

# Análisis ético del manejo de datos personales en el contexto académico: Un estudio sobre la Universidad Técnica Estatal de Quevedo (UTEQ)

Shander Guanin<sup>1</sup>, Emerson Guerrero<sup>2</sup>, Diego Lucas<sup>3</sup>, Elkyn Mora<sup>4</sup>

Facultad de Ciencias de la Ingeniería  
Universidad Técnica Estatal de Quevedo

**Abstract**—Este estudio aborda los desafíos éticos en el manejo de datos personales dentro del contexto académico de la Universidad Técnica Estatal de Quevedo (UTEQ). Se analizan riesgos como la falta de transparencia en las plataformas institucionales y la posible vulneración de la privacidad de los usuarios. Además, se proponen lineamientos éticos que busquen garantizar la protección de los derechos de estudiantes, docentes y personal administrativo, fomentando prácticas responsables en el ámbito universitario.

## I. RESUMEN

El manejo de datos personales en las plataformas académicas y redes institucionales de la Universidad Técnica Estatal de Quevedo (UTEQ) plantea desafíos éticos cruciales en un entorno universitario digitalizado. Este estudio examina la necesidad de un marco ético que regule la gestión responsable de información personal, enfocado en principios como privacidad, seguridad y uso adecuado.

Se identifican riesgos como vulnerabilidades en plataformas institucionales, usos no autorizados de datos y falta de transparencia. El análisis subraya el rol de los responsables tecnológicos y administrativos para garantizar el cumplimiento de normativas y buenas prácticas éticas.

El enfoque de esta investigación no considera implementaciones técnicas, sino que propone lineamientos éticos que busquen equilibrar la eficiencia académica con la protección de los derechos de estudiantes, docentes y personal administrativo. Los principios fundamentales analizados incluyen privacidad, consentimiento informado y transparencia.

El marco teórico busca fomentar confianza en las plataformas académicas, proteger derechos fundamentales y promover buenas prácticas éticas. Este estudio contribuye al desarrollo de soluciones responsables que minimicen riesgos éticos y potencien un impacto positivo en la comunidad universitaria.

## II. INTRODUCCION

El avance de las tecnologías de la información y la comunicación (TIC) ha transformado radicalmente la gestión y el uso de los datos personales [1].

En un contexto global, los sistemas de información inteligentes y el Internet de las Cosas (IoT) ofrecen oportunidades para optimizar procesos, pero también generan preocupaciones éticas relacionadas con la privacidad, la vigilancia y el sesgo algorítmico [2].

En Ecuador, las infraestructuras de telecomunicaciones, reguladas por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), representan un sector clave. Sin embargo, el manejo de datos personales enfrenta retos significativos debido a la falta de directrices claras que garanticen su protección [3].

Villacís Almeida [4] subraya que los procesos para obtener títulos habilitantes en telecomunicaciones móviles, aunque técnicos y estructurados, requieren una consideración ética más profunda.

En el ámbito educativo, el uso masivo de plataformas digitales plantea desafíos particulares. Según un estudio reciente, las instituciones académicas enfrentan vulnerabilidades como el acceso no autorizado a datos sensibles [5]. Además, se ha identificado que la falta de consentimiento informado y la ausencia de transparencia en el tratamiento de la información representan riesgos adicionales en la gestión de datos académicos [6].

Estos problemas no solo afectan la confianza de los usuarios, sino que también pueden comprometer el cumplimiento de principios éticos fundamentales. Dado este panorama, instituciones como la UTEQ deben priorizar la implementación de marcos éticos robustos. Estos marcos deben considerar normativas locales e internacionales, como la Ley Orgánica de Protección de Datos Personales en Ecuador [3], para garantizar la privacidad, la seguridad y la integridad de los datos personales [7].

En este estudio se pretende analizar el manejo ético de los datos personales en las plataformas académicas y redes institucionales de la UTEQ. Además, pro-

pone lineamientos que busquen equilibrar la eficiencia académica con la protección de los derechos de estudiantes, docentes y personal administrativo, específicamente en lo que respecta a la privacidad, la confidencialidad, el acceso a la información y la autodeterminación informativa, fomentando un entorno digital confiable y sostenible.

El objetivo principal de este trabajo es analizar el manejo de datos personales en las plataformas académicas y redes institucionales de la UTEQ desde una perspectiva ética, identificando problemas actuales y proponiendo lineamientos éticos para su gestión responsable.

De esto se derivan varios objetivos específicos. En primer lugar, se busca generar conciencia sobre los derechos de protección de datos entre los miembros de la comunidad universitaria. Además, se pretende proveer recomendaciones para mejorar la transparencia y responsabilidad en la gestión de datos personales por parte de la UTEQ. Finalmente, se busca contribuir al diseño de políticas internas en la universidad que promuevan una gestión ética y segura de los datos personales.

### III. REVISIÓN DEL ESTADO DEL ARTE

La gestión ética de datos es fundamental para garantizar la transparencia, la protección de información sensible y el cumplimiento de normativas específicas. HogoNext [8] enfatiza la importancia de la rendición de cuentas en la toma de decisiones basadas en datos para prevenir sesgos y malas prácticas, un aspecto relevante en contextos como Ecuador, donde el desarrollo digital enfrenta desafíos éticos particulares en cuanto a privacidad y seguridad de la información.

La gobernanza ágil de datos permite la adaptación a un entorno digital en constante evolución. TM Forum [9] resalta que, en el contexto ecuatoriano, donde el acceso a servicios digitales está en crecimiento, es necesario un marco estándar que asegure la interoperabilidad y la eficiencia en la gestión de datos en tiempo real, equilibrando la innovación con la regulación.

En esta misma línea, el Banco Mundial [10] destaca que la interoperabilidad es un elemento clave para un sector público basado en datos, ya que facilita la comunicación eficiente entre sistemas y reduce las barreras entre instituciones al establecer estándares claros para el intercambio de información. Esto permite mejorar la calidad de los servicios digitales y fortalecer la confianza en la gestión de datos personales en entornos gubernamentales y académicos.

Desde una perspectiva más tecnológica, estudios como el de MDPI [11] subrayan la necesidad de integrar la ética, la gobernanza y tecnologías avanzadas como la inteligencia artificial (IA) y el aprendizaje automático (ML). Estas herramientas resultan clave para la gestión de datos en telecomunicaciones y educación, pero su implementación requiere un marco ético sólido

que priorice la sostenibilidad y la protección de los derechos de los usuarios.

En el ámbito educativo, diversas investigaciones abordan la importancia de la ética en la gestión de datos personales. Popa et al. [12] analizan cómo las universidades promueven una cultura de integridad académica mediante liderazgo ético y políticas de transparencia. De manera similar, Nkosi y Ncube [13] proponen un marco de privacidad de datos adaptado a instituciones de educación superior, destacando la importancia de mitigar riesgos éticos en el manejo de información sensible.

Otros estudios han abordado específicamente los desafíos de seguridad en entornos educativos digitales. Zhu y Huang [14] identifican riesgos administrativos y académicos en la protección de datos, enfatizando la necesidad de estrategias robustas de seguridad. Wright y Adams [15] examinan el impacto de las plataformas educativas en línea en la privacidad estudiantil, señalando la importancia de equilibrar la eficiencia tecnológica con el respeto a la privacidad individual.

Por otro lado, Campbell y Smith [16] destacan los retos en la gestión de datos abiertos y datos grises en las universidades, subrayando la necesidad de encontrar un equilibrio entre transparencia, privacidad y derechos de propiedad intelectual. De manera complementaria, Jones y Patel [17] aplican la teoría de la integridad contextual para evaluar los riesgos éticos en los sistemas de supervisión en línea utilizados en la educación superior.

Estos estudios reflejan un creciente interés en la gestión ética de datos en el ámbito educativo y tecnológico, resaltando la necesidad de marcos normativos que se adapten a contextos específicos y consideren tanto los avances tecnológicos como sus implicaciones sociales y legales.

### IV. MARCO ÉTICO UNIVERSITARIO

Este estudio busca contribuir al ámbito académico y ético mediante la propuesta de un marco ético para la gestión responsable de datos personales en contextos universitarios. Dicho marco se fundamenta en principios éticos esenciales, tales como la transparencia, el consentimiento informado, la privacidad y la rendición de cuentas, alineándose con normativas internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea [18], así como con normativas nacionales como la Ley Orgánica de Protección de Datos Personales en Ecuador [19].

A través del análisis de prácticas actuales en la UTEQ, este trabajo pretende identificar posibles riesgos asociados al manejo de datos personales en plataformas académicas y propone lineamientos que fomenten una cultura de responsabilidad y cumplimiento normativo en la gestión de información sensible.

El marco ético propuesto establece directrices teóricas y prácticas aplicables a entornos educativos, con el objetivo de fortalecer la confianza en los

sistemas institucionales, promover el respeto a los derechos digitales de la comunidad universitaria y garantizar un manejo seguro de la información en el ecosistema académico.

## V. METODOLOGÍA DE DESARROLLO

Este estudio analiza cómo la UTEQ maneja la información personal de estudiantes, docentes y personal administrativo, con el objetivo de identificar prácticas existentes, posibles áreas de mejora y los retos éticos asociados al manejo de dicha información en un entorno universitario.

### A. Diseño de la Investigación

La metodología utilizada en este estudio siguió un enfoque descriptivo y analítico. Inicialmente, se llevó a cabo una revisión de la normativa y las mejores prácticas en el manejo ético de datos personales, tomando como referencia marcos regulatorios nacionales e internacionales como la *Ley Orgánica de Protección de Datos Personales de Ecuador* y el *Reglamento General de Protección de Datos (GDPR)* de la Unión Europea [18]. Esta revisión permitió fundamentar las recomendaciones éticas propuestas en el marco del estudio.

### B. Desarrollo de los Modelos de Encuestas

Para recolectar datos, se diseñaron tres modelos de encuestas dirigidos a tres grupos clave: estudiantes, docentes y personal administrativo/técnico. Cada modelo fue desarrollado siguiendo las mejores prácticas recomendadas por plataformas como Qualtrics [20], adaptando las preguntas para abordar las particularidades de cada grupo. El diseño de las encuestas se basó en los siguientes criterios:

- **Preguntas:** Se emplearon principalmente preguntas cerradas utilizando escalas tipo Likert para medir el grado de acuerdo o percepción de los encuestados sobre diversos aspectos del manejo de datos personales en la universidad. Además, se incluyeron preguntas abiertas para recopilar opiniones cualitativas que permitieran comprender mejor las preocupaciones y sugerencias de los participantes sobre la protección de sus datos.
- **Validación:** Las preguntas fueron revisadas y validadas por un experto en ética de datos y tecnología, garantizando que cubrieran aspectos clave relacionados con la privacidad, la seguridad y el consentimiento informado.

### C. Distribución de las Encuestas

Las encuestas fueron distribuidas utilizando canales oficiales de la UTEQ, tales como correos electrónicos institucionales y grupos de comunicación interna en plataformas como WhatsApp. Este enfoque buscó asegurar una amplia participación y facilitar el acceso a

los encuestados de manera eficiente y centralizada. Se procuró mantener la confidencialidad y anonimato de los participantes, por lo que no se recolectaron datos personales identificables, como direcciones de correo electrónico.

### D. Recopilación y Análisis de Datos

Los datos obtenidos fueron procesados utilizando técnicas estadísticas descriptivas para analizar las respuestas a las preguntas cerradas. Se evaluaron frecuencias, tendencias y patrones en las respuestas de los participantes. En cuanto a las respuestas abiertas, se aplicó una categorización temática para identificar las principales preocupaciones y sugerencias respecto al manejo de los datos personales en la universidad.

### E. Ética en la Investigación

Para garantizar que el estudio se realizara de manera ética y respetuosa con los derechos de los participantes, se siguieron los principios establecidos por las normativas internacionales sobre protección de datos. Cada formulario de encuesta incluyó una declaración de consentimiento informado, en la cual se detallaban los objetivos del estudio y se aseguraba que la participación era completamente voluntaria. Además, se especificó que no se recopilarían datos sensibles y que los resultados serían utilizados exclusivamente con fines de investigación académica.

## VI. MARCO ÉTICO

La privacidad constituye uno de los pilares centrales en la administración de datos. Para salvaguardarla, toda recolección de información personal debe realizarse mediante un consentimiento libre e informado, explicando a los titulares de los datos tanto los fines específicos como el alcance y los posibles usos de su información [21]. En Ecuador, la *Ley Orgánica de Protección de Datos Personales* refuerza esta necesidad de claridad y transparencia, al establecer la adopción de medidas que garanticen la confidencialidad y la seguridad de la información [22]. Este enfoque promueve prácticas que no solo cumplen un requisito legal, sino que refuerzan la confianza de la comunidad universitaria en las plataformas de gestión académica.

En cuanto a la responsabilidad y la rendición de cuentas, se considera esencial que las instituciones asuman el compromiso permanente de cumplir con las regulaciones en materia de protección de datos. Este compromiso implica la existencia de protocolos formales ante eventuales brechas de seguridad, la realización de auditorías periódicas y la capacitación constante de aquellas personas encargadas de recolectar, procesar y resguardar la información [23]. La integración de estos elementos en la cultura organizacional universitaria garantiza que la toma de decisiones relacionadas con la información respete los principios

éticos y salvaguarde los derechos de todos los actores involucrados.

Al mismo tiempo, la gestión de datos personales requiere de total transparencia en sus métodos y propósitos. Tal transparencia implica comunicar de manera abierta y permanente el tratamiento que se otorga a la información, así como describir los mecanismos de protección implementados [24]. Esta práctica debe acompañarse de un esfuerzo por eliminar cualquier tipo de discriminación o sesgo en la interpretación de los datos, de modo que las decisiones institucionales no perjudiquen de forma injusta a ningún grupo de la comunidad universitaria. La combinación de transparencia y equidad fomenta un entorno donde la confianza y el respeto mutuo son valores fundamentales.

Desde la perspectiva internacional, el RGPD de la Unión Europea constituye uno de los principales referentes en materia de protección de la privacidad y salvaguarda de derechos. Aunque su aplicación directa se limita a los Estados miembros de la Unión Europea, sus lineamientos —como la necesidad de consentimiento expreso y la adopción de salvaguardas organizativas y tecnológicas— sirven como buenas prácticas que pueden extrapolarse a distintos contextos académicos [21]. Esta referencia internacional refuerza la importancia de integrar en las instituciones un marco robusto de actuación, aun cuando la normativa local posea características propias.

En la práctica, es necesario fortalecer la cultura de protección de datos a través de capacitaciones dirigidas a toda la comunidad universitaria, de tal forma que estudiantes, docentes y personal administrativo comprendan no solo sus derechos y obligaciones, sino también las implicaciones éticas del manejo de información personal. Asimismo, resulta fundamental disponer de políticas claras y públicas sobre el uso y la retención de datos, en las cuales se incluyan los derechos de acceso, rectificación, cancelación y oposición. El establecimiento de una figura como el Delegado de Protección de Datos, o de un comité especializado, contribuye a la evaluación y supervisión periódica del cumplimiento de la normativa y los principios éticos. De igual modo, la adopción de tecnologías de cifrado y la implementación de mecanismos de autenticación robustos reduce la probabilidad de vulneraciones o accesos no autorizados.

En síntesis, este marco ético se orienta a alinear la gestión de datos personales con los principios de responsabilidad, transparencia y respeto a la dignidad humana. Al robustecer los procedimientos y reforzar la comunicación interna sobre la protección de la información, se promueve un ambiente seguro que fortalece la confianza en las plataformas académicas y, al mismo tiempo, garantiza la tutela de los derechos de todos los integrantes de la vida universitaria.

## VII. RESULTADOS Y DISCUSIÓN

En esta sección se presentan los resultados obtenidos a partir de las encuestas realizadas a tres grupos clave: estudiantes, docentes y personal administrativo de la UTEQ. El análisis de estos datos permite identificar percepciones, desafíos y necesidades en relación con la gestión ética de los datos personales en el entorno académico.

### A. Resultados de la Encuesta al Área Administrativa y Técnica

La encuesta dirigida al personal administrativo y técnico permitió conocer su percepción sobre la seguridad y protección de datos personales dentro de la UTEQ. Se recopilaron **13 respuestas** en total, obteniendo los siguientes hallazgos más relevantes:

- **Autenticación de Dos Factores:** La mayoría de los encuestados, un **69.2%**, considera que la UTEQ cuenta con sistemas de autenticación de dos factores, mientras que una minoría, **30.8%**, no está segura sobre ello.

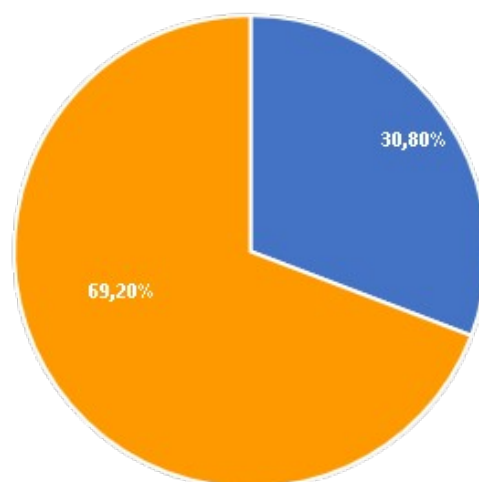


Fig. 1. Percepción del personal administrativo sobre la autenticación de dos factores en la UTEQ.

- **Frecuencia de Auditorías de Seguridad:** Una parte significativa de los encuestados cree que se realizan auditorías mensualmente, aunque una proporción aún mayor no está segura de su periodicidad (30.8% frente a 46.2%).

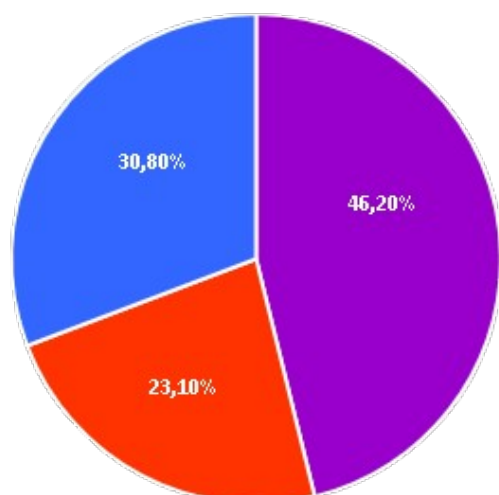


Fig. 2. Frecuencia con la que el personal administrativo percibe que se realizan auditorías de seguridad en la UTEQ.

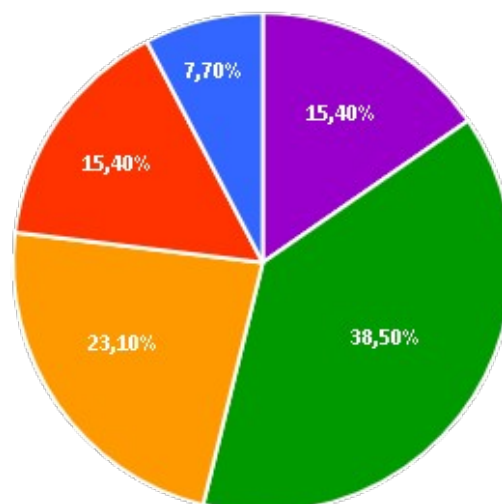


Fig. 4. Percepción sobre la capacitación en normativas de protección de datos para el personal administrativo y técnico.

- **Protocolos para Manejo de Incidentes:** La mayoría de los encuestados considera que existen protocolos adecuados para el manejo de incidentes de seguridad, aunque una proporción menor tiene dudas o no está de acuerdo con ello (69.2% frente a 15.4%).

- **Disponibilidad de Recursos Tecnológicos:** Más de la mitad de los encuestados considera que la UTEQ cuenta con recursos suficientes para garantizar la seguridad de los datos personales, mientras que una proporción menor mantiene una postura neutral (53.8% frente a 23.1%).

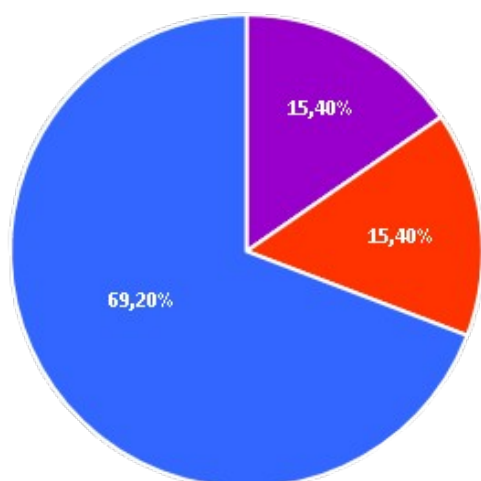


Fig. 3. Percepción sobre la existencia de protocolos adecuados para el manejo de incidentes de privacidad.

- **Capacitación en Normativas de Protección de Datos:** Una proporción significativa de los encuestados considera que la UTEQ ofrece capacitación periódica sobre normativas de protección de datos, aunque una parte menor duda de ello o está en desacuerdo (38.5% frente a 23.1% y 15.4%).

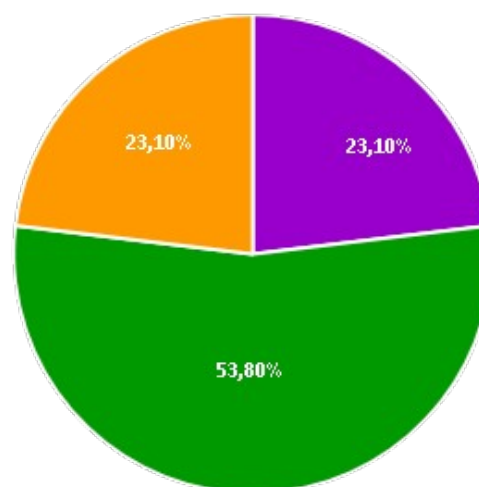


Fig. 5. Percepción sobre la disponibilidad de recursos tecnológicos en la UTEQ para la seguridad de datos.

**Discusión:** Los resultados reflejan que el personal administrativo percibe la existencia de medidas básicas de seguridad en la UTEQ, como la autenticación de dos factores y protocolos para el manejo de incidentes. Sin embargo, persisten dudas sobre la frecuencia de auditorías de seguridad y la capacitación en normativas de protección de datos. Además, aunque se reconoce la disponibilidad de recursos tecnológicos, no hay un consenso claro sobre su suficiencia. Estos hallazgos sugieren la necesidad de fortalecer la capacitación y

mejorar la comunicación interna sobre las medidas de protección de datos dentro de la institución.

### B. Resultados de la Encuesta a Docentes

Se recopilaron **11 respuestas** en total. A continuación, se presentan los principales hallazgos:

- **Seguridad en el Manejo de Datos Personales:**

La mayoría de los docentes considera que el manejo de los datos personales en las plataformas académicas de la UTEQ es seguro, aunque una pequeña proporción tiene una opinión neutral o lo percibe como poco seguro (81.8% frente a 9.1% y 9.1%).

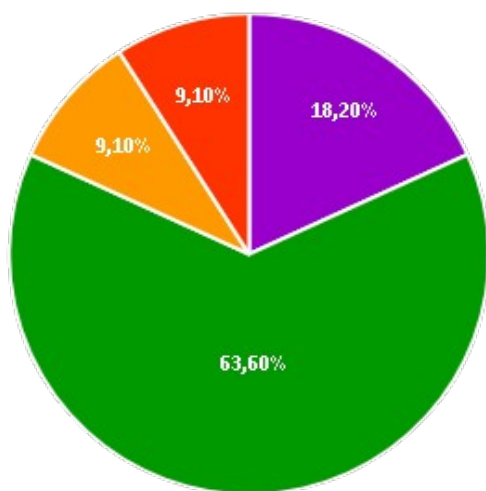


Fig. 6. Percepción de los docentes sobre la seguridad del manejo de datos personales en la UTEQ.

- **Capacitación sobre Protección de Datos:** Una mayoría de los docentes indicó no haber recibido capacitación en protección de datos personales en su rol docente, mientras que una proporción menor señaló haber recibido capacitación y otra mantuvo una postura neutral (63.6% frente a 18.2% y 9.1%).

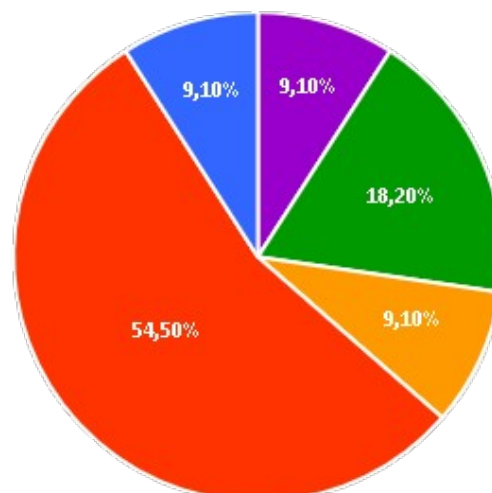


Fig. 7. Docentes que han recibido capacitación sobre protección de datos personales.

- **Preparación para Informar a los Estudiantes:**

Más de la mitad de los docentes se considera poco o nada preparado para informar a los estudiantes sobre la gestión de sus datos personales, mientras que una proporción menor mantiene una postura neutral y solo una pequeña fracción se siente bastante o totalmente preparado (54.6% frente a 36.4% y 9.1%).

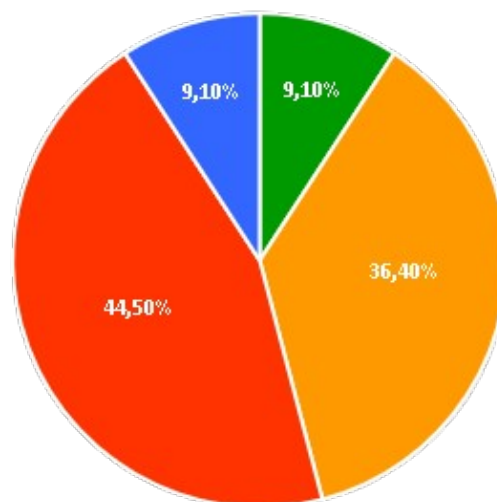


Fig. 8. Preparación de los docentes para informar a los estudiantes sobre la gestión de sus datos personales.

- **Conciencia de los Estudiantes sobre el Uso de Datos:** Más de la mitad de los docentes cree que los estudiantes son poco o nada conscientes sobre el manejo de sus datos personales en la universidad, mientras que una proporción cercana tiene una percepción neutral (54.6% frente a 45.5%).

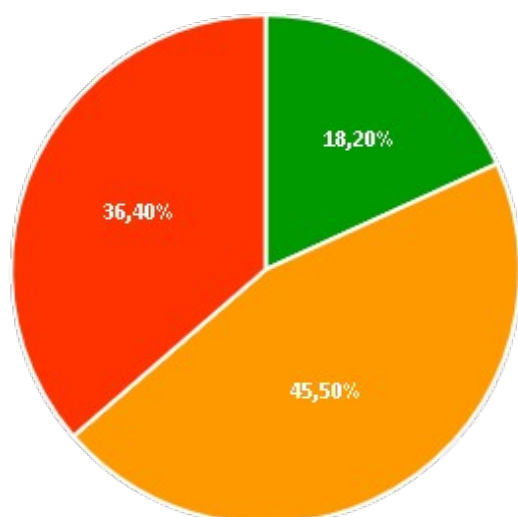


Fig. 9. Conciencia de los estudiantes sobre el uso de sus datos personales.

- **Implementación de Medidas Adicionales:** La gran mayoría de los docentes está de acuerdo en que se deben implementar medidas adicionales para garantizar la privacidad y seguridad de los datos personales (90.9%).

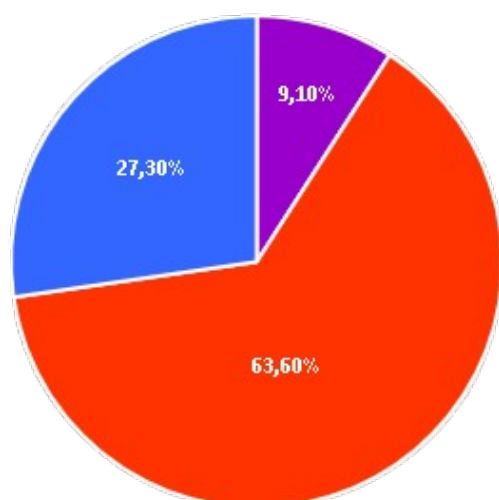


Fig. 10. Opinión de los docentes sobre la implementación de medidas adicionales para la seguridad de los datos personales.

**Discusión:** Los resultados muestran que la mayoría de los docentes confía en la seguridad de los datos en la UTEQ, aunque persisten preocupaciones. La falta de capacitación en protección de datos podría estar limitando su capacidad para orientar a los estudiantes en esta materia. Además, la baja percepción sobre la conciencia de los estudiantes respecto al manejo de sus datos y la necesidad de medidas adicionales resaltan la importancia de fortalecer la educación en ciberseguridad y actualizar las políticas institucionales.

### C. Resultados de la Encuesta a Estudiantes

Se recopilieron **132 respuestas** en total. A continuación, se presentan los principales hallazgos:

- **Seguridad en el Manejo de Datos Personales:**

La mayoría de los estudiantes considera que el uso de las plataformas académicas de la UTEQ en términos de protección de datos personales es seguro, mientras que una proporción significativa mantiene una postura neutral y una minoría lo considera poco seguro (68.9% frente a 25.8% y 5.1%).

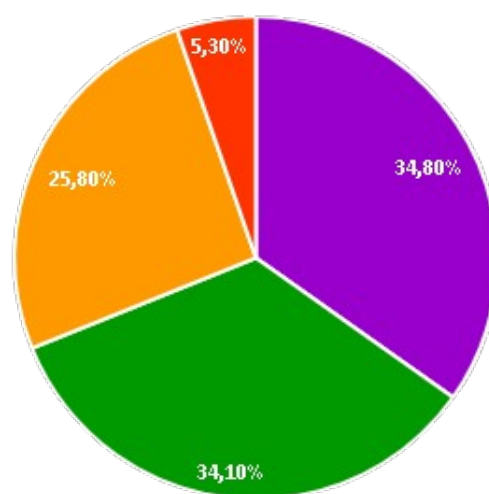


Fig. 11. Percepción de los estudiantes sobre la seguridad en el manejo de datos personales en la UTEQ.

- **Información sobre Manejo de Datos:** Menos de la mitad de los estudiantes considera que la UTEQ informa adecuadamente sobre el manejo de sus datos personales, mientras que una proporción significativa mantiene una postura neutral y una parte considerable está en desacuerdo (43.2% frente a 27.3% y 29.5%).



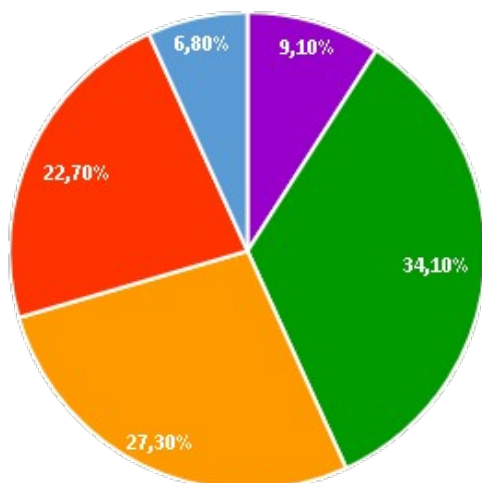


Fig. 12. Opinión de los estudiantes sobre la claridad en la información del manejo de datos personales.

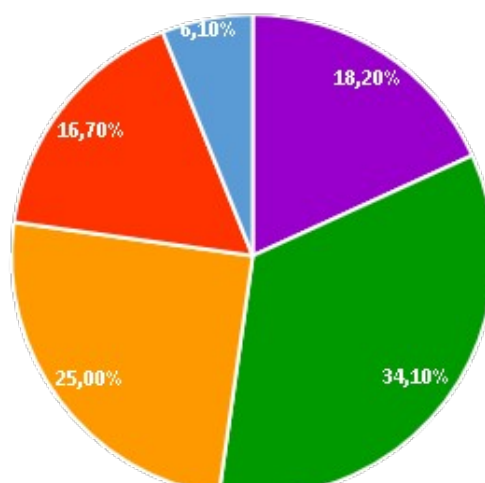


Fig. 14. Percepción de los estudiantes sobre las medidas de seguridad aplicadas en la UTEQ.

- **Problemas de Acceso o Uso No Autorizado de Datos:** La mayoría de los estudiantes afirma no haber experimentado problemas relacionados con el acceso o uso no autorizado de sus datos personales, mientras que una proporción menor menciona que casi nunca los ha tenido y una parte aún más pequeña ha tenido algún problema ocasionalmente (56.1% frente a 28% y 15.9%).

- **Claridad de la Política de Privacidad:** Menos de la mitad de los estudiantes considera clara la política de privacidad de las plataformas académicas, mientras que una proporción similar mantiene una postura neutral y otra parte la encuentra poco clara (42.5% frente a 23.5% y 23.5%).

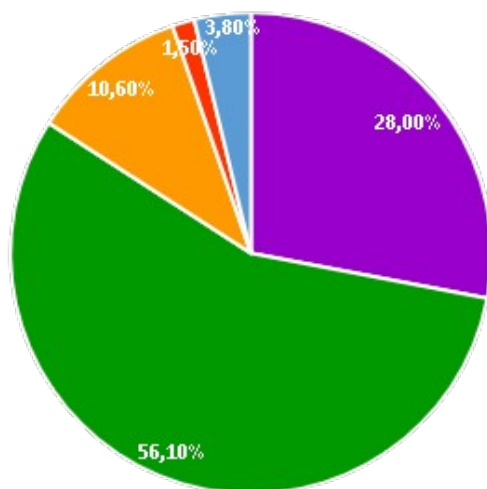


Fig. 13. Experiencias de los estudiantes con problemas de acceso o uso no autorizado de datos personales.

- **Uso de Medidas de Seguridad:** Más de la mitad de los estudiantes considera que la UTEQ aplica medidas de seguridad adecuadas, como autenticación de dos factores, mientras que una proporción menor mantiene una postura neutral y una parte significativa está en desacuerdo (52.3% frente a 25% y 22.9%).

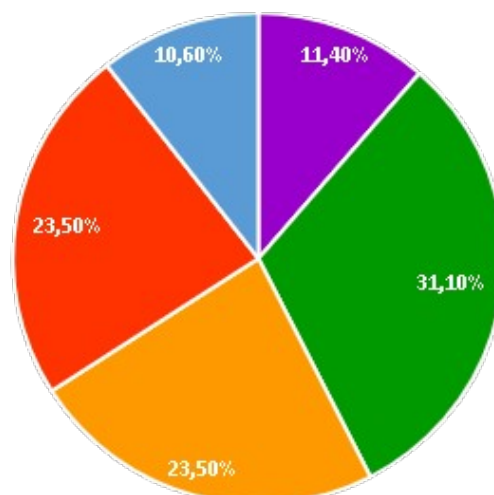


Fig. 15. Opinión de los estudiantes sobre la claridad de la política de privacidad.

- **Necesidad de Medidas Adicionales:** La gran mayoría de los estudiantes está de acuerdo en que la universidad debe implementar más medidas para proteger los datos personales (90.2%).



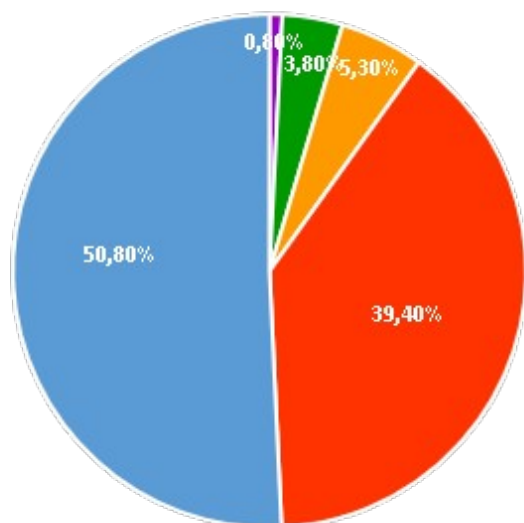


Fig. 16. Percepción de la necesidad de implementar más medidas de seguridad en la UTEQ.

- **Lectura de los Términos y Condiciones:** Casi la mitad de los estudiantes lee rara vez los términos y condiciones del Sistema de Gestión Académica (SGA) antes de usarlo, mientras que una proporción similar nunca lo hace (40.2% frente a 35.6%).

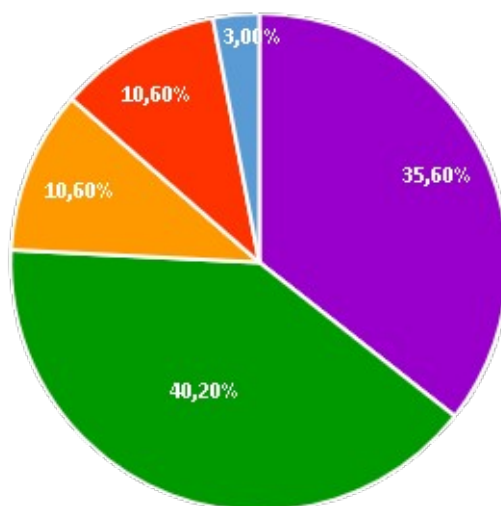


Fig. 17. Frecuencia con la que los estudiantes leen los términos y condiciones del SGA.

- **Posible Uso Indevido de Datos:** Una parte significativa de los estudiantes cree que sus datos personales podrían ser utilizados sin su consentimiento en las plataformas académicas, mientras que una proporción menor considera que esto no ocurriría (43.1% frente a 15.9%).

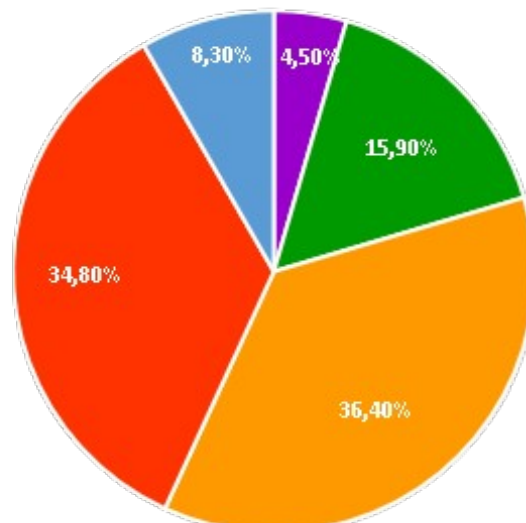


Fig. 18. Percepción de los estudiantes sobre el posible uso indebido de sus datos personales.

**Discusión:** Los resultados reflejan que, aunque la mayoría de los estudiantes confía en la seguridad de los datos en la UTEQ, un porcentaje significativo tiene dudas sobre el manejo de su información personal. La percepción de falta de claridad en la política de privacidad y el bajo porcentaje de estudiantes que leen los términos y condiciones evidencian la necesidad de estrategias de comunicación más efectivas. Además, la alta demanda de medidas adicionales de seguridad sugiere que aún hay espacio para mejorar la protección de los datos personales en la universidad.

#### D. Discusión General

Los resultados muestran una percepción variada sobre la gestión de datos personales en la UTEQ. Si bien existen medidas como autenticación de dos factores y protocolos de seguridad, la falta de información y capacitación genera incertidumbre en estudiantes, docentes y personal administrativo.

Uno de los principales problemas identificados es la deficiente comunicación institucional sobre la protección de datos. Aunque una parte significativa de los docentes (63.6%) y del personal administrativo (38.5%) ha señalado no haber recibido capacitación en normativas de protección de datos, muchos estudiantes (43.2%) consideran que la universidad no informa adecuadamente sobre el manejo de su información personal.

Desde la perspectiva de los estudiantes, aunque la mayoría (68.9%) percibe que sus datos están protegidos en las plataformas académicas, muchos consideran que las medidas de seguridad deberían reforzarse. Esta preocupación se ve reflejada en el temor de una parte considerable de los estudiantes (43.1%), que temen que sus datos puedan ser utilizados sin su consentimiento, lo que indica una falta de confianza en la gestión actual de la universidad.

En el ámbito administrativo, una parte del personal (46.2%) no tiene certeza sobre la frecuencia de las auditorías de seguridad, y aunque muchos (69.2%) reconocen la existencia de protocolos de seguridad, persisten dudas sobre su efectividad. Respecto a la infraestructura, una proporción significativa (53.8%) considera que la UTEQ dispone de los recursos adecuados, pero existe una creciente demanda por mejorar los sistemas de autenticación y encriptación de los datos sensibles.

En conclusión, la mejora en la transparencia en la gestión de datos, la implementación de auditorías más claras y la capacitación continua son fundamentales para fortalecer la confianza en los sistemas de información de la UTEQ. La comunidad universitaria exige mayores esfuerzos para garantizar la seguridad de los datos personales y una comunicación más efectiva sobre su tratamiento.

### E. Conclusiones Generales

Los resultados evidencian que, aunque la UTEQ ha implementado medidas para la protección de datos personales, persisten desafíos en capacitación, transparencia y aplicación de normativas. Para fortalecer la confianza en la gestión de datos, se recomienda:

- 1) Implementar **capacitaciones periódicas y accesibles** para docentes, estudiantes y personal administrativo, asegurando su comprensión sobre la protección de datos.
- 2) Garantizar una **mayor transparencia** en la gestión de datos, incluyendo la comunicación clara de políticas, procedimientos y auditorías de seguridad.
- 3) Revisar y fortalecer los **protocolos de seguridad**, priorizando la encriptación de datos sensibles y la autenticación avanzada.
- 4) Designar un **Delegado de Protección de Datos** encargado de supervisar el cumplimiento de normativas y atender inquietudes de la comunidad universitaria.

La implementación de estas medidas permitirá a la UTEQ mejorar la protección de los datos personales, fortalecer la confianza institucional y garantizar una gestión de información más segura y ética.

## VIII. ANEXOS

### A. Modelo de Encuesta para Estudiantes

A continuación se presentan las preguntas diseñadas para estudiantes, enfocadas en su percepción sobre la seguridad de sus datos personales:

- ¿Qué tan seguro(a) te sientes al utilizar las plataformas académicas de la UTEQ en términos de protección de tus datos personales?
- ¿Consideras que la UTEQ informa adecuadamente sobre cómo se manejan tus datos personales?
- ¿Alguna vez has experimentado problemas relacionados con el acceso o uso no autorizado de tus datos personales, ya sea en general o dentro de la UTEQ?
- ¿Crees que la UTEQ utiliza medidas de seguridad específicas, como autenticación de dos factores, para proteger el acceso a los datos personales?
- ¿Qué tan clara consideras la política de privacidad de las plataformas académicas que utilizas?
- ¿Crees que la universidad debería implementar más medidas para proteger los datos personales?
- ¿Con qué frecuencia lees los términos y condiciones del Sistema de Gestión Académica (SGA) de la UTEQ antes de utilizarlo?
- ¿Consideras que tus datos personales podrían ser utilizados sin tu consentimiento en las plataformas académicas?
- ¿Crees que el manejo ético de tus datos personales influye sobre la confianza hacia las plataformas académicas?
- ¿Qué medidas recomendarías para mejorar la seguridad de tus datos personales en las plataformas académicas? (Opcional)

### B. Modelo de Encuesta para Docentes

Las preguntas para docentes están enfocadas en su conocimiento y percepción sobre la gestión ética de datos personales:

- ¿Qué tan seguro(a) considera que es el manejo de los datos personales en las plataformas académicas de la UTEQ?
- ¿Ha recibido alguna capacitación o información sobre la protección de datos personales en su rol docente?
- ¿Cree que las plataformas académicas cumplen con principios éticos en la gestión de datos personales?
- ¿Se siente capacitado(a) para informar a los estudiantes sobre cómo se gestionan sus datos personales?
- ¿Considera que los estudiantes son conscientes de cómo se utilizan sus datos personales?
- ¿Qué tan claro(a) considera que es el reglamento institucional sobre la protección de datos personales?

- ¿Está de acuerdo con implementar medidas adicionales para garantizar la privacidad y seguridad de los datos?
- ¿Qué tan efectivo(a) considera que es el sistema actual de seguridad de las plataformas académicas?
- ¿Alguna vez ha tenido dudas o preocupaciones sobre cómo la universidad gestiona los datos personales?
- ¿Qué sugerencias tiene para mejorar la gestión ética de los datos personales en la UTEQ? (Pregunta abierta).

### C. Modelo de Encuesta para Personal Administrativo/Técnico

Las preguntas dirigidas al personal administrativo y técnico se centran en las prácticas actuales y los retos relacionados con la seguridad de datos personales:

- ¿La UTEQ cuenta con sistemas de autenticación de dos factores para proteger el acceso a las plataformas académicas?
- ¿Con qué frecuencia se realizan auditorías de seguridad en las plataformas institucionales?
- ¿Considera que las políticas de protección de datos personales están alineadas con las normativas locales e internacionales?
- ¿Existen protocolos establecidos para manejar incidentes relacionados con la privacidad de los datos personales?
- ¿Qué tan efectivos considera los mecanismos actuales de protección de datos implementados en la universidad?
- ¿Se realiza capacitación periódica sobre normativas de protección de datos para el personal administrativo y técnico?
- ¿Qué nivel de encriptación considera que se implementa para proteger la información sensible en las plataformas institucionales?
- ¿Considera que los usuarios finales de las plataformas son informados adecuadamente sobre las medidas de seguridad implementadas?
- ¿La universidad cuenta con recursos tecnológicos suficientes para garantizar la seguridad de los datos personales?
- ¿Qué retos considera que enfrenta la universidad en la gestión y protección de los datos personales? (Pregunta abierta).

### REFERENCES

- [1] A. Josephina and A. Andreas, "Case study: The internet of things and ethics," *The ORBIT Journal*, vol. 2, no. 2, pp. 1–29, 2019. DOI: 10.29297/ORBIT.V2I2.111.
- [2] M. Ryan, J. Antoniou, L. Brooks, *et al.*, "The ethical balance of using smart information systems for promoting the united nations' sustainable development goals," *Sustainability*, vol. 12, no. 12, p. 4826, 2020. DOI: 10.3390/SU12124826.
- [3] G. del Ecuador, *Ley orgánica de protección de datos personales*, Último acceso: Enero 2025, 2021. [Online]. Available: [https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley\\_organica\\_de\\_proteccion\\_de\\_datos\\_personales.pdf](https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf).
- [4] V. K. Villacís Almeida, *Tutorial para obtener en ecuador títulos habilitantes de registro para proveer el servicio de telecomunicaciones móviles por satélite: Revisión de la ley orgánica de telecomunicaciones, sus reglamentos y reformas, y estudio de los requisitos para la obtención de títulos habilitantes de registro en ecuador para proveer el servicio de telecomunicaciones móviles por satélite; elaboración de un ejemplo para la obtención de este título habilitante de registro y del respectivo tutorial*, Disponible en: <https://bibdigital.epn.edu.ec/handle/15000/25185>, 2023.
- [5] I. MQR, "Protección de datos personales en plataformas educativas digitales en el sistema de educación superior de ecuador," *Revista MQR*, 2024, Último acceso: Enero 2025. [Online]. Available: <https://investigarmqr.org/ojs/index.php/mqr/article/view/1760>.
- [6] U. Hemisferios, *Manual de capacitación en protección de datos personales*, Último acceso: Enero 2025, 2023. [Online]. Available: <https://www.uhemisferios.edu.ec/wp-content/uploads/2023/06/manual-capacitacion-proteccion-datos.pdf>.
- [7] F. C. y Desarrollo, *Guía de protección de datos personales en ecuador*, Último acceso: Enero 2025, 2023. [Online]. Available: <https://www.ciudadaniaydesarrollo.org/publicaciones/datos-personales/>.
- [8] Hogonext. "How to address ethical considerations in data analysis." Last accessed: December 25, 2024. (2024), [Online]. Available: <https://hogonext.com/how-to-address-ethical-considerations-in-data-analysis/>.
- [9] D. Bushaus. "Telecoms needs a standardized agile data governance framework." Last accessed: December 25, 2024. (2021), [Online]. Available: <https://inform.tmforum.org/features-and-opinion/telecoms-needs-a-standardized-agile-data-governance-framework>.

- [10] W. Bank, *Interoperability: Towards a data-driven public sector*, Accessed: 2025-02-26, 2023. [Online]. Available: <https://hdl.handle.net/10986/38520>.
- [11] L. Zhou, A. Smith, and R. Johnson, "Ai ethics in practice: Impact and challenges," *AI*, vol. 4, no. 3, p. 24, 2023, Last accessed: December 25, 2024. [Online]. Available: <https://www.mdpi.com/2624-800X/4/3/24>.
- [12] F. Popa, E. Barna, and C. N. Ciocoiu, "Ethical universities of integrity and ethics management in the romanian university environment," *Journal of Applied Ethics and Management*, vol. 14, no. 1, pp. 45–67, 2023. DOI: 10.1016/j.jam.2023.01.002.
- [13] L. Nkosi and C. Ncube, "A systematic literature review: Towards developing a data privacy framework for south african higher education institutions," *Computers & Security*, vol. 120, pp. 1–18, 2023. DOI: 10.1016/j.cose.2023.102803.
- [14] W. Zhu and P. Huang, "Information security at higher education institutions: A systematic literature review," *Journal of Information Technology & Education*, vol. 19, pp. 205–229, 2023. DOI: 10.1234/jite.2023.002001.
- [15] T. Wright and J. Adams, "Online student privacy in higher education: A systematic review of the research," *Journal of Educational Technology*, vol. 18, pp. 72–94, 2023. DOI: 10.1080/17439884.2023.1234567.
- [16] K. Campbell and A. Smith, "Open data, grey data, and stewardship: Universities at the privacy frontier," *Data Privacy in Academia*, vol. 22, no. 3, pp. 54–78, 2023. DOI: 10.1016/j.datap.2023.01.004.
- [17] E. Jones and R. Patel, "Privacy as contextual integrity in online proctoring systems in higher education: A scoping review," *Journal of Academic Ethics*, vol. 21, no. 2, pp. 113–138, 2023. DOI: 10.1007/s10805-023-09456-7.
- [18] U. Europea, *Reglamento (ue) 2016/679 del parlamento europeo y del consejo*, Reglamento General de Protección de Datos (GDPR), Accedido: 2025-03-21, 2016. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- [19] Asamblea Nacional del Ecuador, *Ley orgánica de protección de datos personales*, Última consulta: 21 de marzo de 2025, 2021. [Online]. Available: <https://www.asambleanacional.gob.ec/>.
- [20] Q. Blog. "Ethical issues for online surveys." Last accessed: December 25, 2024. (2024), [Online]. Available: <https://www.qualtrics.com/blog/ethical-issues-for-online-surveys/>.
- [21] M. Ryan, J. Antoniou, L. Brooks, and et al., "The ethical balance of using smart information systems for promoting the united nations' sustainable development goals," *Sustainability*, vol. 12, no. 12, p. 4826, 2020. DOI: 10.3390/su12124826.
- [22] Asamblea Nacional del Ecuador, *Ley orgánica de protección de datos personales*, Última consulta: 21 de marzo de 2025, 2021. [Online]. Available: <https://www.asambleanacional.gob.ec/>.
- [23] L. Nkosi and C. Ncube, "A systematic literature review: Towards developing a data privacy framework for south african higher education institutions," *Computers & Security*, vol. 120, pp. 1–18, 2023. DOI: 10.1016/j.cose.2023.102803.
- [24] F. Popa, E. Barna, and C. N. Ciocoiu, "Ethical universities of integrity and ethics management in the romanian university environment," *Journal of Applied Ethics and Management*, vol. 14, no. 1, pp. 45–67, 2023. DOI: 10.1016/j.jam.2023.01.002.