DISCE
REVISTA CIENTÍFICA EDUCATIVA Y SOCIAL

ARTICULO DE INVESTIGACIÓN

Modelo de gestión de controles para la privacidad de la información en Instituciones de Educación Superior

Management model for information privacy controls in Higher Education Institutions

Recibido: 26/09/2025, Revisado: 16/10/2025, Aceptado: 24/11/2025, Publicado: 31/12/2025

Para citar este trabajo:
Ríos Barona, D. J., Palmera Quintero, L. M., Ortiz Cañares, L. A., & Sánchez Thomas, L. (2025). Modelo de gestión de controles para la privacidad de la información en Instituciones de Educación Superior. *DISCE. Revista Científica Educativa Y Social*, *2*(2), 594-611. https://doi.org/10.69821/DISCE.v2i2.88

Danny Jhoan Ríos Barona
Universidad Popular del Cesar, Cesar, Colombia
https://orcid.org/0009-0009-1333-6893
djrios@unicesar.edu.co

Luis Manuel Palmera Quintero
Universidad Popular del Cesar, Cesar, Colombia
https://orcid.org/0000-0002-3242-2115
lmpalmera@unicesar.edu.co

Lisbeth Alejandra Ortiz Cañares
Universidad Popular del Cesar, Cesar, Colombia
https://orcid.org/0009-0009-0491-5092
lalejandraortiz@unicesar.edu.co

Leonel Sánchez Thomas
Universidad Popular del Cesar, Cesar, Colombia
https://orcid.org/0000-0003-2748-5717
lsanchezt@unicesar.edu.co

Resumen

Esta investigación se enfocó en que es muy importante que las Instituciones de Educación Superior (IES) protejan la privacidad de la información, especialmente en esta era donde el uso de datos personales y sensibles es una de las mayores preocupaciones. Teniendo en cuenta estos antecedentes, se creó un modelo de gestión para el control de la privacidad de la información que permita responder a los desafíos particulares y únicos que tienen las IES y estas puedan enfrentar al intentar proteger la privacidad de los activos de la información. La investigación empleó una metodología cuantitativa y como instrumento de recolección de datos la encuesta con una población representativa de 5 IES del Nor-Oriente Colombiano, tomando como muestra las 5 instituciones. El propósito del estudio fue evaluar las perspectivas de los profesionales sobre la efectividad de los controles de privacidad actuales en sus instituciones y determinar si un modelo de control específico podría ser efectivo para mejorar la protección de la información. El estudio encontró que, aunque la mayoría de las IES tenían políticas y procedimientos destinados a salvaguardar la privacidad de los datos, había deficiencias evidentes en la implementación y cumplimiento de estas medidas. Los desafíos comunes informados por los encuestados incluyeron la falta de recursos, la capacitación insuficiente del personal y la ambigüedad sobre las responsabilidades en la gestión de la privacidad. Los hallazgos revelan que un enfoque holístico y sistemático que incluya políticas, procedimientos, así como concienciación y capacitación del personal es crucial para garantizar la protección de datos en esta era de creciente digitalización dentro de los entornos de educación superior.

Palabras clave: Privacidad de la información, gestión de controles, Seguridad de la información, Educación Superior

Abstract

This research focused on the fact that it is very important for Higher Education Institutions (HEIs) to protect the privacy of information, especially in this era where the use of personal and sensitive data is one of the greatest concerns. Taking this background into account, a management model was created for the control of information privacy that allows us to respond to the particular and unique challenges that HEIs have and may face when trying to protect the privacy of information assets. The research used a quantitative methodology and as a data collection instrument the survey with a representative population of 5 HEIs in Northeast Colombia, taking the 5 institutions as a sample. The purpose of the study was to evaluate professionals' perspectives on the effectiveness of current privacy controls at their institutions and determine whether a specific control model could be effective in improving information protection. The study found that although most HEIs had policies and procedures aimed at safeguarding data privacy, there were evident deficiencies in the implementation and enforcement of these measures. Common challenges reported by respondents included lack of resources, insufficient staff training, and ambiguity over responsibilities for privacy management. The findings reveal that a holistic and systematic approach including policies, procedures, as well as staff awareness and training is crucial to ensure data protection in this era of increasing digitalization within higher education environments.

Keywords: Information privacy, controls management, Information security, Higher Education

INTRODUCCIÓN

La realidad de las universidades es que necesitan soluciones viables a los muchos desafíos que enfrentan las actividades centrales de las universidades donde la investigación es un elemento importante de la gobernanza del sistema institucional, ya que no existe una estructura suficiente para sustentarla. Pérez Mayo et al. (2018) expresa que, "El control se basa en el supuesto de que la búsqueda de la consistencia y previsibilidad en el comportamiento individual asegura el logro de las metas organizacionales". Asimismo, Carreño Bernal (2025) señala que la información es uno de los activos más importantes de la universidad y por ello necesita ser debidamente protegida ya que la seguridad de la información está ligada a los conceptos de confidencialidad, integridad y disponibilidad de la información. Por su parte, Sánchez Pacheco y Rebolledo Hinojosa (2017) hablan sobre las dificultades que enfrentan las universidades de orden público, para proteger y asegurar la información y los documentos que tienen en su poder los funcionarios de varios departamentos el cual no tienen controles debido a la falta de buenas estrategias para enfrentar las amenazas.

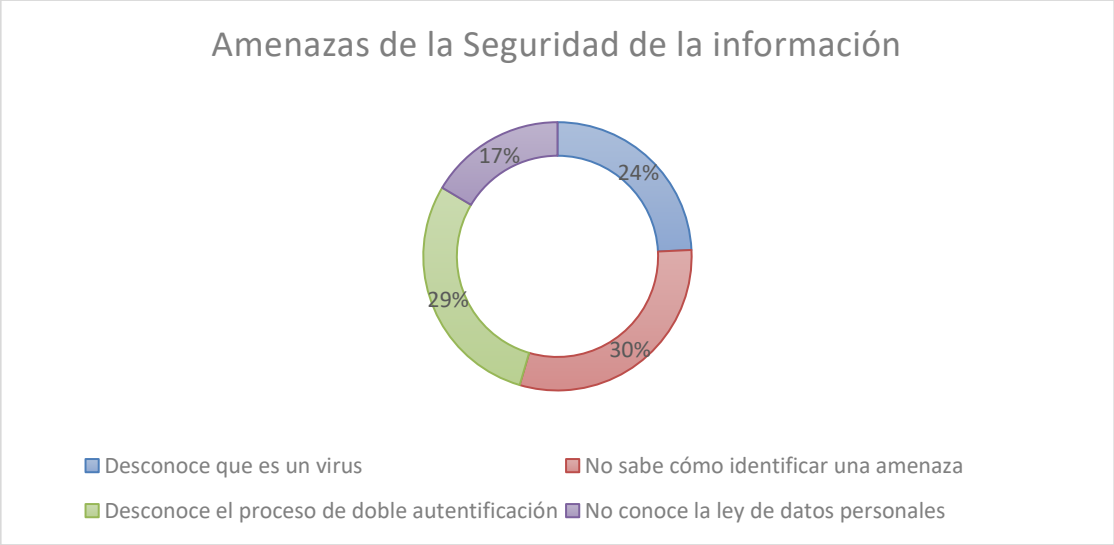
En la actualidad, el hacking con fines maliciosos se está convirtiendo cada vez más en una forma de adquirir toda una serie de herramientas que pueden utilizarse para atacar a las empresas y obtener su información. Tal y como recoge el estudio de Deloitte como se cita en García (2019) sobre el sector universitario, el 80% de las universidades participantes admitieron haber sufrido algún tipo de incidente de ataque; por lo tanto, la digitalización siempre debe ir asociada a mayores riesgos y una mayor responsabilidad en la seguridad de los datos. En contraste, Sánchez Jaime (2019) sostiene que la ausencia o falta de filtros de comunicación entre las instituciones educativas y su personal representa una seria amenaza porque cualquier tercero puede utilizar las redes y sistemas. Según Lurcu (2020), el 73% de las organizaciones tardó tres días en resolver sus problemas de seguridad; por lo tanto, los piratas informáticos consideran que las universidades son uno de sus objetivos preferidos.

A pesar de las medidas tomadas en las Universidades del Nor-Oriente Colombia

como lo son: Universidad Popular del Cesar – Aguachica, Universidad del Magdalena, Universidad Abierta y a Distancia UNAD – Aguachica y Ocaña, Universidad Francisco de Paula Santander Ocaña, aún predominan conductas de riesgo en materia de seguridad de la información, como se logra observar en la Figura 1, producto de un modelo de gestión que no promueve estrategias ni buenas prácticas y tiene poco o ningún conocimiento sobre temas relacionados con la privacidad de datos. El nivel de conocimiento del personal administrativo en temas relevantes a la seguridad de la información es el siguiente:

Figura 1

Amenazas más frecuentes



Como se muestra en la (Figura 1), con información brindada por los profesionales de las Universidades del Nor-Oriente Colombiano escogidas, existe una gran brecha de conocimiento sobre cómo el control y operación efectivos de los procesos de seguridad de la información son esenciales. Donde estas situaciones se han hecho más notables, ya que la infraestructura tecnológica ha crecido y se están utilizando más herramientas que están soportadas en internet.

Por otro lado, las universidades son ejemplos comunes de instituciones de

educación superior que manejan datos financieros, académicos y administrativos que son sensibles y susceptibles de estar expuestos a una serie de amenazas. (Aguilar Quintero, 2019) en su estudio tuvo como objetivo analizar si las universidades cuentan con medidas de seguridad de la información para prevenir malware en su infraestructura tecnológica. Al disponer de información tan sensible y adherirse a protocolos que garanticen la seguridad y privacidad de los datos. La superintendencia de Industria y Comercio SIC reportó que en el 2021 recibió 28.610 quejas ciudadanas, un 74,49% más respecto al número de quejas recibidas durante 2020. El 90% de las quejas que se presentaron fueron por presuntas violaciones de la Ley de Habeas Data Financiero, donde la principal fue el "Incumplimiento del principio de veracidad o calidad de la información", es decir, los datos no son ciertos o están desactualizados (Mesa, 2023).

Además, como lo mencionan (Sánchez Pacheco & Rebolledo Hinojosa, 2017), un modelo de gestión de protección de la información puede permitir a los administradores de activos lograr un equilibrio entre las dimensiones clave de seguridad de la integridad, la confidencialidad y la disponibilidad de la información en el soporte de las funciones comerciales. También es útil desarrollar una cultura corporativa orientada a influir positivamente en el uso de las medidas de seguridad por parte de los empleados. Por otra parte, según (Castro Márquez & Camargo Barbosa , 2017), cualquier organización que carezca de un adecuado control de la información está expuesta a riesgos.

En este sentido, es fundamental que las instituciones de educación superior fomenten el adecuado manejo de la información como un acto para garantizar la seguridad y prevenir posibles amenazas que puedan perjudicar los intereses de la organización. Por lo tanto, la investigación actual tiene como objetivo desarrollar un modelo de protección de datos eficaz alineando sus políticas, prácticas, visión y objetivos con la misión de la universidad, así como con las prioridades estratégicas, para facilitar un mejor funcionamiento interno.

Proteger la información consiste en garantizar que la identificación, evaluación y

control de los recursos de información, así como de las amenazas, se basen en su impacto en la organización. Además, con sistemas de información digitales y abundancia de datos, es necesario descubrir flujos de información prácticos que faciliten la toma de decisiones (Altamirano Di Luca, 2019). (Ríos C, 2016), sin embargo, analiza los datos, que son el elemento central de cualquier tipo de organización; por lo tanto, necesitan una administración eficaz del mismo. En este sentido, es necesario realizar acciones como capturar, gestionar y entregar adecuadamente los flujos de datos.

La seguridad digital debe considerarse un sistema integrado con capacidad de proteger los activos digitales, lo que fomentará el desarrollo de una cultura de ciberseguridad, ya que está interconectada con la comprensión y prevención de amenazas que comprometen la información procesada, almacenada y transmitida. Que exponen a riesgos la identidad y los mensajes de los usuarios, como correos electrónicos robados y spam, donde se puede reducir el acceso al correo. La seguridad digital involucra sistemas y usuarios y tiene la capacidad de administrar, prevenir y mitigar el riesgo de amenazas digitales.

Las instituciones de educación superior enfrentan un problema grave con la privacidad de la información ya que manejan una gran cantidad de datos personales sobre estudiantes, profesores, personal, investigadores y finanzas. Para salvaguardar estos datos y garantizar su confidencialidad, integridad y accesibilidad, es necesario implantar un modelo de gestión de control. Las medidas ayudan a las organizaciones a detectar y evaluar amenazas a la privacidad de la información y a establecer los controles adecuados que mitiguen y prevengan estas amenazas, Ito et al. (Vásquez Rizo, Rodríguez Muñoz, Gómez Hernández, & Gabalán Coello, 2023). Además, por este motivo, se propone un modelo que ofrece un plan para la gestión de seguridad de la información con un marco definido y de esta manera hacer más fácil y efectiva la aplicación de controles de seguridad.

Fundamentación teórica

La teoría de la seguridad informática se refiere al marco informativo que contiene hechos, principios, metodologías y prácticas que se aplican para salvaguardar los sistemas de información de riesgos y vulnerabilidades que podrían poner en peligro su confidencialidad, integridad o disponibilidad. Los aspectos dentro de esta teoría giran en torno a cómo se desarrollan y examinan los mecanismos y políticas de seguridad, junto con la prevención, detección y reacción ante incidentes de seguridad informática (Martínez Troncoso, 2018).

El contenido de la investigación aborda una perspectiva interdisciplinaria, que utiliza diversos temas que van desde la ingeniería de software, la teoría de la complejidad, la teoría de la información, la teoría de sistemas y la criptografía. Además, está alineado con estándares internacionales como ISO 27001 e ISO 27002; Estándares estadounidenses como NIST SP 800-53; y marcos de mejores prácticas, incluidos COBIT, ITIL y CIS Controls. Hoy en día la seguridad en los ordenadores es un tema de mucho debate, pero es muy necesario su implementación debido a la creciente dependencia de los sistemas de información tanto de las organizaciones como de la sociedad en general. La gestión de los controles de ciberseguridad debe abarcar no sólo la protección sino también la gestión de riesgos, la concientización de los usuarios y la capacitación porque este tema es extremadamente importante y debe abordarse de manera exhaustiva y metódica (Martínez Troncoso, 2018).

Además, el énfasis de la seguridad de la información radica en salvaguardar los activos de datos de una organización, como lo destaca (Figueroa Cubillos, 2018), esto implica confidencialidad, integridad y disponibilidad de los datos. Además, incluye medidas contra amenazas tanto internas como externas. Evitar el acceso no autorizado a los datos es confidencialidad, mientras que integridad se refiere a garantizar que la información no se modifique sin permiso y, finalmente, disponibilidad es la garantía de que los usuarios autorizados puedan recuperar información cuando sea necesario.

Establecer políticas, procedimientos y controles es otro paso esencial para proteger

los recursos de información. Esto implica la identificación de riesgos de seguridad, evaluación de vulnerabilidades, implementación de medidas de seguridad requeridas y monitoreo regular de la eficiencia de los controles implementados. Además, la seguridad de la información debe estar respaldada por una cultura de seguridad de la información arraigada en toda la organización y con responsabilidad compartida entre los empleados (Cuenca León, 2019).

COBIT 2019 es un marco que ayuda a las organizaciones a gestionar riesgos, cumplir con leyes y regulaciones y garantizar la utilización adecuada de las inversiones en TI. COBIT significa Objetivos de Control para la Información y Tecnologías Relacionadas. También se lo conoce como un conjunto de pautas bien definidas para el gobierno y la gestión de TI. Sigue cinco principios: abordar las necesidades de las partes interesadas, cubrir todo el ciclo de vida de la información, utilizar un enfoque integrado, ser integral y orientado a los procesos y, finalmente, gestionar la privacidad de los datos al tomar decisiones. Hay otros aspectos que incluyen 40 objetivos de gestión y gobierno de TI divididos en las siguientes categorías: Evaluar, Dirigir, Monitorear (EDM); Alinear, Planificar, Organizar (APO); Construir, Adquirir, Implementar (BAI); Entrega, Soporte, Servicio (DSS); y, por último, Monitorear, Evaluar, Mejorar (MEA), (ISACA, 2018).

El ciclo de vida del servicio consta de cinco fases, conocidas como estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio. Cada etapa tiene los arreglos necesarios para garantizar que los procesos de gestión de TI se entreguen de manera eficiente y efectiva y puedan evolucionar cuando sea necesario en una organización (Axelos, 2019).

METODOLOGÍA

Este estudio adoptó un diseño de investigación cuantitativa para explorar modelos de gestión para controlar la seguridad de la información. Utiliza datos fácilmente cuantificables y permite analizar en qué medida estas medidas de seguridad son efectivas. El uso de encuestas, cuestionarios y mediciones facilita la recopilación de datos numéricos, que serán sometidos a análisis estadísticos para determinar patrones y asociaciones fuertes entre las variables que se investigan. Esto puede identificar amenazas y riesgos asociados con la información, junto con áreas donde las políticas de seguridad de la organización necesitan mejorar (Galalrdo Echenique, 2017).

Por otra parte, (Ramos Galarza, 2020), ha afirmado que un método cuantitativo basado en un estudio descriptivo podría ser realmente práctico en casos como la recopilación de información imparcial y confiable sobre las prácticas de seguridad organizacional porque implica la recopilación y análisis de datos numéricos, por ejemplo, estadísticas y mediciones numéricas. Este tipo de estudio permite la descripción y análisis de las características de un fenómeno específico. Un estudio descriptivo cuantitativo puede revelar qué medidas de seguridad implementan comúnmente las organizaciones, así como las áreas más críticas que requieren atención y desarrollo en la gestión de la seguridad de la información. Además, los resultados de la evaluación comparativa entre varias organizaciones pueden ayudar a establecer mejores prácticas o estándares para la gestión de la seguridad de la información.

Tabla 1

Población y Muestra

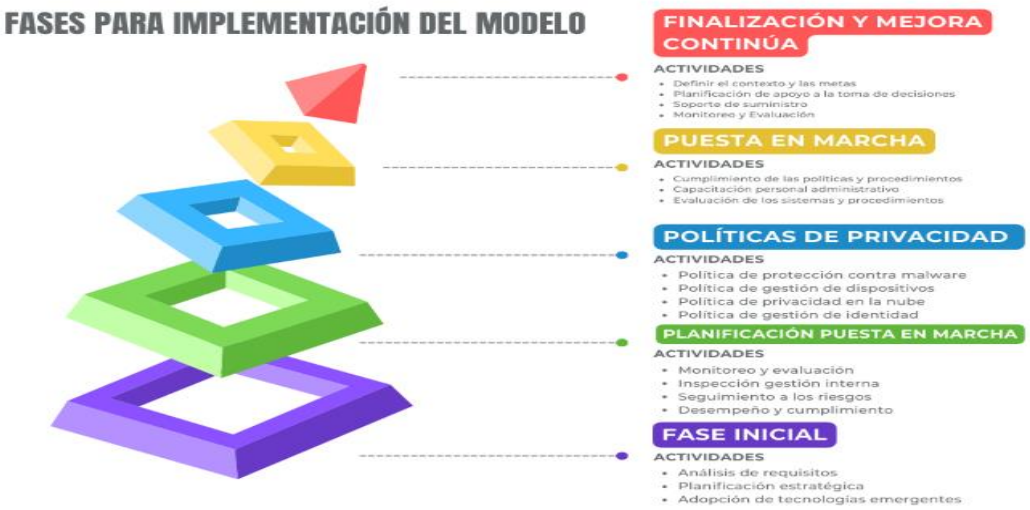
Población	Muestra
En cuanto a la población objeto de estudio se tomaron en cuenta las universidades del Nor- Oriente Colombiano que están en la actualidad en el Cesar, Magdalena y Norte de Santander, como lo son la Universidad	Se tomaron en cuenta para la investigación las cinco (5) universidades mencionadas en la población.

Popular del Cesar, la UFPSO, la UNIMAG del Magdalena, UNAD de Ocaña y UNAD de Aguachica.	

El ámbito de la educación superior está repleto de múltiples sistemas, y hacer cumplir la confluencia de un modelo de control en el paradigma de privacidad de la información es un proyecto a gran escala. Estas etapas son pasos distintos que van desde el inicio hasta el final del programa. En todo momento, el análisis juega un papel crucial que es la planificación cuidadosa, un proceso esencial que incluye estrategias elaboradas y específicas para llevar a cabo su ejecución adecuadamente (Mejía Rodríguez, Palmera Quintero, Rincón Pinzón, & Arévalo Vergel, 2022). De esta manera se plantean cinco fases que permitirán la implementación del modelo dentro de cualquier institución educativa, con la finalidad que sea escalable. Al comienzo de la investigación, se ejecuta una serie de operaciones tácticas que se incluyen en la primera etapa. Es en este punto que se realiza un análisis para identificar necesidades y posibles riesgos respecto a la seguridad de la información en la empresa. Se identifican los objetivos del proyecto y se crea un equipo que contiene experiencia técnica de diferentes departamentos como TI, marketing, finanzas, entre otros.

Figura 2

Fases implementación del modelo



RESULTADOS Y DISCUSIONES

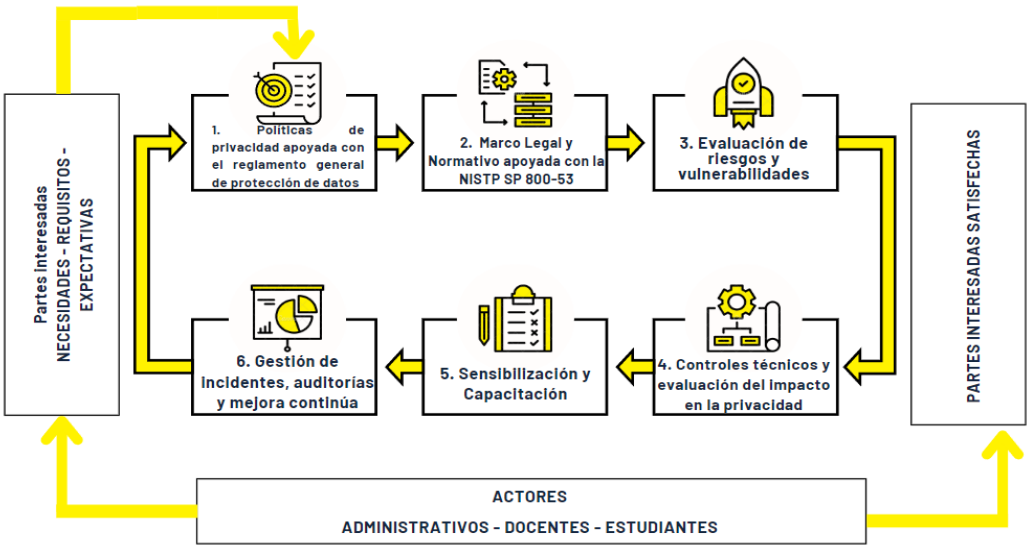
Estructurar un modelo integral de control de la privacidad de la información en las instituciones de educación superior (IES) es una tarea crítica en la era digital donde la protección de datos sensibles es fundamental. En primer lugar, (Sagbini Echávez, Velásquez Perez, & Espinel Blanco, 2024) expresa que se requiere de una evaluación integral de los riesgos y vulnerabilidades relacionados con la seguridad de la información en el entorno de la educación superior. Este debe centrarse en las categorías de datos confidenciales que maneja la agencia, identificar amenazas e identificar estrategias para mitigar los impactos potenciales. El modelo debe basarse en un marco legal y regulatorio sólido para garantizar el cumplimiento de la protección de datos en el sector educativo. Adaptarse a las regulaciones locales e internacionales es importante para construir una base sólida y evitar posibles sanciones.

Crear políticas claras y específicas es esencial, ya que estas políticas deben cubrir aspectos importantes como la recopilación, el procesamiento, el almacenamiento y la divulgación de información personal. La incorporación de principios de privacidad como el consentimiento informado proporciona un enfoque ético a la gestión de datos. La

concientización y educación del personal y los estudiantes es esencial. Un programa estructurado centrado en las mejores prácticas de privacidad de datos es esencial para crear una cultura de seguridad en la que todos comprendan y acepten su papel en la protección de datos. Implementar buenas medidas técnicas es una parte importante. Esto incluye el uso de cifrado de datos, firewalls y sistemas de detección de intrusos para garantizar la integridad y confidencialidad de la información. El control de acceso basado en roles limita el acceso únicamente a personas autorizadas.

Figura 3

Estructura del modelo para controles de privacidad de la información

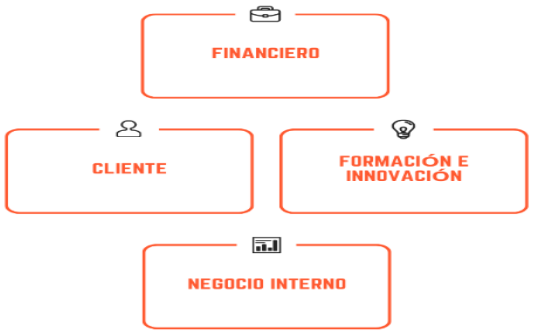


Salvaguardar los activos digitales y garantizar la privacidad de los datos confidenciales son de suma importancia en las Instituciones de Educación Superior (IES). En este entorno exigente y en constante evolución, la implementación de un modelo robusto de seguridad de la información es esencial (Caballero Paredes, Velásquez Pérez, & Flórez Villamizar, 2020). Este proceso abarca varias etapas, comenzando desde la fase inicial y culminando con el establecimiento de un comando de control integral, sirve como un logro fundamental en el ámbito de la gestión tecnológica contemporánea. Dentro de la

intrincada estructura de las instituciones, existe una demanda creciente de un modelo de mando integral que abarque la gestión de los controles de privacidad de la información. Este enfoque estratégico tiene como objetivo unificar la salvaguardia de datos confidenciales, establecer controles efectivos y adaptarse al panorama tecnológico en constante cambio.

Figura 4

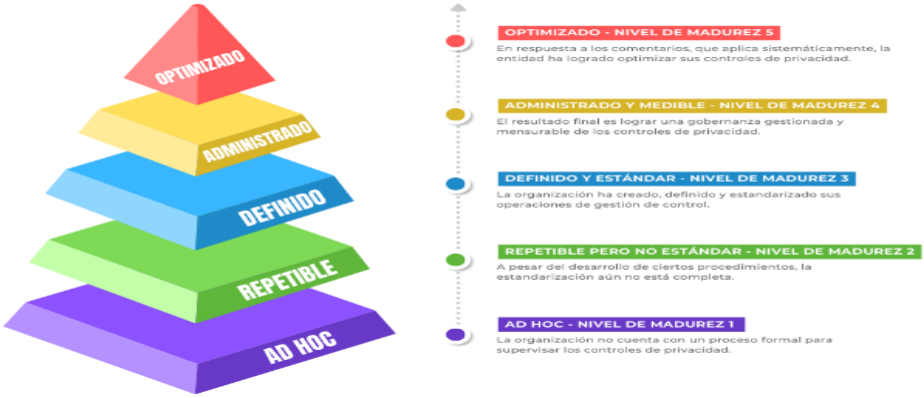
Cuadro de mando integral propuesto



La protección de la privacidad de la información es un foco clave del aspecto financiero del CMI, que ofrece una perspectiva con visión de futuro sobre la inversión necesaria para garantizar esta salvaguardia. Las medidas de ciberseguridad no sólo protegen los activos digitales de la institución, sino que también minimizan el posible impacto financiero de las violaciones de datos. La asignación de recursos para la implementación de tecnologías de punta y la capacitación continua del personal es esencial, y el CMI simplifica el proceso de seguimiento y evaluación de la efectividad de estas inversiones. Dentro del ámbito de la educación, los estudiantes y su información personal son recursos invaluables. La Iniciativa de Gestión del Cliente (CMI) se centra en el punto de vista de los estudiantes y sus familias, garantizando que los protocolos de seguridad no solo cumplan con los estándares regulatorios, sino que también establezcan un sentido de confianza. La apertura en el manejo de datos y la pronta resolución de cualquier problema potencial son componentes esenciales para cultivar una conexión confiable con la comunidad educativa.

Figura 5

Nivel de madurez propuesto



Un uso importante de esta tabla es utilizarla como herramienta que simplifica el proceso de evaluación y medición para garantizar que una organización haya establecido sus sistemas de control en relación con la privacidad de la información en su nivel de madurez. Cada etapa representa un desarrollo en la dirección de un mejor control, productividad y progreso. Una evaluación continua de estos niveles ayuda a identificar puntos débiles que luego pueden convertirse en baluartes para la defensa y cuidado de todos los datos sensibles dentro de la institución.

CONCLUSIONES

Los controles de privacidad institucional para las instituciones de educación superior deben diseñarse con atención al detalle. Esto se debe a varias coincidencias; donde el enfoque principal es que proporciona una visión general amplia de todos los ángulos legales, técnicos, organizativos y culturales que deben cubrirse para ofrecer una protección eficaz de la información contra la filtración a manos equivocadas. Un enfoque tan completo y holístico garantiza que no se pierda ningún ámbito de la privacidad en los datos sensibles, permitiendo recopilar, almacenar y procesar cierta cantidad de informacion hasta su divulgación. La aplicación de un marco bien organizado de controles

de privacidad sobre información confidencial puede reducir considerablemente los riesgos concernientes con no lograr acceder y/o las violaciones de datos.

En conclusión, el estudio cumple con un requisito de la era de la información que va más allá de una mera necesidad y sienta las bases para mejores métodos de gestión de la privacidad en el campo educativo, con ética y sostenibilidad. Con una visión integral de la gestión de riesgos, el cumplimiento normativo, la confianza de la comunidad, la innovación y la cultura de la privacidad como componentes de un marco integrado y no como variables individuales, este proyecto presenta un camino a seguir que no solo beneficia a las instituciones individuales, sino que también contribuye a la educación en general. La integración adecuada de este modelo es un gran avance que cambiará la forma en que las instituciones educativas abordan la protección de datos y garantizará que la futura vida universitaria se produzca en un clima en el que se respeten los derechos de privacidad de cada persona.

REFERENCIAS

Aguilar Quintero, N. (2019). Modelo de seguridad de la información para instituciones de Educación Superior. *Universidad Francisco de Paula Santander Ocaña*, 1-123.

Altamirano Di Luca, M. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. *Revista redalyc*, 1-10.

Axelos. (2019). ITIL 4. *ITIL Foundation*, 1 - 244. Obtenido de https://worldaedait.com.mx/wp-content/uploads/2019/09/ITIL-4-Foundation-Material-Participante.pdf

Carreño Bernal, E. G. (2025). Contratación transfronteriza: necesidad e importancia de su armonización en un mundo globalizado. *Cuadernos de derecho transnacional*, *17*(1), 281-307. https://doi.org/10.20318/cdt.2025.9330

Caballero-Paredes, M. A., Velásquez-Pérez, T., & Flórez-Villamizar, L. (2021). Seguridad de la información de la jurisdicción especial para la paz. *REVISTA COLOMBIANA DE TECNOLOGIAS DE AVANZADA (RCTA)*, *1*(37), 118-123. https://doi.org/10.24054/rcta.v1i37.1263.

Castro Márquez, D., & Camargo Barbosa , J. (2017). Modelo de gestión de tratamiento de la Información. *Institución Universitaria Politécnico GranColombiano*, 1-81.

Cuenca León, W. (2019). Gestión de la Seguridad de la Información basado en la Norma ISO/IEC 27001 y su incidencia en las Instituciones de Educación Superior de la ciudad de Machala. *Universidad Tecnica de Ambato*, 1 - 227. Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/29844/1/Tesis_t1585msi.PDF

Figueroa Cubillos, C. (2018). Diseño de un sistema de gestión de seguridad de la información para el colegio Germán Arciniegas I.E.D, bao la Norma Técnica Colombiana NTC ISO/IEC 27001:2013. *Universidad Nacional Abierta y a Distancia UNAD*, 1 - 105. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/25633/%20fccarolina.pdf?sequence=1&isAllowed=y

Galalrdo Echenique, E. (2017). Metodología de la Investigación. *Universidad Continental*, 1-98. Obtenido de https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_UC_EG_MAI_UC0584_2018.pdf

García, N. (17 de Octubre de 2019). *Ciberseguridad: Las universidades son las terceras instituciones más atacadas*. Obtenido de elEconomista: https://www.eleconomista.es/ecoaula/noticias/10144866/10/19/Ciberseguridad-Las-universidades-son-las-terceras-instituciones-mas-atacadas.html

ISACA. (2018). COBIT 2019. *ADACSI*, 1-43. Obtenido de https://iaia.org.ar/wp-content/uploads/2019/07/COBIT2019-IAIA.pdf

Lurcu, V. (08 de septiembre de 2020). *Ciberataques en la Universidad: ¿Qué universidades son objetivo de los piratas, cómo y porqué?* Obtenido de AVIRA: https://www.avira.com/es/blog/ciberataques-en-la-universidad-que-universidades-son-objetivo-de-los-piratas-como-y-por-que

Martínez Troncoso, C. (2018). Protocolo de gobierno y gestión de identidades digitales y de control de acceso en el contexto de una Institución de Educación Superior. *Fundación Universitaria del Norte*, 1 - 74. Obtenido de http://manglar.uninorte.edu.co/bitstream/handle/10584/8326/133657.pdf?sequence=1

Mejía Rodríguez, C., Palmera Quintero, L., Rincón Pinzón, M., & Arévalo Vergel, L. (2022). Moodle como herramienta e-learning en la educación superior: caso preguntas calculadas para estadística. *Revista Mundo Fesc, 12*(2), 72-80. Obtenido de https://www.fesc.edu.co/Revistas/OJS/index.php/mundofesc/article/view/1156/829

Mesa, A. (26 de enero de 2023). *Datos personales: muchas compañias no cumplen con el principio de seguridad y las personas no son precavidas*. Obtenido de Actualícese: https://actualicese.com/datos-personales-muchas-companias-no-cumplen-con-principio-de-seguridad/

Pérez Mayo, A., Guzmán Cáceres, M., Romero Torres, F., Silos Vaquera, A., & Silos Vaquera, M. (2018). Los modelos de gestión de control como estrategia directiva para la optimización de los recursos en las organizaciones universitarias: Un Estado del Arte. *Universidad Veracruzana*, 1-14.

Ramos Galarza, C. (2020). Los alcances de una investigación. *Revista CienciAmérica*, 1-5. Obtenido de https://dialnet.unirioja.es/descarga/articulo/7746475.pdf

Ríos C, C. (2016). Modelo de Gestión de Información y Toma de decisiones en el Instituto Superior Enrique López Albujar. *Rev. Ciencia, Tecnología y Humanidades*, 1-10.

Sagbini Echávez, J., Velásquez Perez, T., & Espinel Blanco, E. (2024). Modelo de seguridad de la información bajo los principios de gobierno TI para el sector industrial manufacturero. *Revista Ingenio, 21*(1), 9-12. https://doi.org/10.22463/2011642X.3588

Sánchez Jaime, D. (19 de noviembre de 2019). *Los seis riesgos de internet para los centros educativos*. Obtenido de Magisterio: https://www.magisnet.com/2019/11/los-seis-riesgos-de-internet-para-los-centros-educativos/

Sánchez Pacheco, E., & Rebolledo Hinojosa, F. (2017). Diseño de un modelo de gestión de la seguridad de la información en el área de talento humano de la secretaría de Educación. *Institución Universitaria Politécnico GranColombiano*, 1-85. http://alejandria.poligran.edu.co/handle/10823/1039

Vásquez Rizo, F., Rodríguez Muñoz, J., Gómez Hernández, J., & Gabalán Coello, J. (2023). Relación entre gestión de información y sistema de aseguramiento de la calidad en Instituciones de Educación Superior. Una revisión. *Universidad de la Costa*, 1 - 20. https://revistascientificas.cuc.edu.co/culturaeducacionysociedad/article/view/3570/4461

Conflicto de intereses

El autor (o los autores) declara(n) que esta investigación no tiene conflicto de intereses y, por tanto, acepta(n) las normativas de publicación de esta revista.

Financiación

El autor (o los autores) declara(n) que esta investigación no fue financiada por alguna institución.

REVISTA CIENTÍFICA DISCE ISSN: 3028-7642 EDUCATIVA Y SOCIAL