Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), septiembre-octubre 2024,
Volumen 8, Número 5.

https://doi.org/10.37811/cl_rcm.v8i5

SISTEMA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SU IMPACTO EN EL GOBIERNO Y GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

INFORMATION SECURITY MANAGEMENT SYSTEM AND ITS IMPACT ON INFORMATION TECHNOLOGY GOVERNANCE AND MANAGEMENT

Verónica Villarreal Morales
Universidad Estatal Amazónica, Ecuador

Katherine Estefania Coro Villarreal
Universidad Estatal Amazónica, Ecuador

Edwin Gustavo Fernández Sánchez
Universidad Estatal Amazónica, Ecuador

Jhon Paul Cueva Martinez
Universidad Estatal Amazónica, Ecuador

DOI: https://doi.org/10.37811/cl_rcm.v8i6.14758

Sistema Gestión de Seguridad de la Información y su impacto en el Gobierno y Gestión de las Tecnologías de la Información

Verónica Villarreal Morales[1]
vvillarreal@uea.edu.ec
https://orcid.org/0000-0002-6401-3404
Universidad Estatal Amazónica
Provincia de Pastaza- Puyo
Ecuador

Katherine Estefania Coro Villarreal
ke.corov@uea.edu.ec
https://orcid.org/0009-0009-7667-7767
Universidad Estatal Amazónica
Provincia de Pastaza- Puyo
Ecuador

Edwin Gustavo Fernández Sánchez
gfernandez@uea.edu.ec
https://orcid.org/0000-0002-2613-4774
Universidad Estatal Amazónica
Provincia de Pastaza- Puyo
Ecuador

Jhon Paul Cueva Martinez
jp.cuevam@uea.edu.ec
https://orcid.org/0009-0005-5803-497X
Universidad Estatal Amazónica
Provincia de Pastaza- Puyo
Ecuador

RESUMEN

El presente documento examina cómo la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) ha influido significativamente en los procesos de gobernanza y gestión de Tecnologías de la Información (TI) en la Universidad Estatal Amazónica (UEA). El análisis se enfoca en la implementación de un SGSI basado en estándares internacionales, como la ISO/IEC 27001, y en cómo este sistema mejora la protección de los activos de información, reduce los riesgos relacionados con la seguridad y optimiza la toma de decisiones tecnológicas. El análisis incluye una evaluación detallada de dos procesos clave en el marco de la gobernanza y gestión de TI: EDM03: Asegurar la Optimización del Riesgo y DSS05: Gestionar los Servicios de Seguridad, antes y después de la implementación del SGSI. Antes de la implementación, el proceso EDM03 alcanzó un nivel de madurez de 1, lo que indicaba que estaba gestionado, pero con un nivel básico de control, mientras que el proceso DSS05 obtuvo un nivel de madurez de 2,6, sugiriendo una gestión más estructurada, pero con posibles desviaciones no controladas. Tras la adopción del SGSI, se evidenció una mejora significativa: el proceso EDM03 alcanzó un nivel de madurez de 2,1, mientras que DSS05 llegó a un nivel de 3,7. Estas mejoras fueron cuantificadas mediante métricas aplicadas en la gobernanza y gestión de TI, basadas en las normas ISO 38500 y COBIT 5, implementadas en la universidad desde 2018. En este contexto se concluye que la implementación del SGSI no solo ha mejorado la seguridad de la información en la UEA, sino que ha tenido un impacto positivo en la gestión y gobernanza de TI, optimizando la madurez de los procesos críticos y alineando mejor las estrategias tecnológicas con los objetivos institucionales.

Palabras clave: seguridad de la información, gobierno y gestión de TI, ISO 27001

[1] Autor principal
Correspondencia: vvillarreal@uea.edu.ec

Information Security Management System and its impact on Information Technology Governance and Management

ABSTRACT

This paper examines how the implementation of an Information Security Management System (ISMS) has significantly influenced Governance and Management of Information Technology at the Universidad Estatal Amazónica (UEA). The analysis focuses on the implementation of an ISMS based on international standards, such as ISO/IEC 27001, and how this system improves the protection of information assets, reduces security-related risks, and optimizes technological decision-making. The analysis includes a detailed assessment of two key processes within the IT governance and management: EDM03: Ensure Risk Optimization and DSS05: Manage Security Services, before and after the implementation of the ISMS. Before implementation, the EDM03 process reached a maturity level of 1, indicating that it was managed but with a basic level of control, while the DSS05 process obtained a maturity level of 2.6, suggesting a more structured management but with possible uncontrolled deviations. After the adoption of the ISMS, a significant improvement was evident: the EDM03 process reached a maturity level of 2.1, while DSS05 reached a level of 3.7. These improvements were quantified through metrics applied to IT governance and management, based on the ISO 38500 and COBIT 5 standards, implemented at the university since 2018. In this context, it is concluded that the implementation of the ISMS has not only improved information security at UEA but has had a positive impact on IT management and governance, optimizing the maturity of critical processes and better aligning technological strategies with institutional objectives.

***Keywords*:** information security, IT governance and management, ISO 27001

Artículo recibido 30 octubre 2024
Aceptado para publicación: 20 noviembre 2024

INTRODUCCIÓN

En la actualidad, los avances en las Tecnologías de la Información y Comunicación (TIC) han llevado a que directivos de organizaciones y empresas presten mayor atención a la protección de sus activos de información, ya que la información física y digital desempeña un rol importante (Rodriguez et al., 2020). Además de ser un insumo vital para que los servicios de tecnologías de información (TI) puedan operar de manera necesaria (Ali et al., 2019).

La información forma parte de un proceso en la toma de decisiones estratégicas, esto permite conocer la relación de los datos con lo estratégico de la información de una empresa, basado en normas y reglamentos que rigen el buen uso de la información dentro y fuera de las instituciones (Beesley et al. 2020).

La tecnología está jugando un rol fundamental dentro del funcionamiento de las instituciones, la seguridad de los datos vulnerables no solo es esencial para evitar pérdidas y filtraciones, sino también para generar confianza entre proveedores, clientes y socios. A nivel mundial, de acuerdo con (Martínez, 2020) las tecnologías están sometidas a un elevado número de riesgos y amenazas informáticas, lo que se han convertido en una preocupación primordial debido al impacto significativo que pueden tener en el funcionamiento de las organizaciones, ocasionando cuantiosas pérdidas económicas, tal como menciona (Wiley & Calic, 2020). Puesto que en la actualidad el activo más preciado para una organización es su información y los datos que maneja (Gantiva Rincon, C. C., 2021).

En Ecuador, el Gobierno ha acreditado la relevancia de la seguridad de la información a través de regulaciones específicas. Mediante el Acuerdo Nro. MINTEL-MINTEL-2024-0003 (2024), que describe el "Esquema Gubernamental de Seguridad de la Información" (EGSI) proporcionando lineamientos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en el sector público. Este esquema es relevante para garantizar la confidencialidad, integridad y disponibilidad de los datos en las instituciones gubernamentales.

La gestión de la seguridad de la información se puede describir como la implementación de la colección de protocolos o regulaciones que llevan a cabo todas las transacciones de información.

Estos criterios de seguridad deben estar en condiciones de proteger la seguridad de la información de diferentes empresas contra una serie de peligros innegables (Ibrahim, 2022).

En su estudio, (Panaqué Domínguez et al, 2022), menciona que los SGSI basados en la ISO 27001 demuestran ser una herramienta eficaz para mitigar riesgos inherentes a la gestión de la información. Un SGSI también contribuye a una mejor imagen externa y a generar confianza ya que terceros pueden verificar que la información confidencial se maneja de forma segura (Yungán Cazar & Narváez Contero, 2022). La norma ISO 27001 especifica los requisitos para una correcta implementación de un sistema de gestión de la seguridad de la información. Esta norma fue publicada por primera vez en el año 2005 y brinda las pautas para establecer, implementar, mantener y mejorar continuamente dicho sistema dentro del contexto de la organización tal como menciona (Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M, 2022).

La ISO/IEC 27001 es el único estándar de toda la familia de normas ISO 27000 que se utiliza para brindar certificaciones a las organizaciones. Las demás normas de esta familia se usan para brindar un apoyo robusto y profundo para que la organización pueda construir e implementar un Sistema de Gestión de la Seguridad de la Información de manera correcta y duradera de acuerdo con (Zhu & Zhu,2019).

La Universidad Estatal Amazónica (UEA) no es ajena a estos desafíos. Dentro de los proyectos aplicados en la institución, se ha efectuado un proceso de valoración de madurez del Gobierno y Gestión de TI, tal como lo menciona (Villarreal, 2018), quien señala el estado inicial previo a la implementación del Gobierno y Gestión de TI de dos procesos clave en la gestión de la seguridad de la información: el EDM03, que asegura la optimización del riesgo, y el DSS05, que gestiona los servicios de seguridad. Sin embargo, el nivel de madurez de estos procesos en la UEA en su estado inicial fue bajo, con puntajes de 0.4 y 1, respectivamente, en una escala de 5 puntos.

Caamaño y Gil (2020) destacan que las organizaciones enfrentan una creciente exposición a diversas amenazas y son cada vez más vulnerables a ataques cibernéticos. En este sentido, Ramírez Camargo y Rincón Pinzón (2022) subrayan que las instituciones públicas tienen el mandato constitucional de proteger la información de los ciudadanos, tanto de funcionarios como de usuarios. Villarreal (2023) señala que, sin políticas adecuadas y buenas prácticas en seguridad de la información, tanto los

dispositivos móviles como los equipos de escritorio pueden convertirse en vías para la vulneración de datos, lo que podría generar daños irreversibles a nivel institucional.

Este trabajo se centra en analizar la Implementación de un Sistema de Gestión de Seguridad de la Información y su impacto en la gobernanza de TI en la Universidad Estatal Amazónica, con el objetivo de identificar garantizar la confidencialidad, integridad y disponibilidad de los datos institucionales, optimizar la madurez de los procesos críticos y alinear las estrategias tecnológicas con los objetivos institucionales.

METODOLOGÍA

Tipo de Investigación

Para la obtención de resultados se implementó un enfoque cuali-cuantitativo, cuantitativa porque se utiliza parámetros de medición; también es cualitativa porque se emite juicios de valor respecto al riesgo y seguridad de la información en miras de mejorar el Gobierno y Gestión de Tecnologías de la Información, con diseño metodológico Pre - experimental y cuasi - experimental.

Investigación Bibliográfica

La investigación será bibliográfica porque se apoya en libros, documentos técnicos, tesis del área seguridad de la información e informática, revistas, artículos y leyes existentes para el análisis de datos, así como también del riesgo y seguridad de la información en miras de mejorar el Gobierno y Gestión de Tecnologías de la Información.

Investigación de Campo

Se emplea la investigación de campo ya que se buscará obtener información respecto a los procesos de gestión de la información que se realiza, así como el riesgo de TI dentro de la institución y con el personal involucrado en el tema.

Investigación Exploratoria

La investigación será de nivel exploratorio porque se acudirá directamente con las personas encargadas del área de Tecnologías de la Información y Comunicaciones, y se revisarán los procesos de gestión de la información.

Población o muestra

Se trabaja con la población total, que es el grupo de 4 profesionales que laboran en la Dirección de Tecnologías de la Información en la UEA directamente relacionados al área de Seguridad.

Análisis Situación Actual

Los avances tecnológicos en las Tecnologías de la Información y Comunicación (TIC) han llevado a los líderes de diversas organizaciones y empresas a enfocarse más en la protección de sus recursos informáticos, con el propósito de resguardar información sensible y fortalecer la confianza con sus proveedores, clientes y colaboradores. Las ciberamenazas han adquirido una relevancia global debido a las serias consecuencias que pueden generar.

(Aguilar A, 2020) destaca que las ciberamenazas globales representan un riesgo para la seguridad nacional, y América Latina enfrenta brechas en sus capacidades cibernéticas (p. 17). De manera similar, muchas entidades aún no han implementado plenamente canales digitales, lo que las expone a riesgos de seguridad de la información y ciberseguridad, afectando su capacidad para ofrecer servicios seguros (Hernández, M, 2022).

En los últimos años, la adopción de políticas y estándares que garanticen la seguridad y privacidad de la información ha ganado relevancia en las organizaciones.

La familia de normas ISO 27000 proporciona una guía sólida para la implementación de Sistemas de Gestión de Seguridad de la Información. No obstante, aunque estas normas establecen lineamientos sobre qué se debe hacer, no especifican cómo lograrlo. Esto resalta la importancia de desarrollar metodologías específicas que orienten a las organizaciones en la gestión de procesos de seguridad, siempre respaldados por estándares internacionales.

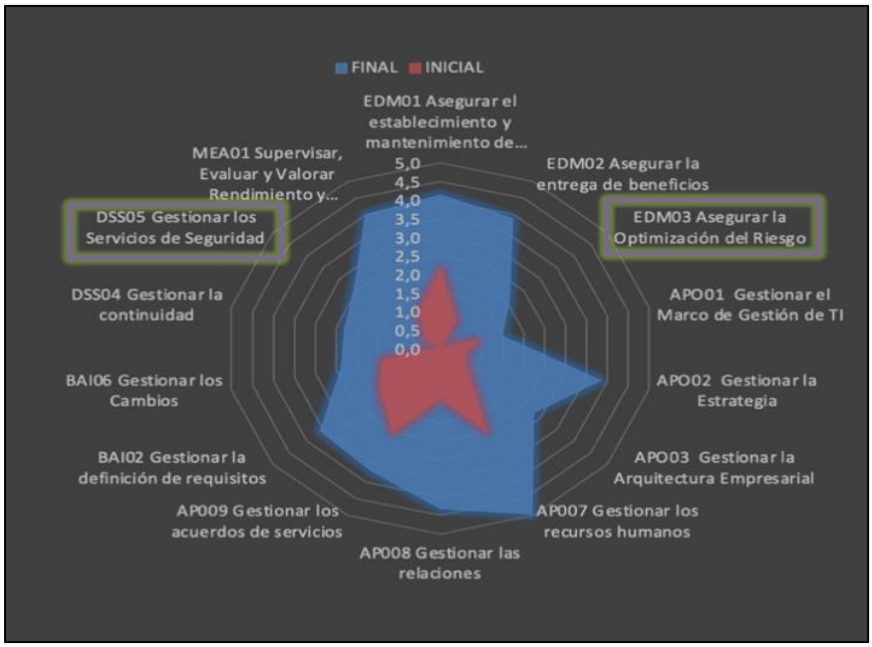
Para gestionar eficazmente sus riesgos, las instituciones deben contar con procesos formales de administración integral de riesgos y de seguridad en el marco del cumplimiento de la Gobernanza y Gestión de las Tecnologías de la Información. En el caso de la Universidad Estatal Amazónica, (Villarreal, 2018) identifica dos procesos clave para la gestión de la seguridad de la información, los cuales se detallan a continuación:

Tabla 1 | Proceso relacionados a la Seguridad de la Información

Proceso	Práctica
EDM03.- Asegurar la Optimización del Riesgo	EDM03.01 Evaluar la gestión de riesgos. EDM03.02 Orientar la gestión de riesgos. EDM03.03 Supervisar la gestión de riesgos.
DSS05.- Gestionar los Servicios de Seguridad	DSS05.01 Proteger contra software malicioso (malware). DSS05.02 Gestionar la seguridad de la red y las conexiones. DSS05.03 Gestionar la seguridad de los puestos de usuario final. DSS05.04 Gestionar la identidad del usuario y el acceso lógico. DSS05.05 Gestionar el acceso físico a los activos de TI. DSS05.06 Gestionar documentos sensibles y dispositivos de salida. DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

En el trabajo de investigación realizado por (Villarreal, 2018), se menciona que los procesos EDM03 y DSS05 detallados en la tabla, luego de la implementación del Gobierno de TI, refleja un nivel de madurez final de 2,1 y 2,6 respectivamente, evidenciando que son procesos gestionados, pero que pueden tener desviaciones no controladas por el personal de TI de la UEA, los niveles obtenidos luego de la implementación del Gobierno de TI para cada proceso se pueden apreciar en la figura 1:

Figura 1 | Nivel de madurez de Gobierno y Gestión de TI de la UEA



Modelo Operativo

Con el objetivo de mejorar los niveles de madurez del Gobierno y Gestión de las TI, se plantea la implementación de un Sistema de Gestión de Seguridad de la Información basado en el modelo PDCA (Plan-Do-Check-Act) como marco metodológico.

En el contexto de un Sistema de Gestión de Seguridad de la Información (SGSI), el ciclo PDCA permite una estructura sistemática para identificar y mitigar riesgos. (Yin, Y., 2023).

Inventario de activos de información

La UEA cuenta con activos que son gestionados, administrados o custodiados por la Dirección de Gestión de Tecnologías de la Información y Comunicación, enlistando los más relevantes, en la siguiente tabla:

Tabla 2 | Activos de Información

Nro.	Id	Categoría	Activos de Información Pura	Descripción de Activo
1	SOFTA-01	Software de Aplicación	Entorno Virtual de Aprendizaje	Aplicación para el despliegue de entornos virtuales de aprendizaje
2	DG-01	Datos digitales	Gestor de base de datos	Administración de base de datos
3	INF-TI-01	Infraestructura de TI	Centro de Datos	Espacio físico, donde se alojan los equipos servidores, y core de distribuidores
4	SER-01	Servicio de TI	Servicio de autenticación de usuario	Autenticación de usuario a través de dominio uea.edu.ec
5	TH-I-01	Talento Humano Internos	Personal administrativo y trabajadores	Personal que labora en la institución

Gestión del Riesgo

Poseer el inventario de activos de información, permite efectivizar la comprensión de riesgos que contemplan analizar las amenazas, probabilidad, riesgo y la aplicación de salvaguardas, como lo menciona Magerit v3, todas las consideraciones anteriores desembocan en una calificación de cada riesgo significativo.

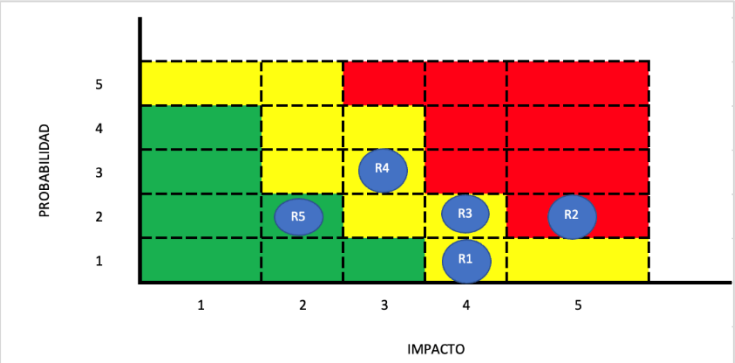
Determinándose si el riesgo es crítico, grave, apreciable, asumible. A continuación, se detalla el análisis del riesgo efectuado a activos de información:

Tabla 3 | Análisis de Riego

Activos de Información Pura	Descripción del Activo	Responsable Análisis de Riesgo	Id Riesgo	Amenazas	Proba-bilidad	Impacto	Riesgo	Calificación del riesgo
Entorno Virtual de Aprendizaje	Aplicación para el despliegue de entornos virtuales de aprendizaje	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	1	4	4	Asumible
			R2	Degradación de los soportes de almacenamiento de la información	2	5	10	Apreciable
			R3	Caída del sistema por sobrecarga	2	4	8	Asumible
			R4	Errores de los usuarios	3	3	9	Apreciable
			R5	Errores de configuración	2	2	4	Asumible
Gestor de base de datos	Administración de base de datos	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	2	3	6	Asumible
			R2	Interrupción de otros servicios y suministros esenciales	2	3	6	Asumible
			R3	Caída del sistema por sobrecarga	2	3	6	Asumible
			R4	Indisponibilidad del personal	2	4	8	Asumible
Centro de datos	Espacio físico, donde se alojan los equipos servidores.	Ing. Verónica Villarreal	R1	Fuego	2	5	10	Apreciable
			R2	Desastres Naturales	2	5	10	Apreciable
			R3	Condiciones inadecuadas de temperatura o humedad	2	4	8	Asumible
			R4	Fallo de servicios de comunicaciones	2	5	10	Apreciable
			R5	Corte del suministro eléctrico	2	5	10	Apreciable
Servicio de autenticación de usuario	Autenticación de usuario a través de dominio uea.edu.ec	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	Apreciable
			R2	Fallo de servicios de comunicaciones	2	5	10	Apreciable
Personal administrativo y trabajadores	Personal que labora en la institución	Ing. Verónica Villarreal	R1	Errores de los usuarios	2	5	10	Apreciable
			R2	Indisponibilidad del personal	2	5	10	Apreciable
			R3	Víctimas de Ingeniería social	3	4	12	Grave

En la siguiente imagen se expresa gráficamente el análisis de riesgo del primer activo de información:

Figura 2 | Análisis de Riesgo



Implementación de un Sistema de Gestión de Seguridad de la Información

La implementación de un Sistema de Gestión de Seguridad de la Información se desarrolla en las siguientes etapas:

a) Establecer el SGSI

La Autoridad Universitaria se mantiene comprometido con la implementación del SGSI en la Universidad Estatal Amazónica.

b) Implementar y operar el SGSI

Seguido del análisis de riesgos, se viabilizó la creación de políticas de seguridad que permita mitigar las amenazas más altas, cumpliendo con los 14 dominios de la norma ISO27001, la cual especifica con detalle los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información (SGSI) dentro del contexto interno y externo de la organización. Y algunos de los requisitos que dicta la norma son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza (Culot, 2021) para lo cual se ha generado el manual de políticas de Seguridad de la Información en la Universidad Estatal Amazónica, la cual se encuentra en proceso de revisión y presentación. Adicional se ha implementado el Sistema de Gestión Documental de la UEA, en el cual se digitaliza y automatiza el procesamiento de expedientes y documentación sensible de la UEA, con esto se garantiza que las dependencias de la institución cuenten con el archivo físico y digital, garantizando la disponibilidad, integridad y confiabilidad de la información.

Figura 3 | Sistema de Gestión documental

c) Monitorear y revisar el SGSI

Para el monitoreo y revisión del Sistema de Gestión de la Seguridad de la Información, se aplicará, encuestas a los actores involucrados, con la finalidad de conocer la adaptabilidad y los problemas que pueden emerger del sistema.

d) Mantener y mejorar el SGSI

La evaluación del Sistema de Gestión de Seguridad de la Información junto a la Evaluación del Gobierno y Gestión de las Tecnologías de la Información en la Universidad Estatal Amazónica permitió identificar los puntos que requieren ser fortalecidos y mejorados, identificándoles a continuación:

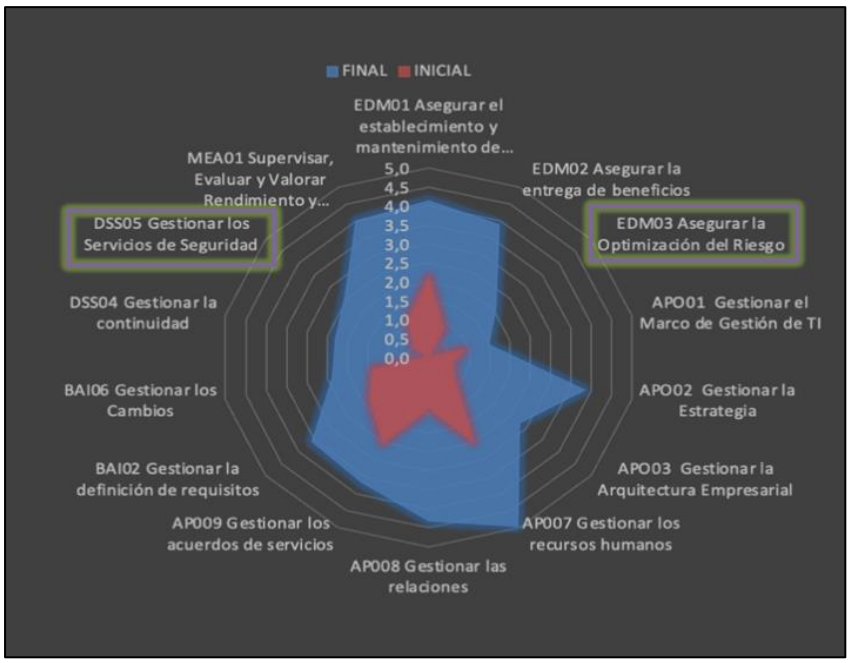
Tabla 4 | Procesos para mejora continua del Gobierno y Gestión de TI

Proceso	Detalle	Nivel de Cumplimiento
EDM03	Asegurar la Optimización del Riesgo	2,7
BAI06	Gestionar los Cambios	2,0
DSS04	Gestionar la continuidad	1,5
MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	2,9

RESULTADOS Y DISCUSIÓN

El Gobierno y Gestión de TI en la Universidad Estatal Amazónica presenta un estado inicial antes de su implementación, detallado en la figura 4, representado en color rojo y una calificación diferenciadora luego de su implementación, representado en la figura con color azul, evidenciando un cambio significativo en el Gobierno y Gestión de TI al implementar procesos catalizadores mediante la ISO 38500 y Cobit 5:

Figura 4 | Evaluación Gobierno y Gestión de TI correspondiente al año 2022



De esta manera se puede evidenciar que la implementación de un Sistema Gestión de Seguridad de la Información impacta significativamente en el Gobierno y Gestión de TI, elevando los niveles de madurez y fortaleciendo Confiabilidad, Integridad y Disponibilidad de la información sensible de la Institución de Educación Superior.

CONCLUSIONES

Ecuador es un país que ha fortalecido su legislación, normativas y reglamentos para fomentar la Seguridad de la información en las diferentes instituciones públicas.

Para la implementación de un Sistema de Gestión de Seguridad de la información es fundamental la identificación de los activos de información, análisis, evaluación y tratamiento de riesgos que garantice conocer el estado actual de la organización y la implementación de políticas que asegure la confidencialidad, integridad y disponibilidad de la información

La implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la UEA, impacto el nivel de madurez del Gobierno y Gestión de TI de manera significativa, mejorando los niveles de madurez de los procesos de gestión de riesgos y seguridad. Esto es evidente en la evaluación de los procesos EDM03 y DSS05, que incrementaron su nivel de madurez, lo que refleja una mayor capacidad para gestionar amenazas y vulnerabilidades.

REFERENCIAS BIBLIOGRÁFICAS

Camaño Fernández, E.E., y Gil Herrera, R.J. *Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional*, NOVUM, 1(10), 61 – 80, 2020. https://revistas.unal.edu.co/index.php/novum/article/view/84210/73652

Ramírez Camargo, E. A., & Rinconc Pinzon, M. A. *La importancia de la seguridad de la información en el sector público en Colombia. Revista lbérica de Sistemas y Tecnologías de Información*, 87 - 99. 2022. https://scielo.pt/pdf/rist/n46/1646-9895-rist-46-97.pdf

Villarreal, V. Sistema de gestión de seguridad de la información en la Universidad Estatal Amazónica. Universidad Técnica de Ambato, 2023. https://repositorio.uta.edu.ec/jspui/handle/123456789/37329

Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). Acuerdo Nro. MINTEL-MINTEL-2024-0003: *Expídese el Esquema Gubernamental de Seguridad de la Información – EGSI, mecanismo para implementar el Sistema de Gestión de Seguridad de la Información en el Sector Público. Registro Oficial Orgánico de la República del Ecuador,* 2024. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2024/03/Registro-Oficial-Acuerdo-Ministerial-No.-0003-2024-EGSI-version-3.0.pdf

Villarreal Morales, V. *Modelo de gestión y gobierno de tecnologías de la información en la Universidad Estatal Amazónica*, 2018.

Martínez, F. *Ciberseguridad y Estado autonómico. ICADE*. Revista de la Facultad de Derecho, 109, 1–19, 2020. https://doi.org/https://doi.org/10.14422/icade.i109.y2020.001

Wiley, A., McCormac, A., & Calic, D. (2020). *More Than the Individual: Examining the Relationship Between Culture and Information Security Awareness. Computers and Security*, 88, 1–8. Recuperado a partir de: https://doi.org/10.1016/j.cose.2019.101640

Cristian Camilo Gantiva Rincon, "*Análisis de soluciones DPL (prevención de perdida de datos) como estrategia para la Seguridad de la Información en Organizaciones Colombianas*", trabajo de grado, UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD, Acacías, 2021.

Rodriguez, L. S., Cruzado Puente de la Vega, C. F., Mejía Corredor, C., & Diaz, M. A. A. (2020). *Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. Propósitos y Representaciones*, 8(3). http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2307799920200004000011&lng=es&nrm=iso&tlng=es.

Ali, O., Shrestha, A., Chatfield, A., y Murray, P. (2019). *Assessing information security risks in the cloud: A case study of Australian local government authorities. Government Information Quarterly*. https://doi.org/10.1016/j.giq.2019.101419

Beesley, K., McLeod, A., Hewitt, B., & Moczygemba, J. *Health Information Management Reimagined: Assessing Current Professional Skills and Industry Demand*. Perspectives in health information management, 18(Winter), 1b, 2020.

A. Ibrahim, «*Integrated e-commerce security model for websites*, » International Journal of Advanced and Applied Sciences, vol. 9, nº 4, p. 8, 2022

G. Culot, «*The ISO/IEC 27001 information security management standard: literature review and theory- based research agenda*» The TQM Journal, 2021

Panaqué Dominguez, J. A., Lizárraga Caipo, Y. G., & Mendoza de los Santos, A. *Efectos de la implementación de un SGSI basado en la norma ISO 27001 para las organizaciones. Perfiles de Ingeniería*, 18(18), 67-76, 2022 https://doi.org/10.31381/perfiles_ingenieria.v18i18.5399

Aguilar Antonio, J. M. *La brecha de ciberseguridad en América Latina frente al contexto global de amenazas. Revista de Estudios en Seguridad Internacional*, 6(2), 17-43, 2020. http://dx.doi.org/10.18847/1.12.2

Yin, Y. *Information security and risk control model based on Plan-Do-Check-Action for digital libraries*. Journal of Cyber Security and Mobility, 13(2), 305–326, 2023. https://doi.org/10.13052/jcsm2245-1439.1326

Yungán Cazar, J. C., & Narváez Contero, C. V. *Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información. Dominio De Las Ciencias*, 8(3), 1025–1041, 2022. https://doi.org/10.23857/dc.v8i3.2854

M. Podrecca, G. Culot, G. Nassimbeni y M. Sartor, «*Information security and value creation: The performance implications of ISO/IEC 27001* » Computers in Industry, vol. 142, pp. 2-10, 2022.

X. Zhu y Y. Zhu, «*Extension of ISO/IEC27001 to Mobile Devices Security Management* » Communications in Computer and Information Science, 2019.

Hernández, M. *Situación de los servicios financieros digitales, la seguridad de la información y ciberseguridad en el Sector Financiero Popular y Solidario. X-Pedientes Económicos*, 6(14), 18–32, 2022. https://ojs.supercias.gob.ec/index.php/X-pedientes_Economicos/article/view/100