrollo del pensamiento universal, al despliegue de la producción científica, de las artes y de la cultura y a la promoción de las transferencias e innovaciones tecnológicas;
- b) Fortalecer en las y los estudiantes un espíritu reflexivo orientado al logro de la autonomía personal, en un marco de libertad de pensamiento y de pluralismo ideológico;
- h) Contribuir en el desarrollo local y nacional de manera permanente, a través del trabajo comunitario o vinculación con la sociedad;
- i) Impulsar la generación de programas, proyectos y mecanismos para fortalecer la innovación, producción y transferencia científica y tecnológica en todos los ámbitos del conocimiento;

Plasma una visión amplia y progresiva del rol de la educación superior en la sociedad ecuatoriana, al establecer objetivos que integran tanto la producción científica como la responsabilidad ética y social, en este sentido, se debe entender que el respeto a los derechos de los estudiantes forma parte esencial de estos fines, el fortalecimiento de la autonomía personal, por ejemplo, implica el reconocimiento de la capacidad de cada estudiante para decidir sobre el uso de su información personal, aspecto directamente vinculado al principio de consentimiento informado.

El sistema de educación superior se estructura sobre principios fundamentales que orientan

su organización, funcionamiento y evaluación. Entre ellos se destacan la autonomía responsable, la igualdad, la calidad y, especialmente, la transparencia y no discriminación, los cuales guardan estrecha relación con el correcto tratamiento de los datos personales en el entorno universitario.

CAPITULO 3

PRINCIPIOS DEL SISTEMA DE EDUCACION SUPERIOR

Art. 12.- Principios del Sistema. - El Sistema de Educación Superior se rige por los principios de autonomía responsable, cogobierno, igualdad de oportunidades, calidad, pertinencia, integralidad, autodeterminación para la producción del pensamiento y conocimiento, en el marco del diálogo de saberes, pensamiento universal y producción científica y tecnológica global.

El Sistema de Educación Superior, al ser parte del Sistema Nacional de Inclusión y Equidad Social, se rige por los principios de universalidad, igualdad, equidad, progresividad, interculturalidad, solidaridad y no discriminación; y funcionará bajo los criterios de calidad, eficiencia, eficacia, transparencia, responsabilidad y participación.

Estos principios rigen de manera integral a las instituciones, actores, procesos, normas, recursos, y demás componentes del sistema, en los términos que establece esta Ley.

Este artículo sienta las bases para entender que la gestión institucional en la educación superior debe ser coherente con principios rectores. La transparencia y la igualdad de oportunidades, en particular, son claves para estructurar políticas adecuadas de tratamiento de información personal. El principio de transparencia exige que los estudiantes conozcan cómo se recolectan, almacenan, utilizan y eliminan sus datos. Por su parte, la no discriminación impone que ningún estudiante sea afectado o condicionado por el uso indebido de su información personal. Por tanto, el principio de finalidad se alinea directamente con estos principios rectores y fortalece la seguridad jurídica en el ámbito académico.

Las funciones del sistema de educación superior están dirigidas a garantizar el derecho a la educación mediante la docencia, la investigación y la vinculación con la sociedad. Este conjunto de funciones debe estar alineado con prácticas institucionales que respeten derechos fundamentales como el de la protección de datos personales.

CAPITULO 3

PRINCIPIOS DEL SISTEMA DE EDUCACION SUPERIOR

Art. 13.- Funciones del Sistema de Educación Superior. - Son funciones del Sistema de Educación Superior:

- a) Garantizar el derecho a la educación superior mediante la docencia, la investigación y su vinculación con la sociedad, y asegurar crecientes niveles de calidad, excelencia académica y pertinencia;
- p) Implementar políticas y programas institucionales con el fin de erradicar cualquier forma de violencia;
- q) Crear programas de prevención orientados a identificar las diferentes formas de violencia (institucional, sexual, psicológica, física, simbólica, patrimonial- económica, emocional);
- s) Establecer mecanismos de denuncia y ulterior reparación en caso de hechos probados. Estos mecanismos podrán ser implementados contra cualquier integrante de la comunidad universitaria.

Dentro de sus funciones sustantivas, el sistema de educación superior debe implementar políticas que erradiquen la violencia en todas sus formas, incluidas aquellas relacionadas con la exposición indebida o uso incorrecto de datos personales, lo que puede derivar en situaciones de acoso, discriminación o exclusión. Asimismo, se establece la obligación de contar con mecanismos de reparación, lo cual se alinea con los postulados de la Ley Orgánica de Protección de Datos Personales cuando se vulneran principios como el consentimiento o la finalidad. Por tanto, este artículo refuerza la necesidad de sistemas internos que supervisen el tratamiento adecuado de la información estudiantil.

La transparencia es un principio esencial del sistema universitario. No obstante, esta debe ejercerse sin vulnerar otros derechos fundamentales, como la privacidad y protección de datos personales. Por ello, el artículo 43 establece una obligación de publicar información institucional, pero sin perder de vista la normativa específica sobre protección de datos.

CAPITULO 2 PATRIMONIO Y FINANCIAMIENTO DE LAS INSTITUCIONES DE EDUCACION SUPERIOR

Art. 43.- Publicación de información en portal electrónico. - Las instituciones que conforman el Sistema de Educación Superior, en cumplimiento de la Ley, obligatoriamente deberán publicar en su portal electrónico las remuneraciones de sus autoridades, profesores, investigadores, servidores y trabajadores.

Esta información se integrará de manera obligatoria al Sistema Nacional de Información de la Educación Superior del Ecuador.

Si bien este artículo impulsa la transparencia institucional, también pone de manifiesto la tensión que puede surgir entre este principio y el derecho a la protección de datos personales.

La publicación de información debe respetar el principio de finalidad, es decir, debe tener un propósito claro, legítimo y proporcional. Publicar datos personales más allá de lo estrictamente necesario o sin consentimiento puede constituir una infracción a la normativa vigente. Por ello, las universidades deben implementar protocolos que permitan cumplir con este artículo sin incurrir en prácticas abusivas que comprometan la seguridad de los datos personales de sus miembros.

Estatuto de La Universidad Estatal Península de Santa Elena

El Estatuto Reformado 2021 de la Universidad Estatal Península de Santa Elena, surge como una necesidad de adecuar la normativa interna de la institución a los lineamientos establecidos en la Ley Orgánica de Educación Superior (LOES) y las disposiciones del Consejo de Educación Superior (CES). Este documento regula la estructura, funciones y principios que rigen el funcionamiento de la universidad, asegurando la correcta gestión académica, administrativa y financiera, la reforma responde a las exigencias del marco legal ecuatoriano y busca garantizar el cumplimiento de estándares de calidad en la educación superior, fortaleciendo la autonomía universitaria dentro de los límites que establece la normativa vigente.

Además, el Estatuto es el resultado de un proceso de actualización normativa en el que la UPSE ha buscado alinear sus principios institucionales con el desarrollo tecnológico y la modernización de sus procesos administrativos y educativos, la creciente digitalización de la información y la incorporación de tecnologías en la gestión académica han generado la necesidad de establecer mecanismos que regulen el almacenamiento, procesamiento y protección de los datos de la comunidad universitaria, sin embargo, a pesar de estos avances, el documento aún presenta vacíos normativos en relación con la protección de datos personales.

A continuación, se detallan los artículos del Estatuto de La Universidad Estatal Península de Santa Elena, que son vinculantes al tema.

CAPÍTULO II

Habilitantes de asesoría de orden académico

Art. 78.- Dirección de TIC's.- Es la dependencia encargada de dirigir, coordinar y gestionar estándares, políticas, normas, metodologías e infraestructuras; tendientes a la implementación y uso de tecnologías adecuadas a las necesidades de la Institución, tendencias tecnológicas y disposiciones gubernamentales.

Este artículo establece que la Dirección de TIC's tiene la responsabilidad de coordinar la gestión tecnológica de la universidad. Aunque no menciona explícitamente la protección de datos personales, su competencia en la administración de infraestructuras tecnológicas implica un papel clave en la seguridad de la información y en el tratamiento de datos de estudiantes, docentes y personal administrativo, la ausencia de una mención directa a la protección de datos personales sugiere que la universidad podría requerir normativas complementarias que detallen los procedimientos y mecanismos de resguardo de la información conforme a la Ley Orgánica de Protección de Datos Personales en Ecuador.

CAPÍTULO III

Derechos y Deberes

Art. 124.- Deberes. - Además de los establecidos en la Ley Orgánica del Servicio Público, Código de Trabajo y el Reglamento Interno, son deberes de las/los servidoras y las/los trabajadoras las siguientes:

e) Custodiar y conservar bajo su exclusiva responsabilidad los documentos impresos, digitales y demás información institucional, así como los bienes confiados a su cuidado y utilización. Responder por los daños que ocasionaren, de conformidad con la ley y la normatividad pertinente;

Este artículo resalta la obligación de los funcionarios de la universidad de proteger la documentación institucional, lo que puede incluir datos personales de estudiantes, docentes y empleados. Sin embargo, no se detallan medidas específicas de seguridad ni procedimientos para el almacenamiento y resguardo de la información. La falta de una mención explícita a la protección de datos personales o a la aplicación de la LOPDP podría generar vacíos normativos que permitan tratamientos inadecuados o riesgos de vulneración de derechos. La universidad debería considerar la adopción de reglamentos internos que garanticen la confidencialidad, integridad y disponibilidad de la información en conformidad con la normativa nacional vigente.

2.3 Marco Conceptual

Datos personales sensibles: Son aquellos datos que afectan la esfera más íntima del titular y que, por su uso indebido, pueden causar discriminación o vulneración de derechos. Incluyen el origen étnico, estado de salud, creencias religiosas, orientación sexual, datos biométricos y otros de naturaleza reservada.

Tratamiento de datos personales: Hace referencia a cualquier operación o conjunto de operaciones aplicadas a los datos personales, tales como la recolección, almacenamiento, uso, modificación, transferencia o eliminación. Este tratamiento debe cumplir con principios como la legalidad, finalidad, proporcionalidad, confidencialidad y seguridad.

Finalidad del tratamiento: Es el principio que obliga a que los datos personales sean tratados únicamente para el fin específico, explícito y legítimo para el cual fueron recolectados. Este fin debe ser previamente informado al titular. Cualquier uso posterior distinto sin consentimiento constituye una violación al principio de finalidad y, por tanto, al derecho a la protección de datos.

Consentimiento informado: Es la manifestación de voluntad libre, específica, informada e inequívoca mediante la cual el titular autoriza el tratamiento de sus datos.

Responsable del tratamiento: Es la persona natural o jurídica, pública o privada, que decide sobre el tratamiento de datos personales.

Titular de los datos personales: Es la persona natural a la que se refieren los datos que son objeto de tratamiento.

Protección de datos personales: Es el derecho fundamental que garantiza a toda persona el control sobre el uso de su información personal. Su finalidad es evitar que los datos sean utilizados sin consentimiento o con fines distintos a los autorizados, garantizando la seguridad, confidencialidad y transparencia en su tratamiento.

Violación de datos personales: Consiste en cualquier acción u omisión que provoque una filtración, acceso no autorizado, alteración, pérdida o uso indebido de los datos personales.

Transparencia informativa: Es el principio según el cual toda persona tiene derecho a ser informada sobre el uso que se dará a sus datos personales. Incluye conocer quién los trata, para qué finalidad, durante cuánto tiempo, y si serán compartidos con terceros. La falta de transparencia vulnera la confianza institucional.

Confidencialidad: Se refiere a la obligación que tienen quienes tratan datos personales de garantizar que estos no serán divulgados a personas no autorizadas.

Seguridad de la información: Son las medidas técnicas, organizativas y administrativas implementadas para proteger los datos personales contra accesos no autorizados, pérdida o alteración. En instituciones educativas, estas medidas deben ser robustas y conocidas por la comunidad universitaria.

Recolección de datos: Es la fase inicial del tratamiento de datos personales, que implica solicitar, capturar o registrar información del titular. En el entorno universitario, la recolección debe ser proporcional y ajustada al fin académico o administrativo que justifique su uso.

Entorno digital educativo: Hace referencia al uso de plataformas tecnológicas, formularios en línea, sistemas académicos y entornos virtuales que permiten la gestión institucional en las universidades. Estos espacios requieren especial atención en cuanto a la seguridad y transparencia del tratamiento de datos personales.

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1 Diseño y tipo de Investigación

El diseño de investigación se fundamentó en un enfoque cualitativo, orientado a la comprensión de los fenómenos asociados al principio de finalidad y el consentimiento informado en el tratamiento de datos personales, este enfoque permitió analizar las interacciones normativas y éticas que caracterizan la gestión de datos personales en la Universidad Estatal Península de Santa Elena.

La naturaleza descriptiva y exploratoria del estudio favoreció la interpretación de prácticas institucionales y su formación con el derecho a la protección de datos personales, según lo establecido en los artículos 66 y 92 de la Constitución de la República del Ecuador, y desarrollado por la Ley Orgánica de Protección de Datos Personales.

El diseño cualitativo facilitó un análisis detallado de los componentes, como la transparencia y la finalidad del tratamiento, dentro del ámbito educativo, las obligaciones legales coexisten con desafíos prácticos en su implementación. Además, este enfoque permitió captar percepciones, experiencias y actitudes de los actores involucrados, proporcionando una visión integral que contribuyó a formular recomendaciones basadas en evidencia.

Tipo de Investigación

Este estudio se clasificó como exploratorio, dado que se buscó investigar y comprender el grado de conocimiento, interpretación y aplicación del consentimiento informado y el principio de finalidad en la UPSE. Mediante un análisis documental, entrevistas semiestructuradas y encuestas, se exploraron las prácticas existentes relacionadas con la recolección, almacenamiento y uso de los datos personales de estudiantes y personal administrativo. El carácter exploratorio del estudio fue pertinente debido a la novedad en el marco legal en Ecuador, lo que exigió un examen preliminar para identificar brechas en el cumplimiento normativo y oportunidades de mejora.

3.2 Recolección de la Información

La combinación de técnicas de recolección de información consintió no solo describir las prácticas existentes, sino también evaluar cómo estas se relacionaban con las disposiciones legales vigentes, particularmente contenidas en la Ley Orgánica de Protección de Datos Personales, Reglamento General de Protección de Datos y en instrumentos internacionales, que sirvieron como referencia complementaria.

Población

La población de estudio estuvo compuesta por estudiantes y personal administrativo de la Universidad Estatal Península de Santa Elena, quienes son los actores principales en la gestión y tratamiento de los datos personales en el ámbito universitario, este grupo constituyó el entorno ideal para examinar las prácticas de consentimiento y el uso de datos personales, dado que su experiencia y perspectiva resultaron esenciales para evaluar el cumplimiento del principio de finalidad en la institución.

CUADRO 1: POBLACIÓN

ELEMENTOS	NI.
Constitución de la República del Ecuador	1
Ley Orgánica de Protección de Datos Personales	1
Reglamento de la Ley Orgánica de Protección de Datos	1
Reglamento de Bienestar Estudiantil	1
Estatuto de la Universidad Estatal Península de Santa Elena	1
Director de Bienestar Estudiantil UPSE	1
Vicerrectora Académica	1
Secretaria General de la UPSE	1
Director de TIC UPSE	1
Estudiantes de la UPSE	15.092
TOTAL	15.101

Elaborado por: Nathaly Torres y Carlos Vera

Muestra

Para llevar a cabo esta investigación, se seleccionó una muestra no probabilística por conveniencia, adaptada a la magnitud y características de la población estudiantil de la Universidad Estatal Península de Santa Elena, que contaba con un total de 15.092 estudiantes.

Dado que abordar a toda la población habría generado costos y demandas logísticas significativas, se optó por una reducción de esta muestra de estudiantes, lo cual permitió realizar un análisis más detallado sin comprometer la relevancia y la representatividad del estudio.

La muestra incluyó una selección de estudiantes e incorporación de actores clave, así como documentos normativos que regulan el tratamiento de datos en el ámbito universitario, este grupo comprendió la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales y su reglamento, el Estatuto de la Universidad, el Reglamento de Bienestar Estudiantil y políticas de Tecnologías de la Información y Comunicación (TIC). Estos elementos establecieron el marco legal y normativo para analizar cómo se gestionaban los datos personales dentro de la UPSE, enfocándose en su conformidad con los principios de consentimiento y finalidad en el uso de la información estudiantil.

Los representantes de la Secretaría General y del Vicerrectorado Académico aportaron una perspectiva administrativa, ya que son los responsables de la implementación de las normas internas en la universidad y estas áreas junto con el área de Bienestar Estudiantil juegan un rol determinante en la aplicación de protocolos de seguridad y privacidad en el tratamiento de la información de los estudiantes, ya que estos departamentos son los que manejan los datos personales de los estudiantes, se evaluó la eficacia de los sistemas de protección de datos en aspectos tanto operativos como normativos.

Al reducir la cantidad de estudiantes en la muestra, se buscó obtener un grupo que reflejara la diversidad y las diferentes experiencias de la población estudiantil en relación con la gestión de sus datos personales, esta selección permitió un enfoque en las experiencias concretas de los estudiantes y en cómo estos percibían la protección de sus datos y el manejo

del consentimiento informado por parte de la UPSE, al mismo tiempo, permitió una evaluación detallada de las prácticas que influían en la privacidad y la seguridad de la información personal dentro del ámbito educativo.

El análisis de esta muestra facilitó un abordaje que combinó perspectivas institucionales, normativas y prácticas, ahora bien, con esta metodología, se logró un estudio riguroso sobre los principios de protección de datos en la universidad, no solo con la revisión de la normativa vigente, sino que también considerando las percepciones de los estudiantes y los desafíos específicos que se plantean para la UPSE en la aplicación de estos principios en la gestión interna de los datos.

CUADRO 2. MUESTRA

ELEMENTOS	NI.
Constitución de la República del Ecuador	1
Ley Orgánica de Protección de Datos Personales	1
Reglamento de la Ley Orgánica de Protección de Datos	1
Reglamento de Bienestar Estudiantil	1
Estatuto de la Universidad Estatal Península de Santa Elena	1
Director de Bienestar Estudiantil UPSE	1
Vicerrectora Académica	1
Secretaría General de la UPSE	1
Director de TIC UPSE	1
Estudiantes de la UPSE	400
TOTAL	409

Elaborado por: Nathaly Torres y Carlos Vera

Métodos, Técnicas e Instrumentos

Método Analítico

El método analítico utilizado en esta investigación permitió descomponer y examinar minuciosamente cada uno de los elementos implicados en la protección de datos personales

en la Universidad Estatal Península de Santa Elena, este método se empleó para analizar cómo las normas legales y reglamentarias, tales como la Ley Orgánica de Protección de Datos Personales, su reglamento y las normas internas de la universidad, orientan el tratamiento de los datos personales de los estudiantes, a través de encuestas y guías de entrevista dirigidas a los actores involucrados, se obtuvo información detallada que permitió identificar las prácticas de manejo de datos y su conformidad con los principios de consentimiento y el principio de finalidad.

Mediante el uso de encuestas aplicadas a una muestra seleccionada de estudiantes y entrevistas realizadas a representantes de los distintos departamentos de la universidad, el método analítico facilitó una comparación entre la teoría y la práctica en el ámbito universitario, dentro de esta, cada respuesta obtenida en los cuestionarios y entrevistas fue examinada en detalle para desglosar las distintas dimensiones de la protección de datos, tales como los mecanismos de autorización, las prácticas de almacenamiento y las políticas de acceso a la información personal.

Este método no solo identificó las características de las políticas vigentes en la universidad, sino que también permitió descubrir puntos críticos en los que dichas políticas podrían no estar alineadas con los derechos de privacidad y protección de los estudiantes, dicha información recopilada de los cuestionarios a estudiantes y entrevistas a los departamentos, fue descompuesta y examinada a profundidad, lo que permitió establecer patrones y tendencias en la gestión de datos personales, así, este método proporcionó una visión completa de los elementos normativos y administrativos que impactaban la privacidad estudiantil en la universidad.

Método Exegético

Este método permitió interpretar y analizar las disposiciones legales y normativas relacionadas con la protección de datos personales en Ecuador y su aplicación en el ámbito universitario, se estudiaron textos fundamentales como la Constitución de la República, la Ley Orgánica de Protección de Datos Personales y las normas internas de la universidad, con el objetivo de comprender en profundidad el alcance y significado de cada disposición

aplicable al tratamiento de los datos personales de los estudiantes, estudio que luego fuera confrontado desde su aplicabilidad con la información obtenida de las entrevistas realizadas a representantes institucionales.

La aplicación del método en este trabajo fue de gran relevancia, ya que el análisis normativo permitió alcanzar una comprensión detallada de los temas abordados en el estudio, constituyéndose en una base fundamental tanto doctrinal como legal para sustentar la información obtenida y esto permitió comprender la importancia de la normativa en el desarrollo contemporáneo de la protección de datos personales, convirtiéndose en una herramienta fundamental para lograr el estudio jurídico del tema investigado.

Al examinar y contextualizar las interpretaciones normativas, el método exegético permitió establecer conclusiones sobre el nivel de cumplimiento de la UPSE respecto a las exigencias legales en materia de protección de datos personales de los estudiantes, ya que proporcionó una base sólida para evaluar si la institución había logrado una implementación adecuada de las normas, aspecto fundamental para identificar áreas de mejora en la garantía de los derechos de los estudiantes en cuanto a la seguridad de su información personal.

Método Deductivo

El método deductivo fue aplicado para construir un razonamiento lógico que partió de los principios generales de la normativa de protección de datos, con el propósito de analizar su impacto específico en el ámbito de la Universidad Estatal Península de Santa Elena, este proceso como tal, comenzó con la revisión de disposiciones generales contenidas en la Constitución de la República del Ecuador y en la Ley Orgánica de Protección de Datos Personales, para posteriormente observar cómo los principios se concretaban en las políticas y prácticas institucionales relacionadas con el manejo de datos personales de los estudiantes, infiriendo si las prácticas universitarias se ajustaban a los principios legales establecidos o no.

Las encuestas dirigidas a estudiantes y las entrevistas realizadas al personal administrativo de la UPSE permitió recoger datos que fueron analizados bajo un enfoque deductivo,

verificando si la normativa general en materia de protección de datos era implementada de forma específica en la UPSE y adecuada en la práctica diaria, tomando en cuenta los principios de consentimiento y finalidad, se obtuvo información esencial sobre cómo se comprendían y aplicaban estas disposiciones legales dentro del entorno universitario.

De la misma manera, este método permitió estructurar un análisis que fue enfocándose progresivamente en el ámbito específico de la UPSE, lo que facilitó la extracción de conclusiones concretas sobre la efectividad de las políticas institucionales en materia de protección de datos personales. Considerando tanto la normativa vigente como las prácticas observadas en la recolección y uso de datos estudiantiles, donde se lograron generar recomendaciones, orientadas a fortalecer la protección de los derechos de los estudiantes dentro de la institución.

En el ámbito de las dos técnicas principales para la recolección de información primaria, encuestas y entrevistas, la primera se ejecutó mediante un cuestionario estructurado con 10 preguntas dirigido a los estudiantes universitarios. El formulario fue difundido a través de la plataforma Google Formularios y permitió recopilar respuestas de una muestra de 400 estudiantes contactados a través de los presidentes de paralelos a fin de difundir el enlace y obtener la participación de los estudiantes. Todos los participantes otorgaron su consentimiento para participar, y se aseguró el anonimato y la confidencialidad de la información recabada, conforme a lo estipulado en la Ley Orgánica de Protección de Datos Personales.

La segunda técnica consistió en entrevistas semiestructuradas constituidas de entre 5 y 6 preguntas, realizadas a actores clave dentro del ámbito institucional y académico. Se entrevistó a personal administrativo de la universidad, en particular a funcionarios de áreas vinculadas con el manejo de datos, quienes accedieron a brindar información sobre los procedimientos internos aplicados para la recolección, uso y almacenamiento de los datos personales de los estudiantes.

Para el registro de las entrevistas se solicitó consentimiento explícito, ya sea por escrito en los casos presenciales o verbal en los encuentros virtuales, a fin de permitir la grabación de

audio. Las respuestas fueron transcritas y analizadas respetando los principios éticos de confidencialidad y protección de la identidad. Las entrevistas permitieron obtener una visión complementaria al enfoque estudiantil, revelando vacíos institucionales, debilidades en la implementación de protocolos y desconocimiento sobre los requisitos legales para el tratamiento de datos personales.

3.3 Tratamiento de la Información

Para llevar a cabo un tratamiento adecuado de la información recolectada en el presente estudio, se emplearon diversos elementos metodológicos esenciales que permitieron sustentar las conclusiones del trabajo, en una primera fase, se desarrolló una investigación bibliográfica y normativa, mediante el análisis de fuentes doctrinarias, artículos académicos, normas nacionales e instrumentos internacionales relacionados con la protección de datos personales, este proceso nos permitió establecer el marco teórico y jurídico que sirvió de base para evaluar el cumplimiento del principio de finalidad en el tratamiento de los datos personales de los estudiantes de la Universidad Estatal Península de Santa Elena.

Estos procedimientos arrancaron desde la fase de construcción del diseño de la investigación, etapa en la que se identificaron los temas doctrinarios documentales propicios para el desarrollo del marco teórico, orientados a partir de las variables de investigación, luego de la búsqueda de las fuentes respectivas, se sometió la información documental a una valoración rigurosa, mediante lectura analítica ordenando todos estos datos a través de los fichajes bibliográficos, la forma más propicia para el tratamiento de abundante información bibliográfica fueron las citas y los resúmenes permitiendo ordenar la información y priorizar los contenidos.

En este mismo sentido, la revisión normativa, se sometió a un ordenamiento jerarquizado, desde el más alto nivel según la pirámide kelseniana, esta revisión se realizó en el fichaje normativo, lo que hizo posible abordar de manera explícita el articulado que tributa de al tema, produciendo inferencias sobre el aporte de estas normas en el ámbito de la

investigación.

Respecto a la información obtenida en el trabajo de campo, el uso de los formularios de Google, hizo posible una sistematización ágil de los resultados, ya que la herramienta pone a disposición informes estadísticos de la recopilación, lo que facilitó su representación en el capítulo IV de este trabajo, así la información obtenida de las entrevistas, se materializó en resúmenes a partir de los audios levantados, lo que hizo posible mostrar las principales impresiones de los entrevistados a las preguntas planteadas.

Todos y cada uno de estos procedimientos han hecho posible un tratamiento adecuado de la información y fundamentalmente útil para la verificación de la idea a defender.

3.4 Operacionalización de variables

VARIABLES	CONCEPTO	DIMENSIONES	INDICADORES	ITEMS	TÉCNICA		
VARIABLE DEPENDIENTE Estudiantes de la Universidad Estatal Península de Santa Elena	Es la garantía de que los datos personales solo serán recopilados y tratados para fines específicos, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.	Finalidad declarada vs. uso real de datos	Concordancia entre el propósito declarado y el uso real de datos	¿Conoce usted el objetivo y uso que la UPSE dará a los datos personales que la Universidad solicita en los procesos de matriculación? ¿Conoce si sus datos han sido usados para otros fines?	Cuestionario dirigido a estudiantes		
		Consentimiento de los estudiantes	Claridad sobre el uso de los datos y solicitud de autorización	¿La universidad requirió su consentimiento antes de solicitar sus datos personales? En caso de tener dudas sobre el uso de sus datos personales, ¿sabe usted con quién debe comunicarse dentro de la universidad?		Cuestionario dirigido a estudiantes	
				Control del titular sobre sus datos	Derecho a decidir sobre sus datos personales		¿Cuando le han requerido datos personales le ha dado la opción de rechazar ciertos usos o rechazar la entrega de sus datos personales? ¿Cuando la UPSE requiere de sus datos personales le solicitan algún tipo de autorización para que estos puedan ser compartidos con terceros?
		VARIABLE INDEPENDIENTE Principio de finalidad en la protección de datos personales	Conjunto de operaciones que realiza la universidad sobre los datos de sus estudiantes, desde su recolección hasta su almacenamiento y			Políticas institucionales	Existencia de normativas y su conocimiento por parte de los usuarios

	eventual eliminación.	Consentimiento informado	Verificación del consentimiento previo y específico	¿Cuándo la UPSE le solicita sus datos personales, se le informa claramente sobre los fines y objetivos de su uso, permitiéndole otorgar un consentimiento libre e informado?	Cuestionario dirigido a estudiantes
				¿Ha sentido algún momento preocupación o zozobra respecto a la protección adecuada de los datos personales en la UPSE?	
				¿Conoce si la universidad ha tomado medidas para prevenir filtraciones o mal uso de sus datos?	
				¿Conoce de algún caso o casos en los que los datos personales de los estudiantes de la UPSE hayan sido expuestos generando situaciones de riesgo?	
		Transparencia y consentimiento	Inclusión de avisos digitales y consentimiento previo automatizado	¿Incluyen los sistemas digitales de la universidad avisos claros sobre el uso de los datos personales que recolectan?	Guía de entrevista dirigida a TIC
				¿Se exige el consentimiento digital del estudiante antes de ingresar su información en las plataformas institucionales?	
			Supervisión de información al titular y políticas de consentimiento	¿Qué política de control ejecuta la institución para garantizar que los estudiantes sean informados sobre el tratamiento y uso de sus datos personales?	Guía de entrevista dirigida a Vicerrectorado
				¿Qué protocolo o base normativa declara la obligatoriedad de la UPSE de requerir el consentimiento informado de los estudiantes para el tratamiento y uso de los datos personales?	
		Comunicación de	¿Cómo garantiza el Departamento de Bienestar Estudiantil que la recopilación de datos	Guía de	

			usos específico y recopilación con autorización	personales de los estudiantes se realiza con su autorización expresa y previa comunicación sobre los fines específicos de su uso?	entrevista dirigida a Bienestar Estudiantil
				¿Solicitan consentimiento explícito antes de recopilar datos sensibles como la ficha socioeconómica?	
			Información documental y validez del consentimiento físico	¿Qué política de control ejecuta la secretaria general para garantizar que los estudiantes sean informados sobre el tratamiento y uso que se dará a sus datos personales?	Guía de entrevista dirigida a Secretaria General
				¿Los formularios de inscripción o matrícula incluyen una cláusula de consentimiento informado?	
		¿Qué protocolo o base normativa declara la obligatoriedad de la UPSE de requerir el consentimiento informado de los estudiantes para el tratamiento y uso de los datos personales?			
		¿Monitorea secretaria la implementación de medidas de seguridad en el manejo de datos personales?			
		Seguridad en el tratamiento	Medidas tecnológicas aplicadas y control de acceso	¿Qué medidas de seguridad (como cifrado o autenticación) implementa el sistema para proteger los datos estudiantiles?	Guía de entrevista dirigida a TIC
				¿Cómo controla su departamento el acceso interno del personal a bases de datos estudiantiles?	
			Supervisión de políticas de seguridad y evaluación de	¿Qué tipo de auditoria o controles ejecuta la institución como medidas de seguridad en el manejo de datos personales?	Guía de entrevista dirigida a Vicerrectorado

			riesgos	¿Se realizan auditorías o evaluaciones sobre posibles riesgos en el tratamiento de datos estudiantiles?	
			Confidencialidad de datos sensibles y acceso restringido	¿Qué medidas aplican para resguardar la privacidad de la información confidencial del estudiante?	Guía de entrevista dirigida a Bienestar Estudiantil
				¿Quiénes tienen acceso autorizado a los expedientes de estudiantes dentro de esta unidad?	
				¿Qué protocolo utilizan para proteger físicamente los documentos que contienen información personal?	
			Custodia física de archivos y prevención del acceso no autorizado	¿Qué protocolo utilizan para proteger físicamente los documentos que contienen información personal?	Guía de entrevista dirigida a Secretaria General

Elaborado por: Nathaly Torres y Carlos Vera

CAPÍTULO IV

4 RESULTADOS Y DISCUSIÓN

4.1 Análisis, interpretación y discusión de resultados

4.1.1. Cuestionario a Estudiantes de la Universidad Estatal Península De Santa Elena

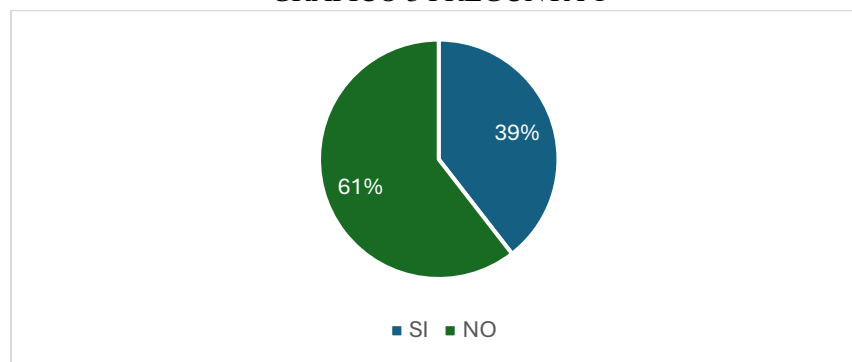
Pregunta 1: ¿Conoce usted el objetivo y uso que la UPSE dará a los datos personales que entrega a la universidad?

CUADRO 3 PREGUNTA 1

Valoración	Frecuencia	Porcentaje
Si	158	39%
No	242	61%
Resultados	400	100%

Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

GRÁFICO 3 PREGUNTA 1



Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

Análisis:

Esta pregunta buscó identificar si los estudiantes son conscientes del fin y propósito por el cual la universidad recolecta sus datos personales. De los 400 estudiantes encuestados, el 61% indicó desconocer esta información, mientras que solo el 39% manifestó estar informado. Este resultado refleja la necesidad de implementar mejores mecanismos que garanticen que los estudiantes reciban una explicación adecuada antes de entregar su información.

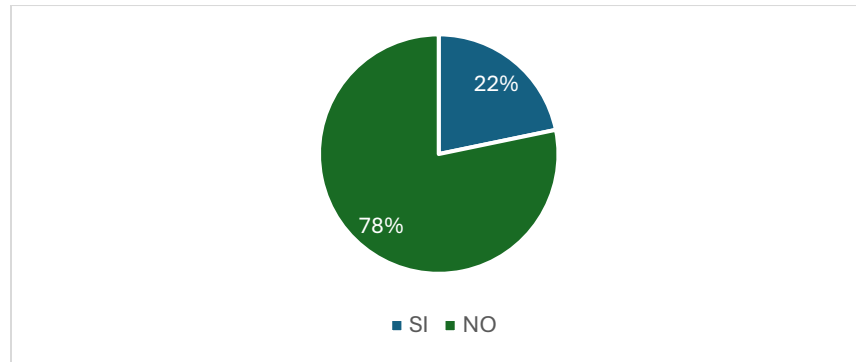
Pregunta 2: ¿Conoce si sus datos han sido usados para otros fines?

CUADRO 4 PREGUNTA 2

Valoración	Frecuencia	Porcentaje
Si	87	22%
No	313	78%
Resultados	400	100%

Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

GRÁFICO 4 PREGUNTA 2



Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

Análisis:

Un 78% de los estudiantes declaró que no tiene conocimiento de que sus datos hayan sido utilizados con fines distintos a los inicialmente previstos.

Este resultado puede interpretarse de manera positiva en cuanto a que, hasta el momento, no existe una percepción generalizada de mal uso, no obstante, para fortalecer esta confianza, sería ideal establecer más canales de información donde se notifiquen los usos institucionales de datos, especialmente cuando se traten con finalidades académicas, administrativas o investigativas, pues estas acciones no solo reflejarían cumplimiento normativo, sino también cultura de derechos informativos.

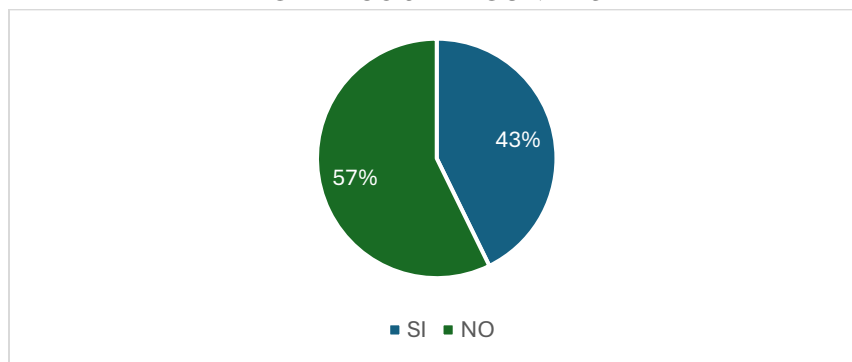
Pregunta 3: ¿La universidad requirió su consentimiento antes de solicitar sus datos personales?

CUADRO 5 PREGUNTA 3

Valoración	Frecuencia	Porcentaje
Si	171	43%
No	229	57%
Resultados	400%	100%

Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

GRÁFICO 5 PREGUNTA 3



Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

Análisis:

Según los resultados, un 57% de estudiantes manifestó que no se les solicitó consentimiento de forma explícita, esta respuesta puede atribuirse a la necesidad de formalización de un procedimiento estandarizado, sin embargo, la Universidad ha manifestado su intención de mejorar en este aspecto.

La creación de formularios digitales con opciones claras y segmentadas de consentimiento representa un paso hacia la modernización institucional, esto se alinea con las tendencias internacionales en gobernanza universitaria, reforzando el perfil institucional de la UPSE como garante de los derechos fundamentales.

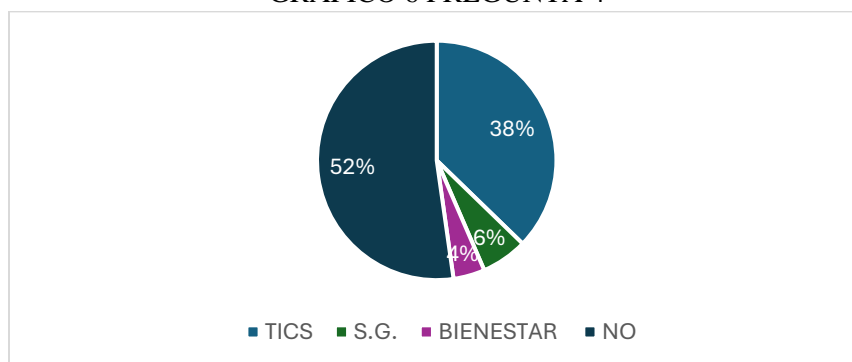
Pregunta 4: En caso de tener dudas sobre el uso de sus datos personales, ¿sabe usted con quién debe comunicarse dentro de la universidad?

CUADRO 6 PREGUNTA 4

Valoración	Frecuencia	Porcentaje
Sí, con el Departamento de (TIC)	149	38%
Sí, con la Secretaría General	25	6%
Sí, con Bienestar Universitario	17	4%
No	209	52%
Resultados	400	100%

Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

GRÁFICO 6 PREGUNTA 4



Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

Análisis:

Dentro de esta pregunta el 52% manifestó no tener claridad sobre a quién acudir en caso de dudas.

Esta situación puede resolverse con medidas sencillas y de gran impacto, como designar un canal exclusivo de atención al estudiante en materia de protección de datos, visibilizar su contacto en todos los formularios institucionales y crear una sección específica en la página web de la universidad, así, se garantizaría el derecho de los estudiantes a recibir información oportuna y adecuada, y se fortalecería la noción de corresponsabilidad entre la institución y sus miembros.

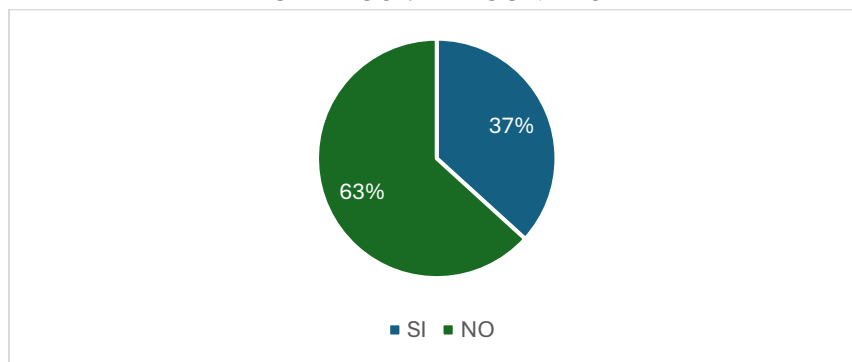
Pregunta 5: ¿Cuándo le han requerido datos personales, le ha dado la opción de rechazar ciertos usos o rechazar la entrega de sus datos personales?

CUADRO 7 PREGUNTA 5

Valoración	Frecuencia	Porcentaje
Si	147	37%
No	253	63%
Resultados	400	100%

Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

GRÁFICO 7 PREGUNTA 5



Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

Análisis:

El 63% de estudiantes expresó que no se le ofreció esa posibilidad de rechazar la entrega de sus datos personales, esto evidencia la necesidad del enfoque institucional de consentimiento, el cual permite aceptar unos usos y rechazar otros.

Esta técnica ya es empleada por instituciones de alto nivel y su adopción en la UPSE no solo sería legalmente válida, sino pedagógicamente formativa, ya que esto enseñaría a los jóvenes a ejercer sus derechos desde un enfoque activo y reflexivo sobre el uso de su identidad digital y el manejo de los datos personales.

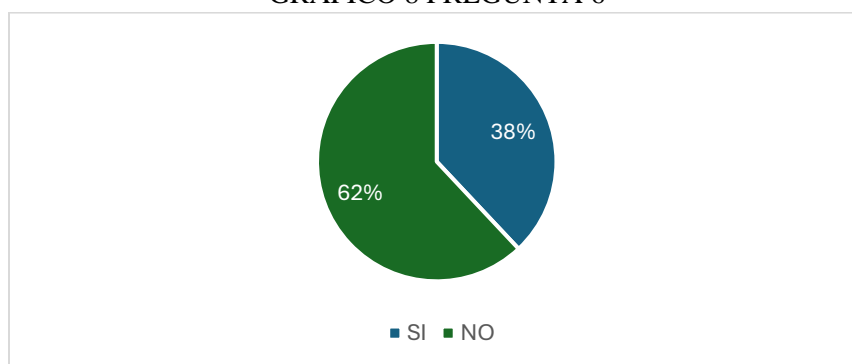
Pregunta 6: ¿Cuándo la UPSE requiere de sus datos personales le solicitan algún tipo de autorización para que estos puedan ser compartidos con terceros?

CUADRO 8 PREGUNTA 6

Valoración	Frecuencia	Porcentaje
Si	152	38%
No	248	62%
Resultados	400	100%

Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

GRÁFICO 8 PREGUNTA 6



Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

Análisis:

El 62% de los encuestados señaló que no se les solicita autorización.

Ante este resultado, se pueden inferir dos situaciones, la primera y que más se acercaría a la realidad, es que los usos de datos estudiantiles son exclusivamente institucionales, la otra es que se obvие el requerimiento de usos con terceros, lo cual es descartado a partir de lo declarado por los encuestados en la pregunta dos.

Sin embargo, al ser una entidad pública que pertenece al sistema de educación superior, parte de su labor es entregar informes a los entes de control, siendo así, se podría incluir cláusulas de cesión de datos con explicación concreta del porqué, bajo qué acuerdos y con qué garantías se realiza tal acción, esto ayudaría a reducir la desconfianza y a blindar la universidad frente a posibles responsabilidades futuras.

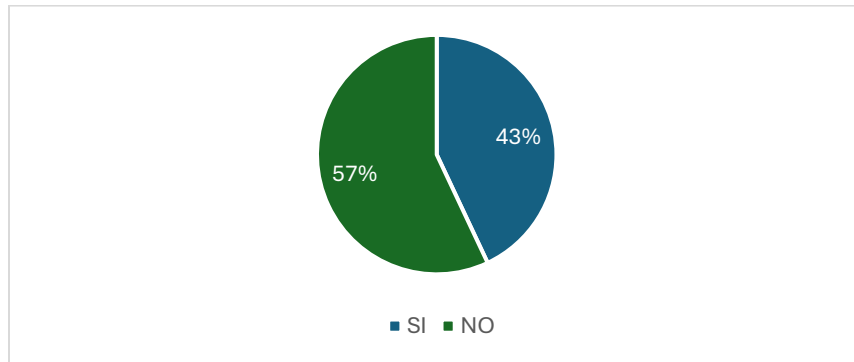
Pregunta 7: ¿Cuándo la UPSE le solicita sus datos personales, se le informa claramente sobre los fines y objetivos de su uso, permitiéndole otorgar un consentimiento libre e informado?

CUADRO 9 PREGUNTA 7

Valoración	Frecuencia	Porcentaje
Si	172	43%
No	228	57%
Resultados	400	100%

Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

GRÁFICO 9 PREGUNTA 7



Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

Análisis:

El 57% de los estudiantes expresó que la información no es clara, esto denota la necesidad de fortalecer uno de los pilares del consentimiento, la claridad, frente a ello se podría implementar un sistema visual para explicar qué tipos de datos son necesarios, opcionales o sensibles, y con qué finalidades específicas serán usados.

Este enfoque pedagógico, además de facilitar la comprensión, generaría una percepción de respeto institucional hacia los derechos del estudiante, fortaleciendo el vínculo de confianza entre ambos.

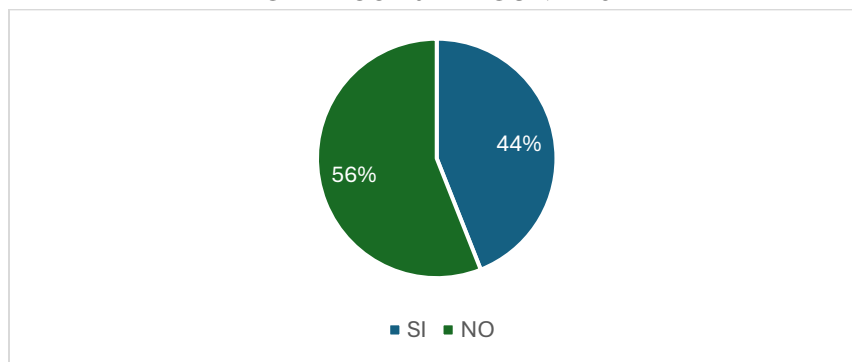
Pregunta 8: ¿Ha sentido algún momento preocupación o zozobra respecto a la protección adecuada de los datos personales en la UPSE?

CUADRO 10 PREGUNTA 8

Valoración	Frecuencia	Porcentaje
Si	176	44%
No	224	56%
Resultados	400	100%

Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

GRÁFICO 10 PREGUNTA 8



Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

Análisis:

Un 44% de los estudiantes señaló haber sentido preocupación respecto a la protección de sus datos, mientras que el 56% no manifestó esta inquietud.

Este dato no debe verse como un reproche institucional, sino como una alerta temprana que revela una comunidad universitaria más consciente, crítica y exigente en temas digitales, por ello, implementar espacios de diálogo como Foros de Privacidad Universitaria o asignaturas optativas sobre los datos personales podría ser una acción pionera, en tiempos donde los datos son activos estratégicos, educar sobre su valor es una forma de formar ciudadanos con criterio.

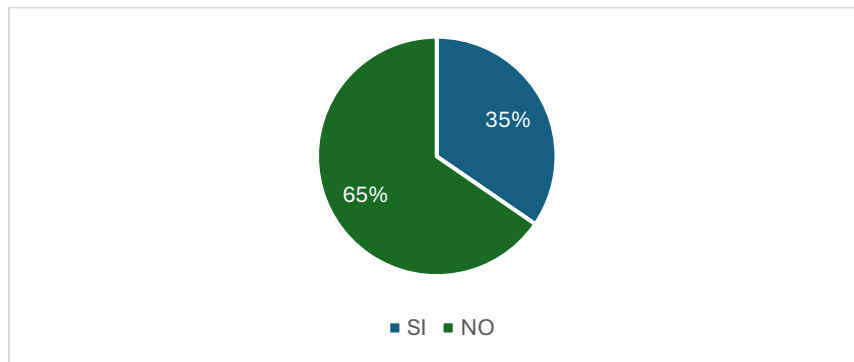
Pregunta 9: ¿Conoce si la universidad ha tomado medidas para prevenir filtraciones o mal uso de sus datos?

CUADRO 11 PREGUNTA 9

Valoración	Frecuencia	Porcentaje
Si	138	35%
No	261	65%
Resultados	400	100%

Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

GRÁFICO 11 PREGUNTA 9



Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

Análisis:

El 65% de los estudiantes manifestó desconocer si la universidad aplica medidas preventivas contra filtraciones o mal uso de la información, mientras que solo el 35% indicó estar informado, esta respuesta evidencia una brecha de información, no necesariamente de gestión.

Es probable que existan medidas de seguridad ya implementadas, pero poco difundidas, visibilizar públicamente los protocolos existentes como el uso de servidores seguros, políticas de confidencialidad o designación de responsables de tratamiento permitiría a la comunidad universitaria conocer y valorar los esfuerzos institucionales por salvaguardar su información, fortaleciendo la confianza y el sentido de pertenencia.

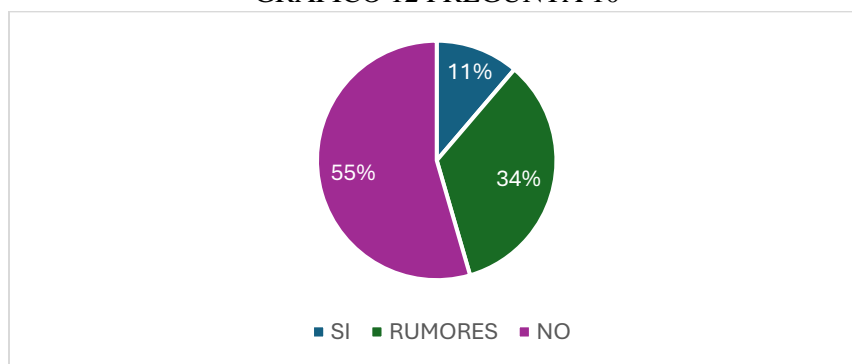
Pregunta 10: ¿Conoce de algún caso o casos en los que los datos personales de los estudiantes de la UPSE hayan sido expuestos generando situaciones de riesgo?

CUADRO 12 PREGUNTA 10

Valoración	Frecuencia	Porcentaje
Sí, conozco uno o varios casos	45	11%
He escuchado rumores	137	34%
No, no conozco ningún caso	218	55%
Resultados	400	100%

Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

GRÁFICO 12 PREGUNTA 10



Elaborado por: Nathaly Torres y Carlos Vera – Fuente: Encuesta realiza a estudiantes

Análisis:

El 55% de los estudiantes indicó no conocer ningún caso, el 34% afirmó haber escuchado rumores, y un 11% dijo conocer uno o varios casos. Esto demuestra que no existe una percepción generalizada de vulneraciones graves, lo que es positivo.

Sin embargo, para evitar que los rumores se conviertan en desconfianza, la universidad podría establecer un sistema interno de reporte de incidentes, con procesos de verificación y medidas correctivas, demostrando así su compromiso con la rendición de cuentas y la mejora continua sobre los datos personales de los estudiantes.

4.1.2. Análisis de entrevista dirigida al Departamento De Tic

Nombre del entrevistado: Ing. Fabricio Ramos Mgt.

Fecha de la entrevista: Lunes, 26 de mayo de 2025

Lugar de la entrevista: Universidad Estatal Península de Santa Elena

Pregunta 1 ¿Cuál es la norma o política de protección de datos establecida por la UPSE?

Actualmente la Universidad Estatal Península de Santa Elena no cuenta con una norma o una política de protección de datos personales, pero ya se encuentra en la creación de políticas de protección de datos personales, por el cumplimiento con lo que dispone la Ley dictada por el ministerio.

Pregunta 2 ¿Dentro del protocolo de protección de datos, se permite al estudiante rechazar la entrega de ciertos datos?

Así es, como les mencioné, si hay restricción de datos obviamente sensibles, datos como el facilitar información ya sea con número de cédula, dirección domiciliaria, número de teléfonos y otros temas netamente personales, obviamente si se rechaza ese tema de información, siempre y cuando igual lo justifique por escrito, exactamente cuál es la información, pero sí existe, netamente como departamento se restringe ese tipo de información y esta información solamente la tiene el área correspondiente o indicada para el proceso de este tipo de información. Datos netamente sensibles, como ya les indiqué en su momento, un caso especial como ejemplo, las fichas socioeconómicas netamente es una información confidencial que solamente la maneja y la procesa el departamento de Bienestar Estudiantil.

Pregunta 3 ¿Incluyen los sistemas digitales de la universidad avisos claros sobre el uso de los datos personales que recolectan?

Como les indiqué en el punto uno, se están armando políticas, obviamente dentro de las políticas se armarán directrices que incluirá el tema de los avisos correspondientes en cada una de las aplicaciones informáticas sobre la Ley de Protección de Datos Personales.

Pregunta 4 ¿Se exige el consentimiento digital del estudiante antes de ingresar su información en las plataformas institucionales?

Es igual al punto anterior, en donde cada estudiante, se creará el tema del consentimiento de sus usos personales, pero en este caso enfocado al tema netamente estadístico y de acuerdo y de pronto alguna exigencia que le solicite con respecto a la revisión de calificaciones y otros temas donde no involucren datos sensibles en este caso.

Pregunta 5 ¿Qué medidas de seguridad (como cifrado o autenticación) implementa el sistema para proteger los datos estudiantiles?

Como departamento de TIC, nosotros tenemos el manejo de medidas de seguridad a nivel de los servicios académicos, como el SGA a través de protocolos de seguridad como mencioné, el HTTPS. Nosotros técnicamente le llamamos servicios SSL y adicional el departamento como tal tiene implementado un tema de equipo de seguridad perimetral que realmente permite cifrar contenido que el estudiante o el docente puede o no puede revisar con respecto al uso del servicio de internet, son políticas que se me ocurren estudiantes de violencia, de pornografía, de juegos estas son políticas que realmente se implementan dentro del equipo de seguridad perimetral.

Pregunta 6 ¿Cómo controla su departamento el acceso interno del personal a bases de datos estudiantiles?

Realmente aquí, nosotros, el departamento controla en la asignación del desarrollo de aplicaciones de manera individual, con la finalidad de tener mayor control de quienes manejan y manipulan ese tema de información para el desarrollo de la aplicación aunque se les mencionó que normalmente el personal que maneja esta información, normalmente no maneja, sino que quien desarrolla este tipo de aplicaciones siempre lo hacen con datos ficticios a nivel de desarrollo, y una vez que esté ya funcionando el proceso de manera correcta ya se colocará en producción ya con datos netamente reales y esta información como les mencioné netamente la maneja el departamento requirente de la aplicación quien netamente procesa la información a nivel de reporte o a nivel de ingreso de información o datos.

Análisis:

De la entrevista realizada al director del departamento de Tic, se puede advertir un proceso que requiere adecuación institucional a la Ley Orgánica de Protección de Datos Personales. Si bien se reconoce que la universidad aún no cuenta con una política formal de protección de datos, se evidencian esfuerzos en marcha para su elaboración, como respuesta a las exigencias normativas vigentes en Ecuador, esto denota una postura proactiva de manera preventiva, a fin de dar con el cumplimiento de la normativa, se activa a partir de la obligatoriedad legal, manifestando un compromiso institucional previo con los derechos digitales de los estudiantes.

En cuanto a la autodeterminación informativa, se resalta que el estudiante tiene la posibilidad de rechazar la entrega de ciertos datos personales, especialmente aquellos considerados sensibles como el número de cédula, dirección domiciliaria o situación socioeconómica, no obstante, esta facultad se encuentra condicionada a una justificación escrita y a la valoración del departamento correspondiente, por otra parte, se menciona que los sistemas digitales de la universidad aún no incorporan avisos claros sobre el uso de los datos personales recolectados, pero se espera que estos se integren dentro de las políticas que se están desarrollando.

En materia de seguridad técnica, se indica el uso de protocolos HTTPS (SSL) y dispositivos de seguridad perimetral, lo cual refleja una infraestructura básica de protección frente a amenazas externas, a pesar de ello, se brindan detalles con poca información sobre el cifrado de bases de datos internas, autenticación multifactorial y medidas contra accesos no autorizados, las cuales eventualmente se verán vulneradas sin no se ajustan correctamente políticas internas basadas en la seguridad de la información.

El testimonio revela un panorama en transición a una cultura consolidada de protección de datos personales, aunque existen señales de avance, las políticas que aún se encuentran en desarrollo, los mecanismos de consentimiento digital, avisos transparentes y medidas de seguridad más integrales, pone en riesgo el ejercicio pleno del derecho a la protección de datos por parte de los estudiantes.

4.1.3. Análisis de entrevista dirigida a la Vicerrectora

Nombre del entrevistado: Lcda. Gisella Paula Chica, PhD.

Fecha de la entrevista: Martes, 20 de mayo de 2025

Lugar de la entrevista: Plataforma de Videoconferencia Zoom

Pregunta 1 ¿Qué política de control ejecuta la institución para garantizar que los estudiantes sean informados sobre el tratamiento y uso de sus datos personales?

Para saber de datos personales, como por ejemplo una ficha socioeconómica el departamento de bienestar universitario mediante una plataforma emite desde el inicio de ese joven, desde nivelación, que van a procesarse ciertos datos y que eso se mantiene en confidencialidad de ese departamento de bienestar universitario, nosotros hacemos el llenado de ficha del estudiante, o el estudiante llena, todos esos datos no los puedo observar a nadie, solamente el departamento de bienestar universitario, una vez el departamento de bienestar universitario coloca dentro de la ficha, ni el programador, el programador lo único que hace es, colocar el porcentaje de ese indicador y la tabulación de la misma, eso es lo que hace el programador, el estudiante llena, se le informa que va a tener que llenar una ficha socioeconómica y que esos datos serán específicamente para el departamento de bienestar universitario hizo el tratamiento, el cual es que vaya directamente al psicólogo, al odontólogo, a la enfermera o al médico, de esa manera ellos tiene la documentación, hasta ahí nadie sabe la información de cada estudiante, porque los datos se mantiene en esa plataforma guardados, en qué momento salen a relucir esos datos, cuando se necesita un tratamiento específico de alguien.

Pregunta 2 ¿Qué protocolo o base normativa declara la obligatoriedad de la UPSE de requerir el consentimiento informado de los estudiantes para el tratamiento y uso de los datos personales?

En el artículo vigente del 2021 se trató muchísimo esta parte sobre la LOPDP del Ecuador, en donde tratamos de llevar esa finalidad que se encuentra en el artículo 7, eso lo maneja el departamento de bienestar junto con USIC, la cual es la unidad que se encarga de todo el procesamiento de la seguridad física de los trabajadores, estudiantes y su procesamiento de datos, la parte de datos se encarga el departamento de TIC, el director Fabricio Ramos, ese tratamiento lo lleva con la finalidad de determinar de manera muy explícita y legítima a la vez toda la información del estudiante y docente, ellos tratan de que todas información sea

guardada y sujeta sobre una base de datos legal, teniendo toda esa información normada, toda esta información se podría habilitar sólo con la autorización de TIC, siempre y cuando el departamento de bienestar universitario emita un oficio diciendo que se habilita la extracción de los datos, todos estos departamentos cuentan con una norma vigente del 2021 que se encuentra sujeta a la LOPDP.

Pregunta 3 ¿Qué tipo de auditoría o controles ejecuta la institución como medidas de seguridad en el manejo de datos personales?

Corresponde a la auditoría externa y la auditoría interna, externa siendo la que viene por parte del gobierno y la interna es la que nosotros posiblemente busquemos a una empresa para que realice todo el seguimiento de la misma, estas auditorías de las plataformas son a las que más atención se le debe prestar, debido a que las plataformas muchas veces por las actualizaciones del sistema, existe vulnerabilidad del ingreso, por lo tanto cuando se realizan éstas evaluaciones internas lo maneja el departamento de TIC y cuando llegara a pasar algo, que si ha ocurrido, no puedo mentir, por ejemplo cuando en el año 2022 a todos los estudiantes se les puso 100, De nivelación a posgrado, en esos momentos se le pidió a TIC que llame a su proveedor que mantiene los datos de todos nuestros estudiantes y docentes, hicieron posible que con 11 programadores ingresen y realicen una auditoría interna para identificar desde qué dirección IP pudieron ingresar y saber quién modificó todas las notas, pero es que nosotros no trabajamos sólo en plataformas, porque por encima de nosotros están ciertas áreas de desarrollo, que se encargan de reservar toda la información y si llegara a pasar algo la responsabilidad cae sobre las partes.

Pregunta 4. ¿Se realizan auditorías o evaluaciones sobre posibles riesgos en el tratamiento de datos estudiantiles?

No, esas auditorías solamente son específicas, no estudiantes, específicas cuando hablamos de periodos o años electivos, no estudiantes, eso significa que es de todos, se enlace anual y se la entrega en el mes de febrero de cada año a la SENECYT.

Análisis:

En síntesis de la entrevista realizada a la vicerrectora de la universidad, se puede observar que aunque la institución muestra un compromiso inicial en función a la confidencialidad de los datos personales, bajo el cumplimiento de lo estipulado en la Ley Orgánica de Protección

de Datos Personales en el Ecuador, se continúan extendiendo esfuerzos en lo relativo a la claridad de la asignación de responsabilidades entre los departamentos, formalidades sobre el consentimiento y manejo de datos, las cuales de no ser intervenidas desembocarían en la posible vulnerabilidad de los datos sensibles del estudiantado. Las auditorías existentes, son generales y no abordan en su totalidad la protección de datos personales, lo cual podría limitar su efectividad; en conjunto, se requiere un plan de gestión integral, con procedimientos normados, roles claramente definidos, auditorías específicas y una cultura institucional sólida en torno a la protección de la información de sus estudiantes, docentes y personal administrativo.

4.1.4. Análisis de entrevista dirigida al Departamento de Bienestar Estudiantil

Nombre del entrevistado: Lic. Marlon Novillo, Mgt.

Fecha de la entrevista: Lunes, 26 de mayo de 2025

Lugar de la entrevista: Universidad Estatal Península de Santa Elena

Pregunta 1 ¿Cómo garantiza el Departamento de Bienestar Estudiantil que la recopilación de datos personales de los estudiantes se realiza con su autorización expresa y previa comunicación sobre los fines específicos de su uso?

Nosotros como bienestar universitario tenemos una plataforma de sistemas, donde prácticamente a casi todos los servicios, el estudiante puede acceder mediante la plataforma, digo casi porque hay otros que son presenciales por la naturaleza de las atenciones que nosotros damos, uno de los servicios son las herramientas o instrumentos socioeconómicos que nosotros tenemos para obtener la información de los estudiantes, que es la denominada ficha socioeconómica, también tenemos un formato de vulnerabilidad y una ficha psicológica, las tres fichas obviamente son netamente personales del estudiante, en el momento que entra al SGA puede obtener la información específica de su ficha, no es una información pública por el tipo de información que tiene, en cada período académico 15 días antes del proceso de matriculación se solicita al departamento de TIC se habiliten las plataforma para que los estudiantes puedan llenar o actualizar la ficha socioeconómica y sus datos como también de las otras dos fichas, se lo realiza antes de la matrícula porque también se apertura el proceso de postulación de becas, luego del periodo de llenado se cierra la ficha socioeconómica para que no sea manipulable porque alguien se entera que hay beca por esto

y después quiere manipular la información, entonces ellos la llenan y esa es la información que queda durante todo el período académico, se la actualiza conforme el siguiente periodo académico según cómo ya se lo mencionó y toda esa información queda en la plataforma.

Pregunta 2 ¿Solicitan consentimiento explícito antes de recopilar datos sensibles como la ficha socioeconómica?

No, no le solicitamos el consentimiento puesto que al menos en lo que es ficha socioeconómica son datos que en cualquier encuesta socioeconómica se las aplica, en el tema de la ficha psicológica el estudiante la llena y si por algún motivo no quiere, no la llena, vendría a ser opcional, no es una obligación, pero en el momento de que un estudiante no la quiera llenar, que no hasta el momento no hemos tenido casos, nosotros haríamos el acercamiento con el estudiante porque puede ser que tenga un inconveniente en el que un no, no la quiero llenar, a la final no es una solución para el mismo porque puede estar teniendo algún tipo de inconvenientes personales, que nosotros queremos abordarlo para poder brindarles la ayuda del caso, pero no ha sucedido, sin embargo no es una obligatoriedad porque los datos psicológicos de los estudiantes pues son muy personales y confidenciales, de la misma forma que solo el área de psicología tiene acceso a esa información, solamente en casos muy estrictos que una carrera solicite alguna información relevante de un estudiante bien justificada nosotros le daríamos la información.

Pregunta 3 ¿Qué medidas aplican para resguardar la privacidad de la información confidencial del estudiante?

Justamente en relación a lo que les conteste hace un momento, toda la información que el área de psicología replica, no solamente con la ficha psicológica sino también con la atención de libre demanda que se tiene acá, estamos nosotros por implementar una plataforma donde se va a ir registrando los casos del estudiante puesto que es importante tener eso porque no solamente en documentos físicos sino que también contar con cuál es el historial psicológico del estudiante, el tema de la confidencialidad es netamente la información receptada del mismo y que solamente se encarga los profesionales del área, que informan quienes son los estudiantes que vinieron a hacerse atender pero los detalles son muy generales donde se

aplican los diagnósticos y las recomendaciones que se emiten incluso a la carreras pero toda esa información queda en el área de psicología clínica y educativa.

Pregunta 4 ¿Quiénes tienen acceso autorizado a los expedientes de estudiantes dentro de esta unidad?

El área de psicología clínica y educativa son las que manejan la información de primera mano y en el caso de ser necesario se lo solicita por medio de vicerrectorado justamente para tratar casos en específicos, como un acto indisciplinario o de pronto algo que sea necesario poder conocer sobre el comportamiento por algún factor muy específico del estudiante, solo de esa manera nosotros podríamos compartir esa información, pero de ahí a nadie, no está visible en plataforma ni nada, toda la información está netamente en el área de psicología clínica y educativa.

Pregunta 5 ¿Qué protocolo utilizan para proteger físicamente los documentos que contienen información personal?

El área de psicología tiene un protocolo de funcionamiento y de aplicación, en el mismo está la manipulación de la información, todo lo referente a la información física que por ahora se lo utiliza como acompañamiento, pero más bien todos se encuentra en las plataformas de ellos, pero es algo que simplemente que ellos las mantiene dentro de las áreas y que como les decía al inicio de la entrevista estamos con una plataforma de sistemas que se la está ampliando para poder en la misma ir teniendo el historial psicológico de los estudiantes, donde ese sería el repositorio ya ni tanto en físico sino en plataforma y en dónde el acceso va a ser exclusivamente para el área de psicología con las dos representantes con las que contamos aquí.

Análisis:

La presente entrevista permite evidenciar que la Universidad Estatal Península de Santa Elena ha implementado mecanismos para la recolección y gestión de información sensible de sus estudiantes, como lo son las mencionadas fichas socioeconómicas, psicológicas y de vulnerabilidad, las mismas que se recolectan a través del Sistema de Gestión Académica, en sus siglas SGA, con el debido acceso restringido solamente para personal autorizado, en este

caso el área de psicología, lo que representa un avance positivo en cuanto al resguardo de la confidencialidad.

Sin embargo, el no consentimiento informado expreso, principalmente en el caso de la ficha socioeconómica, la cual se considera obligatoria para el estudiante, no se manifiesta la posibilidad de aceptar o rechazar el tratamiento de sus datos, esto representa una limitación frente a lo establecido en la Ley Orgánica de Protección de Datos Personales, aunque la ficha psicológica es opcional, no se incluyen protocolos formales que acrediten el consentimiento ni los mecanismos adecuados que podrían garantizar su voluntariedad.

Si bien existen esfuerzos por parte de la universidad para proteger la información estudiantil, es necesario fortalecer el marco normativo interno, adoptando protocolos basados en la legislación vigente, e implementar medidas concretas para garantizar el consentimiento, la seguridad y la integridad de los datos personales.

4.1.5. Análisis de entrevista dirigida a Secretaria General

Nombre del entrevistado: Abg. María Rivera González, Mgt.

Fecha de la entrevista: Lunes, 26 de mayo de 2025

Lugar de la entrevista: Universidad Estatal Península de Santa Elena

Pregunta 1 ¿Qué política de control ejecuta secretaria para garantizar que los estudiantes sean informados sobre el tratamiento y uso de sus datos personales?

Nosotros damos capacitaciones dos veces en el año, a los chicos le informamos sobre las actualizaciones que está realizando la universidad respecto a toda la normativa vigente entre ellas le damos los derechos, le indicamos los derechos a los chicos pero a la vez se coordina con los departamentos de TIC que es de Tecnologías de la Información y con el responsable de tratamiento de datos personales, ellos a su vez mediante la responsabilidad que se le ha atribuido son los que se encargan específicamente de manejar dentro del sistema académico la información personal de los estudiantes para que se mantenga con la privacidad que esta requiere y que solamente sea remitida a petición del mismo solicitante o bajo la autorización del estudiante, la Secretaría General no emite ninguna certificación ni ningún documento personal a personas que sean ajenas al peticionario siempre los documentos que se han emitido Secretaría General son directamente al propietario de la información y a su vez a

aquellas peticiones que nos hacen llegar por la vía judicial a las que si estamos obligados a responder.

Pregunta 2 ¿Los formularios de inscripción o matrícula incluyen una cláusula de consentimiento informado?

Si, normalmente todos los correos ya institucionales desde hace más de un año o dos años creo que ya nos estamos trabajando justamente con aquella cláusula de confidencialidad todos los documentos llenan una ficha socioeconómica y esa ficha socioeconómica se mantiene con la confidencialidad que corresponde de igual manera toda la información que ustedes se manejan en el área de bienestar universitario que es una información muy confidencial y acuérdense que la ficha socioeconómica requiere datos personalísimos que son previos a la ficha ahora la ficha como tal de matrícula ustedes solo llenan los nombres del estudiante y el número de cédula, ahora esa información no se la provee a ninguna otra persona que no sea el estudiante o ya le dije o por orden judicial, pero no se la proporciona a ninguna parte de personal externo es el mismo estudiante el único que puede solicitar el certificado de matrícula esa es la confidencialidad que nosotros guardamos, ahora los sistemas como tal también están protegidos, los sistemas solo pueden ser solo pueden ser revisados y emitidos el certificado como tal de la misma forma que nosotros estamos indicando por el solicitante que en este caso es el estudiante o por orden judicial solamente por estas vías se dan las documentaciones de los estudiantes caso contrario no se emite ninguna información del estudiante ni número de cédula, ni nombres a ninguna persona externa eso si lo tenemos inclusive regulado no como una ley interna de tratamiento de datos personales sino como un manejo de información que maneja la UPSE al ser nosotros una institución pública todos los documentos e información interna que se maneje nosotros tenemos un reglamento que justamente para el tratamiento de entrega de este tipo de información y no se la proporciona a no ser que sea una información pública en todo caso la información los nombres de los estudiantes y los números de cédula no ser públicos no los proporcionamos solo a petición del parte.

Pregunta 3 ¿Qué protocolo o base normativa declara la obligatoriedad de la UPSE de requerir el consentimiento informado de los estudiantes para el tratamiento y uso de los datos personales?

Nosotros nos regimos por la ley de tratamiento de datos personales como ley interna nosotros no la hemos implementado todavía como un protocolo, pero el protocolo general que nosotros seguimos es la Ley Orgánica de Protección de Datos Personales con eso nosotros estamos trabajando y todos los lineamientos que aquí están establecidos se rigen por aquello en este momento ya los ha designado y así lo tenemos declarado ante la Senescyt ante el ministerio de telecomunicaciones que siempre nos solicita los responsables del tratamiento de datos personales entonces hasta ahora ya lo designó a los responsables para esta actividad y ellos son los encargados justamente de emitir el protocolo que imagino yo que ya están trabajando en el protocolo interno como tal pero mientras se establezca el protocolo nosotros nos regimos por la ley de protección de datos personales.

Pregunta 4 ¿Monitorea secretaria la implementación de medidas de seguridad en el manejo de datos personales?

Sí, nosotros como Secretaría General siempre estamos entregando o despachando la documentación que solicitan los estudiantes y al momento que ya observamos que dentro del récord académico o dentro del certificado de matrícula se emite una información que no corresponde inmediatamente se solicita mediante comunicación directa por oficio al vicerrectorado y a su vez a la dirección de TIC que esa información que no corresponde a información pública inmediatamente sea eliminada del récord académico, no sea eliminada, sea ocultada porque esa información no es pública. Solo la información pública es la que sale más, tanto es así que los estudiantes no tienen acceso a los libros de matrícula y el libro de matrícula solo se tramita a petición de oficio, mediante oficio, a petición de parte y solamente puede ser requerido por los directores de carreras, decanos o autoridades para fines académicos, entonces tiene que siempre exponerse el motivo por el cual se solicita esta información, por tanto, esa información siempre se mantiene reservada.

Pregunta 5 ¿Qué protocolo utilizan para proteger físicamente los documentos que contienen información personal?

Ya, nosotros hasta el momento tenemos aprobado el reglamento, como les dije, mediante protección de datos personales, como tal la UPSE todavía no ha implementado protocolos específicos como tales para protección de datos personales y hasta ahora nos manejamos con dos cosas, uno que son un documento de confidencialidad que se firma, que normalmente siempre las personas que manejamos o tratamos datos personales siempre estamos obligados a suscribir esos documentos de confidencialidad, en los cuales nosotros como servidores públicos nos obligamos, aparte de que la ley nos obliga, nosotros como la LOSEP nos obliga a que la información que se mantiene en la institución no puede ser expuesta ni entregada a cualquier persona nosotros manejamos documentos de confidencialidad, donde estamos obligados a mantener confidencialidad de los documentos que están bajo nuestra custodia y aparte de eso, mediante archivo, que es donde al final recae toda la información de toda la institución, si tenemos ya protocolos establecidos, ya está un reglamento para el manejo de archivos y hay un manual de procedimiento donde se establecen los lineamientos que sigue cada persona que requiere un documento institucional solo se remite estos documentos a petición de la unidad productora ¿Cuál es la unidad productora? Si es un documento que corresponde a Secretaría General, solo yo lo puedo solicitar, si es un documento que corresponde a Dirección Financiera y yo lo requiero, entonces tengo que hacer la vía correspondiente, enviar la petición al señor Rector y tengo que exponer los motivos por los cuales yo requiero esa información y que tienen que ser netamente institucionales para un trámite institucional y no se entrega esa documentación a ningún personal externo, a no ser que sea en el marco que establece la Ley para la Entrega de Información Pública, para esto, la persona solicitante debe llenar todos los requisitos que indique el motivo por el cual requiere la información en base a qué solicita esa información y para qué va a ser utilizada esa información entonces debe identificarse la persona, dar nombre, número de cédula y con base a aquello se le entrega la petición de la solicitante, normalmente la UPSE hace aquello, pero solamente lo hacemos por disposiciones de trámites judiciales ya sea la Fiscalía que nos solicite o el Consejo de la Judicatura o alguna institución externa como la FAE, las Fuerzas Armadas por algún trámite de los chicos, de allí el resto de peticiones que aquí se tramitan

son a petición de la parte interesada que normalmente es el estudiante, obviamente el estudiante al solicitar su propia información se le hace llegar la información correspondiente.

Análisis:

La entrevista con la Secretaria General de la UPSE, permite evidenciar la importancia de contar con un protocolo interno específico dentro de la universidad para el tratamiento de datos personales, mediante el cual se podría implementar medidas con prácticas orientadas a garantizar la confidencialidad y el acceso restringido a la información del estudiante, bajo capacitaciones semestrales y la coordinación conjunto con el área de TIC y el responsable designado del tratamiento de datos, donde se refleja una intención institucional de cumplir con la Ley Orgánica de Protección de Datos Personales.

En relación con el consentimiento informado, la secretaría confirma que los formularios de matrícula e inscripción ya cuentan con cláusulas de confidencialidad, especialmente en la ficha socioeconómica, lo que evidencia un manejo reservado de datos personales sensibles, aunque dicha confidencialidad se respaldaría contando con un protocolo formal que la sustente, también se constata que la secretaría monitorea la emisión de documentos como certificados de matrícula, y en caso de detectar información no pertinente, toma medidas en coordinación con otras áreas para corregirla, lo cual está alineado con los principios de minimización y control de acceso.

Respecto a la protección física de documentos, se utilizan reglamentos y manuales internos que limitan el acceso a los servidores que tiene cierto alcance a estos datos sensibles, por ellos es necesario la suscripción de documentos de confidencialidad por parte del personal que maneja los datos, en cumplimiento de la LOPDP y la LOSEP, aunque como se manifestó, la UPSE aún se encuentra en la creación de políticas, protocolos y mecanismo formales basados en el mejoramiento del manejo de datos personales; es importante destacar la existencia una estructura funcional que permite proteger la información personal de los estudiantes, sin embargo, resulta pertinente el fortalecimiento de este sistema mediante políticas internas más claras y procedimientos estandarizados, en concordancia con los principios de legalidad, finalidad y seguridad establecidos en la normativa vigente.

4.2 Verificación de la Idea a Defender

En relación con el presente trabajo de investigación y los datos obtenidos a través de encuestas aplicadas a los estudiantes de la Universidad Estatal Península de Santa Elena y entrevistas a funcionarios universitarios, así como una revisión exhaustiva de fuentes bibliográficas y normativas, se cumple la idea a defender planteada al inicio de la investigación: "La recepción de datos sensibles no se sujeta a mecanismos que garantizan el consentimiento informado en la recolección de datos personales de los estudiantes de la Universidad Estatal Península de Santa Elena."

Por tanto, se establece que, si bien la Universidad recolecta datos personales como parte de su gestión administrativa y académica, denotando la necesidad de protocolos adecuados y mecanismos claros que aseguren que dicha recolección se realice con el consentimiento libre, específico e informado, tal como lo exige la Ley Orgánica de Protección de Datos Personales. De acuerdo con lo investigado es menester fortalecer la política institucional formalizada que informe previamente a los estudiantes sobre los fines concretos del tratamiento de sus datos, a través de solicitudes del consentimiento mediante formatos estandarizados conforme a la ley.

Los resultados de las encuestas aplicadas a los estudiantes evidencian que una amplia mayoría desconoce cuál es el uso que se da a su información personal, asimismo refiere no ser consultada o informada explícitamente respecto a si consiente o no dicho tratamiento. La implementación futura de mecanismos efectivos para recabar el consentimiento descartaría la exposición de datos de los estudiantes o su uso indebido, y mejoraría la confianza institucional promoviendo un entorno de seguridad jurídica en el tratamiento de la información.

La legislación ecuatoriana, particularmente el artículo 10 de la LOPDP y el artículo 66 numeral 19 de la Constitución de la República del Ecuador, exige que los datos personales sean recolectados con fines lícitos, específicos y legítimos, y que el consentimiento del titular sea un requisito previo e indispensable, estos requisitos en la práctica de la UPSE, deben ser protocolizados en la recepción de datos.

CONCLUSIONES

Bajo el análisis de las respuestas emitidas por los estudiantes y el personal administrativo encargado de la protección de los datos personales de la universidad, se logra identificar la necesidad de fortalecer los mecanismos de control en relación al principio de finalidad estipulado en el artículo 10 inciso d) de la LOPDP, normativa la cual direcciona al correcto uso de estos datos sensibles para un solo fin.

No se observa uso indebido de datos personales de los estudiantes UPSE, sin embargo, el riesgo de no contar con medidas correctamente protocolizadas que promuevan el consentimiento informado es una necesidad latente ante la posible vulnerabilidad de la información personal.

La institución requiere una norma interna que oriente a los servidores encargados de custodiar los datos sensibles sobre el correcto tratamiento de dicha información, a fin de estandarizar las reglas de gestión de datos e impulsar una gestión responsable acorde a los principios de la protección de datos.

Adicionalmente se hace latente la necesidad de una cultura institucional en torno al correcto manejo de datos, la misma que puede generar deficiencias si no se cuentan con mecanismos y protocolos acordes a los datos sensibles que se son recolectados, sumado a la escasa concientización tanto de los estudiantes, maestrantes y sector administrativo, bajo el riesgo de que se genere un entorno en donde no se respete el derecho fundamental de la protección de datos.

RECOMENDACIONES

Es primordial que dentro de la Universidad Estatal Península de Santa Elena se implementen los mecanismos y protocolos enfocados en el principio de finalidad al momento de qué se realice la recolección de la información sensible de los estudiantes. Esta medida ayudaría a una mejora significativa en la recolección de datos personales, afianzando la relación de confidencialidad entre el estudiantado y la institución.

Se considera fundamental la implementación del consentimiento informado dentro de cualquier tipo de información que se recolecte, mediante el cual se le pueda manifestar al titular de los datos qué tipo información será recolectada y cual será su finalidad, este enfoque pedagógico, además de facilitar la comprensión, generaría una percepción de respeto institucional hacia los derechos del estudiante, permitiendo fortalecer el vínculo de confianza entre ambos.

Se recomienda que la universidad fortalezca sus mecanismos de control con un enfoque más estricto sobre los departamentos y entidades administrativas que tengan un alcance significativo en los datos personales de los estudiantes, a través de formatos, directrices y protocolos específicos basados en canales de información donde se notifiquen los usos institucionales de datos, especialmente cuando se traten con finalidades académicas, administrativas o investigativas, pues estas acciones no solo reflejarían cumplimiento normativo sino también una cultura de derechos informativos, en donde se garanticen la confidencialidad y seguridad de la información que se vaya a recaudar.

Es primordial que se fortalezca su política en el manejo de datos personales, incluyendo cláusulas de cesión de datos con explicación concreta del porqué, bajo qué acuerdos y con qué garantías se realiza tal acción, esto ayudaría a reducir la desconfianza y a blindar a la universidad frente a posibles responsabilidades futuras, además se sugiere la creación de un comité interno de protección de datos encargado de supervisar continuamente las prácticas que se desarrollen en base a la misma, asimismo implementando capacitaciones de conciencia sobre el uso responsable, correcto y seguro de la información dentro del entorno universitario.

BIBLIOGRAFÍA

- Agencia Española de Protección de Datos (AEPD). (2020). *Informe anual sobre la protección de datos personales en España*. Agencia Española de Protección de Datos.
- Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento No. 459, Quito, Ecuador.
- Asamblea Nacional. (2008). CONSTITUCIÓN. En A. NACIONAL, HABEAS DATA. QUITO.
- ASAMBLEA NACIONAL. (2023). REGLAMENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES.
- Bedrossian, L. (2001). *La ética en el tratamiento de datos personales: Teoría y práctica*. Editorial Jurídica Internacional.
- Oro Badia, Ramon. (s.f.). *La protección de datos*. Editorial UOC.
- Beauchamp, T. L., & Childress, J. F. (1999). *Principios de ética biomédica* (4ª ed.). Editorial McGraw-Hill Interamericana.
- Bertoni, E. (2020). *La protección de los datos personales en América Latina*. Editorial Jurídica Continental.
- Bonavides, P. (2008). Los derechos de cuarta generación: Democracia, información y pluralismo en la globalización política. *Revista Derechos Fundamentales y Justicia*, 12(1), 45–67.
- Cañete, G. (2012). *Protección de datos personales: Principios y prácticas*. Editorial Jurídica.
- Comisión Europea. (2018). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*. Diario Oficial de la Unión Europea. <https://eur-lex.europa.eu>
- Comisión Interamericana de Derechos Humanos (CIDH). (2016). *Informe sobre la protección de los derechos humanos en el contexto digital*. Organización de Estados Americanos (OEA).
- Ferrajoli, L. (2001). *Derecho y razón: Teoría del garantismo penal*. Editorial Trotta.

- Organización de las Naciones Unidas. (1948). *Declaración Universal de los Derechos Humanos*. Asamblea General de la ONU.
- Solove, D. J., & Schwartz, P. M. (2020). *La privacidad en la educación: Principios y prácticas en la protección de datos*. Oxford University Press.
- Thiel, P. (2020). *La protección de datos personales: Principios fundamentales y retos contemporáneos*. Editorial Jurídica Internacional.
- Vázquez Requena, A. (2019). *Ética y legislación en la protección de datos personales*. Editorial Jurídica Continental.
- Wikiwand. (s.f.). *Universidad Estatal Península de Santa Elena*.
https://www.wikiwand.com/es/Universidad_Estatal_Pen%C3%ADnsula_de_Santa_Elena
- Castillo, C., Gómez, V., & Martínez, A. (2014). *Universidad Estatal Península de Santa Elena*.
https://www.upse.edu.ec/images/2019/MODELO_EDUCATIVO_UPSE_2015-1.pdf
- Castillo Gallo, C., & Reyes Tomalá, B. (2015). *Guía Metodológica de Proyectos de Investigación Social*. UPSE. <https://doi.org/E> - ISBN 978-9942-8548-5-8.
- Revista Vistazo. (2025, enero 10). *Universidad Estatal Península de Santa Elena, comprometida con el crecimiento y la calidad académica*.
<https://www.vistazo.com/enfoque/calidad-educativa/2025-01-10-universidad-estatal-peninsula-santa-elena-crecimiento-calidad-academica-NN8593197>

ANEXOS

ANEXO 1 Evidencias Fotográficas

Ilustración 1 Entrevista, Ing. Fabricio Ramos Mgt. Director de Departamento De Tic



Ilustración 2 Entrevista, Lcda. Gisella Paula Chica, PhD. Vicerrectora de la Universidad Estatal Península de Santa Elena



Ilustración 3 Entrevista, Lic. Marlon Novillo, Mgt. Director de Departamento de Bienestar Estudiantil



Ilustración 4 Entrevista, Abg. María Rivera González, Mgt. Secretaria General





UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
CARRERA DE DERECHO
TRABAJO DE INTEGRACION CURRICULAR: PRINCIPIO DE
FINALIDAD EN LA PROTECCIÓN DE DATOS PERSONALES: CASO
ESTUDIANTES DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA
ELENA, 2024



INVESTIGADORES: CARLOS LUIS VERA YAGUAL Y NATHALY VALENTINA TORRES
HERRERA

ANEXO 2 CUESTIONARIO APLICADO A ESTUDIANTES DE LA UNIVERSIDAD
ESTATAL PENÍNSULA DE SANTA ELENA

OBJETIVO: Evaluar el nivel de conocimiento y percepción de los estudiantes sobre el tratamiento de sus datos personales por parte de la Universidad Estatal Península de Santa Elena, en relación con el principio de finalidad, así como su nivel de información, consentimiento y confianza respecto al uso que se da a dicha información en el ámbito institucional.

Estimado/a estudiante: Lea atentamente el siguiente cuestionario, que forma parte de una investigación sobre el uso de sus datos personales en la Universidad Estatal Península de Santa Elena. Marque con una "X" la opción que considere adecuada. Su participación es confidencial y de uso exclusivo para fines académicos.

1. ¿Conoce usted el objetivo y uso que la UPSE dará a los datos personales que entrega a la universidad?

SI

NO

2. ¿Conoce si sus datos han sido usados para otros fines?

SI

NO

3. ¿La universidad requirió su consentimiento antes de solicitar sus datos personales?

SI

NO

4. En caso de tener dudas sobre el uso de sus datos personales, ¿sabe usted con quién debe comunicarse dentro de la universidad?

Sí, con el Departamento de (TIC)

Sí, con la Secretaría General

Sí, con Bienestar Universitario

No

5. ¿Cuándo le han requerido datos personales, le ha dado la opción de rechazar ciertos usos o rechazar la entrega de sus datos personales?

SI

NO

6. ¿Cuándo la UPSE requiere de sus datos personales le solicitan algún tipo de autorización para que estos puedan ser compartidos con terceros?

SI

NO

7. ¿Cuándo la UPSE le solicita sus datos personales, se le informa claramente sobre los fines y objetivos de su uso, permitiéndole otorgar un consentimiento libre e informado?

SI

NO

8. ¿Ha sentido algún momento preocupación o zozobra respecto a la protección adecuada de los datos personales en la UPSE?

SI

NO

9. ¿Conoce si la universidad ha tomado medidas para prevenir filtraciones o mal uso de sus datos?

SI

NO

10. ¿Conoce de algún caso o casos en los que los datos personales de los estudiantes de la UPSE hayan sido expuestos generando situaciones de riesgo?

Sí, conozco uno o varios casos

He escuchado rumores

No, no conozco ningún caso

Agradecemos vuestra colaboración



UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
CARRERA DE DERECHO
TRABAJO DE INTEGRACION CURRICULAR: PRINCIPIO DE
FINALIDAD EN LA PROTECCIÓN DE DATOS PERSONALES: CASO
ESTUDIANTES DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA
ELENA, 2024



INVESTIGADORES: CARLOS LUIS VERA YAGUAL Y NATHALY VALENTINA TORRES
HERRERA

ANEXO 3 ENTREVISTA AL DEPARTAMENTO DE TIC DE LA UNIVERSIDAD
ESTATAL PENÍNSULA DE SANTA ELENA

OBJETIVO: Conocer los procedimientos, medidas técnicas y mecanismos implementados por el Departamento de TIC de la Universidad Estatal Península de Santa Elena para el tratamiento y resguardo de los datos personales de los estudiantes, en relación con el cumplimiento del principio de finalidad establecido en la normativa vigente.

Estimado funcionario: Sírvase dar lectura al presente cuestionario que permitirá profundizar aspectos relevantes en esta investigación.

1. **¿Cuál es la norma o política de protección de datos establecidos por la UPSE?**
2. **¿Dentro del protocolo de protección de datos, se permite al estudiante rechazar la entrega de ciertos datos?**
3. **¿Incluyen los sistemas digitales de la universidad avisos claros sobre el uso de los datos personales que recolectan?**
4. **¿Se exige el consentimiento digital del estudiante antes de ingresar su información en las plataformas institucionales?**
5. **¿Qué medidas de seguridad (como cifrado o autenticación) implementa el sistema para proteger los datos estudiantiles?**
6. **¿Cómo controla su departamento el acceso interno del personal a bases de datos estudiantiles?**

Agradecemos vuestra colaboración



**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
CARRERA DE DERECHO
TRABAJO DE INTEGRACION CURRICULAR: PRINCIPIO DE
FINALIDAD EN LA PROTECCIÓN DE DATOS PERSONALES: CASO
ESTUDIANTES DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA
ELENA, 2024**



INVESTIGADORES: CARLOS LUIS VERA YAGUAL Y NATHALY VALENTINA TORRES
HERRERA

**ANEXO 4 ENTREVISTA A LA VICERECTORA DE LA UNIVERSIDAD ESTATAL
PENÍNSULA DE SANTA ELENA**

OBJETIVO: Conocer la perspectiva institucional de la Vicerrectoría sobre las políticas, directrices y acciones adoptadas por la Universidad Estatal Península de Santa Elena en relación con el tratamiento de los datos personales de los estudiantes, y cómo estas se articulan con el cumplimiento del principio de finalidad establecido en la normativa vigente.

Estimado funcionario: Sírvase dar lectura al presente cuestionario que permitirá profundizar aspectos relevantes en esta investigación.

1. **¿Qué política de control ejecuta la institución para garantizar que los estudiantes sean informados sobre el tratamiento y uso de sus datos personales?**
2. **¿Qué protocolo o base normativa declara la obligatoriedad de la UPSE de requerir el consentimiento informado de los estudiantes para el tratamiento y uso de los datos personales?**
3. **¿Qué tipo de auditoria o controles ejecuta la institución como medidas de seguridad en el manejo de datos personales?**
4. **¿Se realizan auditorías o evaluaciones sobre posibles riesgos en el tratamiento de datos estudiantiles?**

Agradecemos vuestra colaboración



**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
CARRERA DE DERECHO
TRABAJO DE INTEGRACION CURRICULAR: PRINCIPIO DE
FINALIDAD EN LA PROTECCIÓN DE DATOS PERSONALES: CASO
ESTUDIANTES DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA
ELENA, 2024**



INVESTIGADORES: CARLOS LUIS VERA YAGUAL Y NATHALY VALENTINA TORRES
HERRERA

**ANEXO 5 ENTREVISTA AL DEPARTAMENTO DE BIENESTAR ESTUDIANTIL DE LA
UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA**

OBJETIVO: Identificar cómo el Departamento de Bienestar Estudiantil recopila, utiliza y comunica a los estudiantes los fines del tratamiento de sus datos personales, así como conocer si se garantiza su consentimiento informado, en el marco del principio de finalidad establecido en la normativa de protección de datos personales.

Estimado funcionario: Sírvase dar lectura al presente cuestionario que permitirá profundizar aspectos relevantes en esta investigación.

1. **¿Cómo garantiza el Departamento de Bienestar Estudiantil que la recopilación de datos personales de los estudiantes se realiza con su autorización expresa y previa comunicación sobre los fines específicos de su uso?**
2. **¿Solicitan consentimiento explícito antes de recopilar datos sensibles como la ficha socioeconómica?**
3. **¿Qué medidas aplican para resguardar la privacidad de la información confidencial del estudiante?**
4. **¿Quiénes tienen acceso autorizado a los expedientes de estudiantes dentro de esta unidad?**
5. **¿Qué protocolo utilizan para proteger físicamente los documentos que contienen información personal?**

Agradecemos vuestra colaboración



**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
CARRERA DE DERECHO
TRABAJO DE INTEGRACION CURRICULAR: PRINCIPIO DE
FINALIDAD EN LA PROTECCIÓN DE DATOS PERSONALES: CASO
ESTUDIANTES DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA
ELENA, 2024**



INVESTIGADORES: CARLOS LUIS VERA YAGUAL Y NATHALY VALENTINA TORRES
HERRERA

**ANEXO 6 ENTREVISTA A LA SECRETARIA GENERAL DE LA UNIVERSIDAD
ESTATAL PENÍNSULA DE SANTA ELENA**

OBJETIVO: Conocer el rol de la Secretaría General en la gestión, administración y resguardo de los datos personales de los estudiantes, así como los mecanismos institucionales para asegurar que dicho tratamiento cumpla con el principio de finalidad y con los lineamientos establecidos en la normativa vigente de protección de datos personales.

Estimado funcionario: Sírvase dar lectura al presente cuestionario que permitirá profundizar aspectos relevantes en esta investigación.

1. **¿Qué política de control ejecuta secretaria para garantizar que los estudiantes sean informados sobre el tratamiento y uso de sus datos personales?**
2. **¿Los formularios de inscripción o matrícula incluyen una cláusula de consentimiento informado?**
3. **¿Qué protocolo o base normativa declara la obligatoriedad de la UPSE de requerir el consentimiento informado de los estudiantes para el tratamiento y uso de los datos personales?**
4. **¿Monitorea secretaria la implementación de medidas de seguridad en el manejo de datos personales?**
5. **¿Qué protocolo utilizan para proteger físicamente los documentos que contienen información personal?**

Agradecemos vuestra colaboración