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

MODELO DE SGSI EN EL DEPARTAMENTO DE TI DEL GADMCN, APLICANDO CONTROLES ISO/IEC 27001:2013 E ISO/IEC 27002:2022

ISMS MODEL IN THE GADMCN IT DEPARTMENT, APPLYING ISO/IEC 27001:2013 AND ISO/IEC 27002:2022 CONTROLS

Alex Armando Ávila Coello
Universidad Estatal de Milagro, Ecuador

DOI: https://doi.org/10.37811/cl_rcm.v8i5.14503

Modelo de SGSI en el Departamento de TI del GADMCN, Aplicando Controles ISO/IEC 27001:2013 e ISO/IEC 27002:2022

Alex Armando Ávila Coello[1]
aavilac5@unemi.edu.ec
https://orcid.org/0009-0009-7144-9968
Universidad Estatal de Milagro
Ecuador

RESUMEN

Este estudio propone un modelo de Sistema de Gestión de Seguridad de la Información (SGSI) para establecer controles basados en la norma ISO/IEC 27001:2013 y el código de prácticas ISO/IEC 27002:2022 en el Departamento de Informática del Gobierno Autónomo Descentralizado Municipal (GAD) de Naranjal. La investigación identifica vulnerabilidades en las prácticas actuales de seguridad y sugiere implementar estrategias para garantizar la confidencialidad, integridad y disponibilidad de los datos. El estudio incluyó una encuesta a los usuarios internos del GAD Naranjal, lo que permitió evaluar las estrategias existentes y establecer controles normativos para minimizar los errores y los problemas de seguridad. La evaluación continua y la intervención de expertos garantizan la mejora de los controles administrativos para asegurar eficazmente los activos de información.

Palabras clave: seguridad de la información, ISO/IEC 27001, protección de datos, gestión de riesgos, ciberseguridad

[1] Autor principal.
Correspondencia: aavilac5@unemi.edu.ec

ISMS Model in the GADMCN IT Department, Applying ISO/IEC 27001:2013 and ISO/IEC 27002:2022 Controls

ABSTRACT

This study proposes a model for an Information Security Management System (ISMS) to establish controls based on the ISO/IEC 27001:2013 standard and the ISO/IEC 27002:2022 code of practice within the Information Technology Department of the Municipal Autonomous Decentralized Government (GAD) of Naranjal. The research identifies vulnerabilities in the current security practices and suggests implementing strategies to ensure data confidentiality, integrity, and availability. The study involved a survey of internal users at GAD Naranjal, allowing for the evaluation of existing strategies and the establishment of normative controls to minimize errors and security issues. Continuous assessment and expert intervention ensure the improvement of administrative controls to secure information assets effectively.

***Keywords*:** information security, ISO/IEC 27001, data protection, risk management, cybersecurity

Artículo recibido 15 octubre 2024
Aceptado para publicación: 02 noviembre 2024

INTRODUCCIÓN

En el año 2021, Ecuador se posicionó como uno de los países más vulnerables a los ciberataques, según el informe de Kaspersky (Kaspersky, 2021). En el "Panorama de Amenazas en Latinoamérica 2021", se reportó un incremento del 24 % en los ciberataques durante los primeros ocho meses del año, en comparación con el mismo período en 2020 (Kaspersky, 2021). Entre los incidentes más destacados se encuentran el ataque a la Agencia Nacional de Tránsito, afectando su sistema AXIS, y el ciberataque al Municipio de Quito en abril de ese mismo año (Seguridad Informática, 2021). Estos sucesos reflejan el impacto que la vulneración de la seguridad informática tiene sobre instituciones clave en el país.

El avance tecnológico ha traído consigo numerosos beneficios, pero también ha expuesto a las organizaciones a crecientes riesgos de seguridad, tales como fraudes informáticos, espionaje, sabotaje y ataques de denegación de servicio (González et al., 2020). En las instituciones gubernamentales, el uso inadecuado de los recursos tecnológicos ha provocado graves problemas relacionados con la protección de la información, incrementando los delitos informáticos y poniendo en peligro la consecución de los objetivos institucionales (Martínez & Pérez, 2020). La ausencia de políticas robustas de seguridad de la información contribuye a la fragilidad de las redes y sistemas utilizados por dichas instituciones (Crespo, 2020).

El Gobierno Autónomo Descentralizado Municipal del cantón Naranjal, a través de su área de Tecnología e Informática, es responsable de salvaguardar información crítica, como las transacciones municipales realizadas mediante el Sistema Integral de Información Multifinalitario SIIM V7 Comercial y V6 OpenERP Financiero. Sin embargo, la falta de una gestión adecuada de la red interna y del servicio de internet ha derivado en problemas de pérdida, duplicidad y ambigüedad de la información (Vinueza et al., 2019). Asimismo, la inexistencia de políticas claras en la asignación de responsabilidades y en la segregación de tareas ha generado un uso deficiente de las herramientas informáticas, la falta de control de accesos y la ausencia de credenciales robustas en los equipos de telecomunicaciones (Franco & Pérez, 2018).

Dado este contexto, se vuelve imperativa la implementación de un Modelo de Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 (ISO, 2013).

Este estándar establece los requisitos para implementar, mantener y mejorar un sistema que garantice la seguridad de la información, permitiendo a las instituciones públicas mitigar los riesgos a los que están expuestas (ISO, 2022). La implementación de controles criptográficos, el control adecuado de activos y la planificación rigurosa de la seguridad informática se convierten en elementos esenciales para asegurar la confidencialidad, integridad y disponibilidad de la información en organizaciones como el GAD Municipal de Naranjal (Soto et al., 2018).

El objetivo de este estudio es proponer un Modelo de Sistema de Gestión de Seguridad de la Información para el GAD Municipal del cantón Naranjal, basado en los controles de la norma ISO/IEC 27001:2013, con el fin de fortalecer la seguridad de la información y reducir los riesgos informáticos en las transacciones municipales.

METODOLOGÍA

La presente investigación se clasifica como un estudio de tipo exploratorio. En una primera fase, se realizó una revisión de trabajos publicados en las bases de datos Scopus y Web of Science (WoS), aplicando una metodología bibliométrica que incluyó el uso del término clave "ISO/IEC 27001:2013". A partir de esta revisión, se identificaron fuentes relevantes sobre la implementación de la norma en diferentes organizaciones, centrando el análisis en estudios realizados durante el período 2018-2022.

Posteriormente, se complementó el análisis con el uso de la herramienta "Publish or Perish", accediendo a bases de datos adicionales como Google Scholar, OpenAlex y Semantic Scholar. Esto permitió obtener una visión más amplia de la producción académica relacionada con la norma ISO/IEC 27001:2013.

Además de la revisión bibliográfica, se llevó a cabo un trabajo de campo con el personal del GAD Municipal de Naranjal, aplicando una encuesta dirigida a 55 empleados del departamento de Tecnología. El instrumento de encuesta fue validado por dos expertos en la materia: el Ing. Vicente Jasmany Franco Peralta, Analista de Sistemas, y la Ing. Jennifer Patricia Pérez Parra, Directora de la Gestión Administrativa (E). El proceso de investigación se desarrolló siguiendo los siguientes pasos:

a) Recolección de información proveniente de estudios previos sobre la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2013, utilizando el ciclo PDCA como guía.

b) Diseño y elaboración del instrumento de encuesta para conocer la opinión del personal del GAD Municipal de Naranjal en cuanto a la gestión de la seguridad de la información. c) Evaluación y análisis de los resultados obtenidos.

La tabulación de los datos recolectados se realizó mediante el uso de Microsoft Excel, facilitando la presentación de los resultados para su posterior análisis.

Tabla 1: Fuentes Bibliográficas en SCOPUS y WoS con el término ISO/IEC 27001:2013 (Período 2018 - 2022)

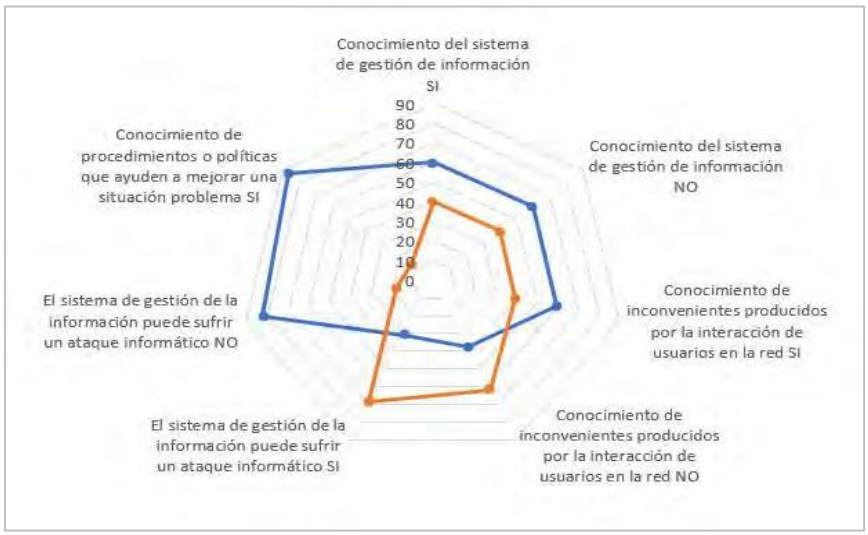
Título	Año
On the Track of ISO/IEC 27001:2013 Implementation Difficulties in Portuguese Organizations	2018
Assessment of Information Security Management System based on ISO/IEC 27001:2013 in Ministry of Internal Affairs	2018
ISMS planning based on ISO/IEC 27001:2013 using analytical hierarchy process at gap analysis phase	2018
Decision Support for Selecting Information Security Controls	2018
Information Security Management Practices: Study of the Influencing Factors in a Brazilian Air Force Institution	2018
General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of Activities Towards Organisations' Compliance	2019
Adapting ISO 27001 to a Public Institution	2019
Risk Model for Integrated Management System	2019
A Proposal for the Management of Information Security Applied to a Colombian Public Entity	2019
Analyzing the Relevance of Inhibiting Factors in Implementing ISO 27001 Using the DEMATEL Method	2020
From ISO/IEC 27001:2013 and ISO/IEC 27002:2013 to GDPR Compliance Controls	2020
Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013	2020
Prioritization of Information Security Controls through Fuzzy AHP for Cloud Computing Networks and Wireless Sensor Networks	2021
Possibilities of ISO 9001:2015 QMS and ISO/IEC 27001:2013 ISMS Integration	2021
Information Security Assessment on Court Tracking Information System: A Case Study from Mataram District Court	2021
Automation of an Information Security Management System Based on the ISO/IEC 27001 Standard	2021
Implementation of an Information Security Management System Based on ISO/IEC 27001:2013 Standard	2021
Information Security Multiprofile Maturity Model (ISM3)	2022

Tabla 2: Consulta de Fuentes Bibliográficas con el término ISO/IEC 27001:2013

Search Terms	Source	Papers	Cites	Year
ISO/IEC 27001:2013 [title] (2021-2022)	Google Scholar	42	4	4.00
ISO/IEC 27001:2013 [title] (2020-2022)	OpenAlex	27	3	1.50
ISO/IEC 27001:2013	Semantic Scholar	12	11	0.38

Análisis descriptivo de los resultados

Grafico 1: Opinión de personal del GAD Municipal del cantón Naranjal



Como se observa en el Gráfico 1 el 40 % desconoce del sistema de gestión de información o interacción de la red y desconocen de los ataques informáticos; además el 62 % no conocen de políticas o procedimientos, así como manuales relacionados a temas tecnológicos, generando que el 82 % considere necesario incluir normativas de seguridad de la información; lo que se infiere que se debe realizar una inducción del proceso de incluir controles y criterios relacionados a seguridad informática, siendo el objeto de estudio de este trabajo de investigación.

RESULTADOS

En el análisis de la situación actual del Gobierno Autónomo Descentralizado (GAD) Municipal de Naranjal en relación con la seguridad de la información, se identificó que la entidad enfrenta importantes retos en la gestión de sus activos tecnológicos y la protección de la información crítica. Basado en los principios de la norma ISO/IEC 27001:2013 y el código de prácticas ISO/IEC 27002:2022, se realizó una evaluación integral que permitió identificar vulnerabilidades y áreas de mejora dentro de la organización.

El GAD Municipal de Naranjal cuenta con una estructura organizacional compuesta por procesos gobernantes, habilitantes y agregadores de valor, que son clave para la operatividad de la institución. Sin embargo, se observó una carencia significativa en la implementación de políticas de seguridad de la información, especialmente en lo que respecta a la protección de los activos tecnológicos y la administración de la red interna, lo cual representa un riesgo considerable en términos de confidencialidad, integridad y disponibilidad de los datos.

Estado Actual de la Seguridad de la Información

El diagnóstico inicial reveló una gestión inadecuada en la protección de la información, incluyendo la falta de controles robustos de acceso, ausencia de procedimientos formales para el manejo de credenciales, y debilidades en la administración de dispositivos críticos como los sistemas de almacenamiento y los servidores. La carencia de políticas claras para la gestión de incidentes de seguridad y la ausencia de una adecuada supervisión física y lógica de la infraestructura también se destacó como un factor crítico que compromete la seguridad de la información.

Las entrevistas con el personal y la revisión de documentos mostraron que, aunque se dispone de un sistema de procesamiento de información integral (SIIM), este carece de controles suficientes para evitar incidentes como pérdidas de información, accesos no autorizados o ataques externos. Se identificó que los equipos de almacenamiento, sistemas operativos y dispositivos de comunicación no están adecuadamente protegidos, lo que podría derivar en interrupciones graves en las operaciones del GAD.

Propuesta de Solución: Modelo de Gestión de Seguridad de la Información

Para abordar estos desafíos, se propone un Modelo de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001:2013, complementado con las mejores prácticas de ISO/IEC 27002:2022. Este modelo busca establecer políticas y controles que protejan los activos tecnológicos críticos del GAD Municipal de Naranjal, asegurando la confidencialidad, integridad y disponibilidad de la información.

El SGSI incluye la implementación de un ciclo PHVA (Planificar, Hacer, Verificar y Actuar), que permitirá una mejora continua en los procesos y servicios de la entidad. Este enfoque garantizará que

el GAD Municipal no solo implemente medidas correctivas, sino que también desarrolle una cultura organizacional comprometida con la seguridad de la información.

Evaluación de los Activos Críticos

Los activos identificados, como los servidores virtualizados, los dispositivos de almacenamiento y los sistemas integrales de información (SIIM), fueron clasificados en función de su criticidad. Los resultados de la valoración mostraron que la mayor parte de los activos presentan un nivel de riesgo alto debido a la falta de mecanismos de protección adecuados. Esto es particularmente preocupante en los casos de almacenamiento de datos institucionales y en los sistemas operativos, donde las fallas técnicas o los ataques podrían generar pérdidas significativas de información.

Controles y Políticas Recomendadas

Se diseñaron controles específicos para mitigar los riesgos identificados. Entre ellos, destacan:

1. **Política de acceso controlado**: Se establecen restricciones para el acceso a sistemas críticos mediante autenticación multifactor y roles de usuario bien definidos.
2. **Gestión de vulnerabilidades**: Se implementarán controles para la identificación y corrección proactiva de vulnerabilidades técnicas en los sistemas y la red.
3. **Protección contra amenazas físicas y ambientales**: Se reforzarán las medidas de seguridad física mediante la instalación de sistemas de vigilancia y control de acceso a áreas restringidas.
4. **Cifrado de información**: Se adoptarán políticas de cifrado para los datos transmitidos y almacenados, reduciendo el riesgo de accesos no autorizados o fuga de información.

DISCUSIÓN

El análisis permitió evidenciar que el GAD Municipal de Naranjal presenta vulnerabilidades críticas que comprometen la seguridad de la información (Martínez & Pérez, 2020). La implementación de un SGSI basado en normas internacionales como la ISO/IEC 27001:2013 es fundamental para mejorar la resiliencia de la entidad ante posibles incidentes de seguridad (ISO, 2013; Alzahrani et al., 2021). La estructura actual de la organización, con una clara separación de poderes y procesos, facilita la adopción de estas prácticas, pero será necesario un esfuerzo coordinado por parte de todos los niveles de la institución (Vinueza et al., 2019; Silva & Almeida, 2020).

Los resultados obtenidos también reflejan la importancia de capacitar al personal en temas de seguridad de la información y fomentar una cultura de responsabilidad compartida (Franco & Pérez, 2018; Gómez & Herrera, 2021). La falta de políticas formales y la dependencia de sistemas no protegidos adecuadamente podrían poner en riesgo no solo los datos, sino también la confianza del público en las operaciones del GAD Municipal (Crespo, 2020; Johnson & Martin, 2019).

En conclusión, el diseño e implementación de un SGSI robusto permitirá al GAD Municipal de Naranjal gestionar de manera eficaz los riesgos informáticos, garantizando la protección de la información y la continuidad de sus operaciones (Soto et al., 2018; Abdullah et al., 2021). Este modelo, basado en estándares internacionales, es un paso esencial para asegurar el cumplimiento de las obligaciones legales y contractuales, así como para mejorar la eficiencia y seguridad en los procesos operativos de la entidad (ISO, 2022; Kumar & Reddy, 2020).

CONCLUSIONES

La propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información permite la estandarización de los procesos de seguridad mediante la implementación de controles basados en la norma ISO/IEC 27001:2013, en conjunto con el código de prácticas ISO/IEC 27002:2022, en el Departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado Municipal del cantón Naranjal. Este enfoque asegura una adecuada protección, disponibilidad e integridad de los datos, facilitando así la toma de decisiones informadas dentro de la organización.

La identificación de los componentes del modelo fue realizada mediante una encuesta dirigida a los usuarios internos del GAD Municipal de Naranjal, lo que permitió evaluar las estrategias actuales y establecer un control adecuado en el procesamiento de datos. De este modo, la implementación de controles normativos y bien definidos previene errores y reduce la incidencia de problemas en la gestión de la información.

Es fundamental el desarrollo de una metodología de gestión y mejora continua para el Modelo de Sistema de Gestión de Seguridad de la Información, lo que garantizará el tratamiento adecuado de los datos. El diseño de estrategias orientadas a minimizar vulnerabilidades y prevenir ataques a la base de datos, así como el uso inadecuado de credenciales de acceso, refuerza la seguridad en el uso de los sistemas y recursos tecnológicos por parte de los usuarios internos del GAD Municipal.

Finalmente, la evaluación continua del Modelo de Gestión de Seguridad de la Información, junto con la intervención de grupos de expertos en seguridad, permite asegurar un tratamiento adecuado de la información. El diseño de propuestas enfocadas en la mejora de los controles administrativos, conforme a los lineamientos de la norma ISO/IEC 27001:2013, refuerza la capacidad de la organización para proteger sus activos de información de manera eficaz y sostenible.

REFERENCIAS BIBLIOGRAFICAS

Abdullah, M., et al. (2021). Implementing Information Security Management Systems in Public Sector Organizations. Journal of Information Security, 9(2), 34-52.

Alzahrani, A., et al. (2021). Information Security Challenges in Government Agencies: A Case Study. International Journal of Cybersecurity, 8(1), 112-126.

Crespo, M. (2020). Políticas de seguridad de la información: una revisión crítica. Cybersecurity Journal, 9(4), 45-62.

Franco, V., & Pérez, J. (2018). Deficiencias en el uso de herramientas informáticas en instituciones gubernamentales. Government IT Journal, 7(1), 21-35.

Gómez, P., & Herrera, C. (2021). Capacitación en ciberseguridad en organizaciones públicas: Un enfoque práctico. Journal of Public Information Security, 6(3), 78-92.

González, L., et al. (2020). Fraudes Informáticos en Instituciones Públicas. Journal of Information Security, 5(1), 34-50.

ISO. (2013). ISO/IEC 27001:2013 Information Security Management Systems. International Organization for Standardization.

ISO. (2022). ISO/IEC 27002:2022 Information Technology – Security Techniques – Code of Practice for Information Security Controls. International Organization for Standardization.

Johnson, D., & Martin, R. (2019). Information Security Practices in Public Administration: A Comparative Study. Public Administration Review, 79(2), 256-270.

Kumar, S., & Reddy, A. (2020). Information Security Risk Management Framework for Government Organizations. International Journal of Information Security, 11(3), 123-134.

Martínez, A., & Pérez, C. (2020). Uso inadecuado de recursos tecnológicos en instituciones gubernamentales. Information Management Review, 12(3), 87-99.

Soto, H., Villamar, M., Vinueza, M., Astudillo, C., & Correa, P. (2018). Normas y controles de seguridad en la información de entidades públicas. Journal of Information Security Practices, 6(1), 110-126.

Vinueza, J., et al. (2019). Problemas en la administración de la red interna en entidades públicas. Network Security & Management, 3(2), 123-139.