Noesis. Revista Electrónica de Investigación
Año 7. Vol 7. N°2. Edición Especial II. 2025
Hecho el depósito de Ley: FA2019000060
ISSN: 2739-0365
INSTITUTO DE INVESTIGACIÓN Y ESTUDIOS AVANZADOS KOINONIA (IIEAK).
Santa Ana de Coro. Venezuela.

DOI 10.35381/noesisin.v7i2.617

Medidas de seguridad para la protección de datos de estudiantes y exestudiantes de Uniandes

Security measures for the protection of data belonging to current and former students of Uniandes

Estefania Monserrath Constante-Mariño
da.estefaniamcm66@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0009-0001-9251-1910

Gladis Margo Proaño-Reyes
posgrado@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0000-0003-1653-5889

Fernando de Jesús Castro-Sánchez
fernandodcs.ainv@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0000-0003-3937-8142

Recibido: 15 de abril 2025
Revisado: 15 de mayo 2025
Aprobado: 15 de julio 2025
Publicado: 01 de agosto 2025

Noesis. Revista Electrónica de Investigación
Año 7. Vol 7. N°2. Edición Especial II. 2025
Hecho el depósito de Ley: FA2019000060
ISSN: 2739-0365
INSTITUTO DE INVESTIGACIÓN Y ESTUDIOS AVANZADOS KOINONIA (IIEAK).
Santa Ana de Coro. Venezuela.

RESUMEN

Este artículo tiene como objetivo proponer medidas necesarias para garantizar una mayor protección de los datos sensibles de los estudiantes y ex estudiantes de Uniandes, abordando las crecientes preocupaciones sobre la privacidad y la seguridad de la información en el entorno académico. Utilizando una metodología cuali-cuantitativa que combina entrevistas con expertos en seguridad y encuestas a la comunidad universitaria, identifica las principales amenazas: accesos no autorizados, ciberataques y brechas en los sistemas. A partir de este análisis, se proponen medidas concretas como la implementación de controles de acceso más estrictos y el desarrollo de programas de concienciación en seguridad de la información. Estas acciones buscan mejorar la integridad, confidencialidad y disponibilidad de los datos, reduciendo riesgos de violaciones y fortaleciendo la confianza en la gestión de información sensible por parte de la universidad.

Descriptores: Protección de datos sensibles; seguridad de la información; entorno académico; Uniandes. (Tesauro UNESCO).

ABSTRACT

This article aims to propose necessary measures to ensure greater protection of sensitive data belonging to current and former Uniandes students, addressing growing concerns about privacy and information security in the academic environment. Using a qualitative-quantitative methodology that combines interviews with security experts and surveys of the university community, it identifies the main threats: unauthorized access, cyberattacks, and system breaches. Based on this analysis, specific measures are proposed, such as the implementation of stricter access controls and the development of information security awareness programs. These actions seek to improve the integrity, confidentiality, and availability of data, reducing the risk of breaches and strengthening confidence in the university's management of sensitive information.

Descriptors: Protection of sensitive data; information security; academic environment; Uniandes. (UNESCO Thesaurus).

INTRODUCCIÓN

Conforme el derecho desarrolla la protección de datos personales ha cobrado una importancia en los últimos tiempos incorporándose en la legislación nacional exigencias y sancionándose inobservancias, el ámbito educativo superior no ha quedado fuera, las universidades públicas como privadas, a diario almacenan datos con información sensible de estudiantes quienes una vez egresados se mantienen en calidad de exestudiantes.

La Universidad Regional Autónoma de los Andes (UNIANDES) no es ajena a esta realidad, desde su creación en el año 1997 recopila datos relacionados a información académica, datos biométricos, datos sensibles; cuya obtención ha sido de forma rutinaria sin que medie una aceptación de condiciones o autorización hacia la universidad para que ésta almacene, utilice o cuide de esta información.

En los últimos años el sistema de educación superior aún no ha implementado un serio proceso para la seguridad en la protección de datos, algunas instituciones se han limitado a establecer pequeñas políticas o instructivos basados en la Ley Orgánica de Protección de Datos. Sin embargo, tanto en la Ley de Educación Superior (LOES) como el reglamento de régimen académico, no existe ninguna reforma o normativa que regule como tal la protección de datos de los estudiantes y ex estudiantes. Los estudiantes al acceder a la Universidad desde el momento de su inscripción entregan datos personales a través de plataformas tecnológicas y la mayoría desconoce el destino de esa información de esa forma existen miles de datos de estudiantes y exestudiantes que permanecen en estado pasivo. Estudios recientes muestran que la percepción de riesgo y la confianza son determinantes para que los estudiantes acepten plataformas de aprendizaje en línea (Jiang et al., 2022).

Por tanto al hablar sobre la protección de los datos personales de los estudiantes y ex estudiantes, la universidad debería implementar un sistema impermeable con el manejo de los datos sensibles de cada estudiante que al utilizar herramientas que la universidad otorga en especial ahora con el auge de la educación en línea, que desde la última

pandemia que sufrió la humanidad ha servido como una herramienta fundamental para la educación continua, aplicaciones y dispositivos para que los estudiantes realicen sus actividades académicas, la institución educativa debe priorizar la implementación de medidas de seguridad destinadas a salvaguardar la información personal de sus estudiantes, asegurándose así de cumplir con lo establecido en la normativa legal relacionada con la protección de datos personales.

La Ley Orgánica de Protección de Datos (LOPD, 2021) en su artículo 4, inciso 10, define que los datos sensibles se refieren a información relacionada con la etnia, la identidad de género, la identidad cultural, la religión, las creencias, la afiliación política, el historial judicial, la situación migratoria, la orientación sexual, la salud, así como datos biométricos y genéticos. Además, incluye aquellos datos cuyo manejo inapropiado podría dar lugar a discriminación o provocar atentados contra los derechos y libertades fundamentales, en consonancia con lo estipulado en la Constitución de la República y en convenios internacionales.

Las medidas de seguridad adoptadas por las instituciones educativas han evolucionado considerablemente en respuesta a las crecientes amenazas cibernéticas. Sin embargo, estudios recientes indican que aún existen brechas significativas en la implementación de políticas de seguridad robustas, lo que expone a los datos a posibles violaciones y usos no autorizados

Torres (2022), se señala que los datos sensibles se consideran como información que identifica a una persona de una manera más personal, es decir, datos personales de naturaleza privada y de su ámbito más íntimo. Por esta razón, su acceso y distribución deben estar limitados y restringidos a aquellas personas que no cuentan con la autorización para manejarlos.

Atendiendo al criterio de Brunet (2020), la protección de datos es un derecho fundamental del ser humano, clasificado como un derecho de nueva generación que forma parte de lo que la doctrina denomina la cuarta generación de derechos humanos. Este derecho está

íntimamente vinculado al desarrollo de las nuevas tecnologías, la globalización, la libertad de expresión en línea y la circulación libre de información.

Para Ortiz (2018), el derecho a la protección de datos abarca un espectro más amplio que el derecho a la intimidad, ya que no se limita únicamente a la protección de la intimidad garantizada constitucionalmente en el artículo 18. Según el Tribunal Constitucional, también abarca la esfera de los bienes de la personalidad relacionados con la vida privada, que incluyen el respeto a la dignidad, el derecho al honor y el pleno ejercicio de los derechos personales. Sin embargo, su protección no abarca cualquier información que pueda ser relevante para el ejercicio de un derecho, ya sea que esté relacionada o no con el honor, la ideología, la vida íntima personal y familiar, u otros derechos protegidos por la constitución.

Se puede mencionar que la protección de datos es un aspecto fundamental en la era digital, ya que garantiza la privacidad y la seguridad de la información personal. Con el aumento continuo de la cantidad de datos que se generan y recopilan cada día, es esencial que tanto las instituciones públicas como privadas adopten medidas adecuadas para proteger la información de las personas que hacen parte de las distintas instituciones sociales, incluidas las instituciones educativas (Roldán, 2021).

La norma ISO/IEC 27002 es una referencia clave en el ámbito de la gestión de la seguridad de la información. Esta norma proporciona un marco de buenas prácticas y controles de seguridad que son aplicables a cualquier tipo de organización, incluyendo las instituciones de educación superior (International Organization for Standardization [ISO], 2022). Al aplicar la ISO 27002, estas instituciones pueden establecer un enfoque sistemático para proteger los datos sensibles, mitigando riesgos de seguridad y cumpliendo con las normativas locales e internacionales de protección de datos, lo que, a su vez, fortalece la confianza de estudiantes y partes interesadas (Rodríguez y López, 2023).

La implementación de la norma ISO 27002 no solo se alinea con el cumplimiento

normativo, sino que también representa una estrategia fundamental para salvaguardar los activos de información y mantener la confianza en la capacidad de las universidades para gestionar de manera segura los datos que manejan (Martínez et al., 2024).

A partir del conjunto de ideas anteriormente desarrolladas, la presente investigación se indaga sobre las posibles medidas de seguridad que se pueden implementar en la Universidad Regional Autónoma de los Andes, como institución parte del Sistema de Educación Superior ecuatoriano, para la protección de los datos sensibles de estudiantes y ex estudiantes, con el fin de identificar vías que fortalezcan la seguridad de la información en la institución. A tono con esto, se formulan el problema de investigación y objetivo general.

Al hablar de protección de datos en las instituciones de educación superior se cita también de la norma ISO 30301 la cual presenta como una guía clave para la implementación de sistemas de gestión de documentos, asegurando un control adecuado sobre los registros y el cumplimiento de los requisitos legales y regulatorios en materia de protección de datos. La norma ISO 30301 proporciona un marco para instituir, implementar y mejorar continuamente un sistema de gestión de documentos que permita a las organizaciones cumplir con sus obligaciones legales, mejorar la eficiencia operativa y gestionar adecuadamente la información a lo largo de su ciclo de vida (International Organization for Standardization [ISO], 2021). En el ámbito de la educación superior, la adopción de esta norma no solo contribuye a la protección de datos personales y académicos, sino que también promueve una gestión más eficiente de los procesos institucionales, reduciendo riesgos asociados con la pérdida o el mal uso de información crítica (Martínez y Ramírez, 2023).

La adopción de un sistema de gestión documental basado en la norma ISO 30301 permite a las universidades garantizar que los datos sensibles de estudiantes, ex estudiantes sean gestionados de acuerdo con las regulaciones actuales, a partir de la Ley General de Protección de Datos Personales en Ecuador.

MÉTODO

La presente investigación tuvo un enfoque mixto, cuali-cuantitativo. Por una parte, se sometió a caracterización y análisis a una relación de procesos institucionales, la protección de datos sensibles de estudiantes y ex estudiantes y las medidas para fortalecer su seguridad. En el caso de la condición cuantitativa se explicó porque se aplicarán encuestas a un grupo especifico de estudiantes y ex estudiantes de Universidad Regional Autónoma de los Andes (UNIANDES) para recabar información diagnóstica que apoye las valoraciones de fortalezas y debilidades y las correspondientes propuestas. Por tanto, la integración de ambos enfoques permitió obtener información directa de los participantes y evaluar su percepción, conocimiento y experiencia en relación con las prácticas de seguridad implementadas por la universidad.

Se utilizo métodos de los niveles teórico y empírico del conocimiento. En el caso de los métodos teóricos, son fundamentales el análisis y la síntesis y en enfoque en sistema, para el procesamiento de la doctrina y la sistematización de conceptos relacionados con las variables de estudio. Por su parte, el método de análisis documental, propiamente de carácter empírico, se da prioridad a la revisión y valoración de la documentación informativa y normativa sobre el objeto de estudio.

Las técnicas e instrumentos de investigación que se utilizaron fueron las encuestas y entrevistas, para ello se realizaron entrevistas a 4 especialistas en recolección de datos de estudiantes y ex estudiantes de la Universidad Uniandes, al igual que una encuesta que incluyó la aplicación de cuestionarios a 25 estudiantes y 25 ex estudiantes de UNIANDES, orientado a obtener los resultados en la parte diagnóstica de la investigación.

RESULTADOS

Análisis conceptual y normativo

La protección de datos sensibles se ha convertido en una prioridad crítica en el ámbito

educativo, especialmente para instituciones de educación superior, que maneja información confidencial de estudiantes y ex estudiantes. Los datos personales, académicos y financieros son especialmente vulnerables a amenazas cibernéticas y violaciones de seguridad.

Los resultados obtenidos en la investigación sobre las medidas de seguridad para la protección de datos sensibles en Uniandes indican que la universidad no cuenta con políticas, controles y herramientas necesarias para garantizar una protección adecuada de la información personal de sus estudiantes y ex estudiantes. A pesar de que Uniandes ha implementado ciertas prácticas de seguridad, estas no cumplen completamente con los estándares internacionales establecidos por normas como la ISO/IEC 20000-2 e ISO 30301, lo que genera vulnerabilidades críticas en la protección de los datos.

La norma ISO/IEC 20000-2, destaca la relevancia de adoptar un enfoque sistemático para la implementación de medidas de seguridad de la información. Sin embargo, los resultados muestran que Uniandes no ha adoptado completamente estos lineamientos, lo que implica que no se han establecido procedimientos claros para la gestión de incidentes de seguridad ni se han implementado auditorías regulares que evalúen la efectividad de los controles existentes.

Por otro lado, la norma ISO 30301, enfocada en la gestión eficiente de los documentos y registros, destaca la necesidad de gestionar los datos sensibles de manera estandarizada y con un enfoque orientado a la trazabilidad y la seguridad. Los hallazgos sugieren que Uniandes no ha implementado un sistema de gestión documental que cumpla con esta norma, lo que genera brechas en la integridad, confidencialidad y disponibilidad de la información durante de su ciclo de vida.

Al analizar los hallazgos, se espera identificar tanto fortalezas como áreas de mejora en los protocolos de seguridad de datos, con el fin de establecer un marco más robusto que garantice la privacidad y la integridad de la información sensible.

Los resultados de esta investigación subrayan la necesidad urgente de que Uniandes

refuerce sus medidas de seguridad mediante la adopción de estándares internacionales como ISO/IEC 20000-2 e ISO 30301, para asegurar una gestión eficaz y segura de los datos sensibles de la comunidad universitaria.

Análisis de los resultados de la técnica de entrevistas realizadas

Conforme se ha desarrollado el presente trabajo de investigación, además del análisis documental y de procesos institucionales, se aplicó como instrumentos las entrevistas a especialistas de recolección de datos en Uniandes además de las encuestas realizadas a estudiante y ex estudiantes de esta institución, en donde a través de cuestionarios reducidos permitió recabar datos sobre las medidas de seguridad que se conocen a nivel personal y las medidas que pueden ser aplicadas en la institución.

A la primera pregunta que se formuló en cuanto a las principales amenazas o riesgos a los que están expuestos los datos sensibles en el entorno universitario, los especialistas encuestados concuerdan que las principales amenazas percibidas en relación con la seguridad de sus datos incluyen el robo de información, la extorsión y el tratamiento indebido de datos personales.

En la segunda pregunta planteada a los especialistas en cuanto a las medidas de seguridad que consideran son más efectivas para proteger los datos sensibles de los estudiantes y ex estudiantes consideran que la segmentación de datos, el manejo adecuado de plataformas y la capacitación constante del personal se destacan como pilares fundamentales para garantizar la seguridad de los datos sensibles en el entorno universitario. Implementar mejoras en estas áreas puede fortalecer significativamente la protección de la información y reducir los riesgos asociados con el manejo indebido o el acceso no autorizado a los datos.

La tercera pregunta a los especialistas fue dirigida a que procedimientos o protocolos están en vigor en Uniandes para garantizar la seguridad de los datos de los estudiantes, los especialistas mencionaron que por ser un tema de actualidad y que relativamente la ley de protección de datos entro en vigor recientemente, la universidad no cuenta con

procedimientos, normativas o sistemas con los que se protejan los datos tanto generales como sensibles.

La cuarta pregunta planteada se refiere al tipo de formación o capacitación que se cree que debería ofrecer la universidad a su personal y estudiantes para mejorar la protección de los datos sensibles, en la cual los especialistas concuerdan que la más importante es la formación y la sociabilización de la normativa actual que rige a nivel nacional, así como la creación de normativas interna sobre protección de datos.

Finalmente, la pregunta cinco que se refiere a si alguno de los encuestados tenía alguna experiencia directa o conocimiento de incidentes de seguridad de datos en el ámbito universitario, dos de los especialistas supieron manifestar que no habían experimentado una situación similar a la pregunta, por tanto, uno de los encuestados supo manifestar que, si conocía de un caso de incidentes de seguridad, pero no dentro de Uniandes.

Análisis de los resultados de la técnica de encuestas realizadas

La primera pregunta planteada que se refería a cuáles son las principales amenazas a la seguridad de los datos personales en una institución universitaria, los encuestados en su mayoría concuerdan que la principal amenaza sin duda es que la información es se almacenan en bases de datos y se convierten en datos públicos y a su vez estar expuestos a hackeos de información.

Como segunda pregunta se planteó lo siguiente: Que medidas de seguridad considera más importantes para proteger la información personal y académica de los estudiantes, los encuestados coinciden que la capacitación constante a sus colaboradores y a la comunidad universitaria así también como el acceso restringido a la visualización de los datos que mantenga la universidad.

La tercera pregunta que se planteó fue si los encuestados han recibido algún tipo de capacitación o información sobre cómo proteger tus datos personales en la universidad, a lo que el 72.7 % de los encuestados mencionan que no han obtenido ningún tipo de información acerca de protección de datos y un 27.3% aduce que si recibió algún tipo de

información para la protección de sus datos.

La cuarta pregunta planteada fue ¿Cómo cree que la universidad podría mejorar la protección de los datos sensibles de los estudiantes y ex estudiantes? En donde los encuestados coinciden que la creación de normativa interna, la capacitación constante a su personal y la seguridad en sus plataformas sería un aliado positivo para mejorar la protección de datos.

La quinta y última pregunta se planteó lo siguiente ¿Qué tipo de información consideras que debería ser tratada con especial cuidado en términos de seguridad dentro de una universidad? En donde los encuestados supieron manifestar que los datos que se deberían manejar con sigilo son los datos privados, datos sensibles y datos biométricos.

DISCUSIÓN

La protección de datos sensibles de estudiantes y ex estudiantes en instituciones educativas, como Uniandes, es un desafío crítico en la era digital actual. Con el aumento de los ciberataques y las crecientes preocupaciones sobre la privacidad, las universidades se enfrentan a la importancia de establecer medidas de seguridad sólidas para proteger la información personal y académica de sus estudiantes. Este estudio ha identificado varias áreas clave donde se pueden mejorar las prácticas de seguridad para reducir los riesgos asociados con la gestión de datos sensibles.

Basándose a los resultados de este estudio se destaca la importancia de implementar medidas de seguridad robustas para la protección de datos sensibles de estudiantes y ex estudiantes en instituciones de educación superior, específicamente en el contexto de Uniandes. A través del análisis de las políticas actuales y la percepción de seguridad entre los estudiantes, se han identificado varias áreas críticas que requieren atención y mejora.

En primer lugar, los datos muestran que existe una conciencia generalizada entre los estudiantes y ex estudiantes sobre la importancia de proteger su información personal. Sin embargo, la percepción de efectividad de las medidas de seguridad implementadas por

Uniandes es variada. Esto sugiere una posible brecha entre las políticas de seguridad y su aplicación o comunicación efectiva a la comunidad universitaria. La literatura respalda estos hallazgos, indicando que, si bien muchas instituciones cuentan con políticas de seguridad formalizadas, a menudo hay un desfase en la aplicación práctica y en la concientización de los usuarios (Smith, 2020; García y López, 2019).

La protección de datos sensibles en las instituciones de educación superior es un tema de creciente relevancia debido al volumen y la sensibilidad de la información gestionada. En el caso de Uniandes, las medidas de seguridad implementadas deben ser robustas y alinearse con estándares internacionales para garantizar la protección adecuada de los datos de estudiantes y ex estudiantes. En este contexto, las normas ISO/IEC 27002 e ISO 30301 juegan un papel fundamental al proporcionar directrices claras sobre la seguridad de la información y la gestión de documentos. Comparativamente, Viberg et al. (2023) observan diferencias culturales significativas en la preocupación por la privacidad entre estudiantes de distintos países, lo que sugiere que políticas institucionales deben adaptarse al contexto local para ser efectivas.

Además, se identificaron deficiencias en la capacitación y educación en ciberseguridad proporcionada a los estudiantes. Aunque Uniandes ha implementado algunas iniciativas de concientización, los participantes del estudio sugieren que estas no son suficientes o no están adecuadamente difundidas. Esta conclusión coincide con estudios previos que enfatizan la necesidad de programas de educación continuos y actualizados para mantener a los usuarios informados sobre las amenazas emergentes y las mejores prácticas en seguridad de datos (Jones et al., 2021). Este hallazgo está en línea con los resultados de Stewart et al. (2023), quienes identifican barreras institucionales y creencias entre el personal docente que obstaculizan la correcta comprensión y adopción de sistemas basados en datos.

El debate en torno a las políticas de privacidad y los marcos regulatorios resalta la importancia de que Uniandes no solo acate las leyes de protección de datos, como el

Reglamento General de Protección de Datos (GDPR) de la Unión Europea y las normativas locales, sino que también busque superar dichos estándares. Al implementar políticas de privacidad claras y transparentes, Uniandes no solo cumple con las obligaciones legales, sino que también fortalece la confianza de los estudiantes y ex estudiantes en la institución. Esta confianza es esencial para mantener una buena reputación y garantizar la cooperación de la comunidad en la implementación de medidas de seguridad más estrictas.

Un hallazgo significativo es la preocupación por el acceso a largo plazo a los datos de ex estudiantes. Si bien la universidad ha establecido protocolos para el manejo de estos datos, existe un riesgo potencial de que los sistemas de seguridad no se actualicen con la frecuencia necesaria para proteger contra nuevas amenazas. La falta de claridad en las políticas de retención y eliminación de datos también fue destacada como un punto de vulnerabilidad. Estudios similares han demostrado que las instituciones que no gestionan adecuadamente los datos de ex estudiantes están más expuestas a incidentes de violación de datos (Miller, 2018).

Las implicaciones a largo plazo de no abordar adecuadamente las vulnerabilidades de seguridad. Los incidentes de seguridad no solo pueden llevar a pérdidas financieras significativas debido a multas y sanciones, sino que también pueden tener un impacto duradero en la reputación de Uniandes. Los estudiantes y ex estudiantes pueden perder la confianza en la capacidad de la universidad para proteger su información personal, lo que podría llevar a una disminución en las inscripciones y la participación de exalumnos.

Además, la falta de medidas de seguridad adecuadas puede exponer a los estudiantes a riesgos de robo de identidad y otros delitos cibernéticos que pueden tener repercusiones a largo plazo en su vida personal y profesional.

En relación con las medidas tecnológicas, se notó que, si bien Uniandes ha incorporado herramientas de seguridad avanzadas, como la encriptación de datos y la autenticación

multifactorial, es necesario realizar una evaluación constante de estas herramientas para garantizar su eficacia frente a las amenazas actuales. La rápida evolución de las técnicas de ataque, como el phishing y el ransomware, exige una actualización constante de las soluciones de seguridad (Wilson, 2023).

Este estudio subraya la importancia de implementar un enfoque integral y proactivo para la protección de datos sensibles en Uniandes. Al adoptar medidas de seguridad más avanzadas, mejorar la concienciación sobre la seguridad de la información y garantizar la conformidad con los estándares y regulaciones de protección de datos, Uniandes puede no solo proteger mejor los datos de sus estudiantes y ex estudiantes, sino también fortalecer su posición como líder en la gestión segura de la información en el sector educativo.

CONCLUSIONES

La protección de los datos sensibles de estudiantes y ex estudiantes es esencial para garantizar la privacidad y la seguridad de la información personal. Una de las propuestas es la implementación de robustas medidas de seguridad que no solo prevengan el acceso no autorizado, sino que también fortalezcan la confianza de los individuos en la gestión de sus datos por parte de la universidad, mediante la designación de un delegado de Protección de Datos.

La capacitación continua del personal en prácticas de seguridad de datos es esencial para mantener la eficacia de las medidas implementadas, lo que conllevará a mayor conciencia sobre las amenazas de seguridad y las mejores prácticas entre los empleados de UNIANDES lo que puede reducir significativamente el riesgo de errores humanos que comprometan la seguridad de la información.

La adherencia a las normativas y regulaciones locales e internacionales sobre protección de datos, como el Reglamento General de Protección de Datos (GDPR), la ley de protección de datos es decisivo para garantizar que las prácticas de seguridad cumplan

con los lineamientos legales. La investigación muestra que el cumplimiento de las normativas no solo previene sanciones, sino que también refuerza la posición de seguridad de la universidad.

La adopción de un sistema de gestión documental fundamentado en la norma ISO 30301, orientada a la gestión eficaz de los documentos y registros, asegura que la información sensible se maneje conforme a procedimientos estandarizados y transparentes. Esto permite a Uniandes optimizar la administración de los datos sensibles, garantizando su integridad y disponibilidad a lo largo del tiempo. Además, el uso de esta norma refuerza la trazabilidad y el control sobre la información, permitiendo cumplir con regulaciones de privacidad y responder de manera eficiente ante incidentes o auditorías relacionadas con la protección de datos.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTOS

A todos los actores sociales involucrados en el desarrollo de la investigación.

REFERENCIAS CONSULTADAS

Brunet, L. N. (2020). Evaluación de impacto en datos personales. *Doctrina: Derechos Fundamentales para el Gobierno de la Información*. https://n9.cl/5rihq

International Organization for Standardization [ISO]. (2021). *ISO 30301:2019 Information and documentation – Management systems for records – Requirements*. Ginebra: ISO. https://n9.cl/mav2p

International Organization for Standardization [ISO]. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. Ginebra: ISO. https://n9.cl/belym

Jiang, X., Goh, T. T., & Liu, M. (2022). On Students' Willingness to Use Online Learning:

A Privacy Calculus Theory Approach. *Frontiers in Psychology, 13*, 880261. https://doi.org/10.3389/fpsyg.2022.880261

Jones, P., Pérez, L., y Gómez, R. (2021). Protección de datos y uso ético de la tecnología para una didáctica sostenible. *Revista Educación y Sociedad, 25*(3), 45-60. https://n9.cl/27y5y

Ley Orgánica de Protección de Datos Personales (Ecuador). (2021). *Registro Oficial Suplemento No. 459, 26 de mayo de 2021*. https://n9.cl/9uqbl

Martínez, A., Pérez, S., y Rivera, J. (2024). Aplicación de normas de seguridad de la información en universidades. *Digital Publisher CEIT, 9*(3), 200-215. https://n9.cl/00u0d

Miller, J. (2018). *Factores para la preservación digital sustentable de archivos.* Madrid: Editorial Anaya.

Ortiz, C. C. (2018). La protección de datos sensibles. *Revista ReconoSer ID*. https://n9.cl/rpg7eo

Reglamento General de Protección de Datos (RGPD). (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales*. Diario Oficial de la Unión Europea. https://n9.cl/r9s8p

Rodríguez, P., y López, M. (2023). Protección de datos personales en el ámbito universitario: Un enfoque desde la ISO 27002. *Revista Transparencia y Sociedad, 17*, 88-104. https://n9.cl/z2vnj

Smith, J. (2020). La inteligencia artificial en la educación superior. *Revista Educación Digital, 12*(2), 55-70.

Stewart, B., Miklas, E., Szczyrek, S., et al. (2023). Barriers and beliefs: A comparative case study of how university educators understand the datafication of higher education systems. *International Journal of Educational Technology in Higher Education, 20*, 33. https://doi.org/10.1186/s41239-023-00402-9

Torres, C. (2022). Qué son los datos sensibles y cómo protegerlos. *Pridatect Blog*. https://n9.cl/445mmu

Viberg, O., Kizilcec, R. F., Jivet, I., Martínez Monés, A., Oh, A., Mutimukwe, C., Hrastinski,

S., & Scheffel, M. (2023). *Cultural Differences in Students' Privacy Concerns in Learning Analytics across Germany, South Korea, Spain, Sweden, and the United States. arXiv preprint*. https://n9.cl/togsj

Wilson, R. (2023, 9 de marzo). Estrategias de atribución y ocultamiento de ataques cibernéticos. *CEDEGYS*. https://n9.cl/49ntc