SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON ESTÁNDARES ISO/IEC 27001 Y MAGERIT EN LA EMPRESA SP SISTEMAS PALACIOS LTDA DE LA CIUDAD DE PASTO
(Resumen Analítico)

INFORMATION SECURITY MANAGEMENT SYSTEM WITH ISO/IEC 27001 AND MAGERIT STANDARDS AT SP SISTEMAS PALACIOS LTDA COMPANY IN THE CITY OF PASTO
(Analytical Summary)

Autores (*Authors*): IBARRA BOLAÑOS, Andrés Alejandro; NARVÁEZ HERNÁNDEZ, Cesar Augusto
Facultad (*Faculty*): Ingeniería
Programa (*Program*): Ingeniería de Sistemas
Asesor (*Support*): Magíster JOSÉ JAVIER VILLALBA ROMERO
Fecha de terminación del estudio (*End of the research*): noviembre de 2023
Modalidad de Investigación (*Kind of research*): Trabajo de Grado

PALABRAS CLAVES:

SGSI – IMPLEMENTACIÓN
MAGERIT – METODOLOGÍA MAGERIT
ANÁLISIS DE RIESGOS – CLASIFICACIÓN DE ACTIVOS

KEY WORDS:

ISMS – IMPLEMENTATION
MAGERIT – MAGERIT METHODOLOGY
RISK ANALYSIS – ASSET CLASSIFICATION

RESUMEN: La investigación se basa en la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) en la empresa SP Sistemas Palacios LTDA, ubicada en la ciudad de Pasto. Para llevar a cabo este proceso, se emplean los estándares ISO/IEC 27001 y la metodología Magerit, adoptando un enfoque cuantitativo, analítico y descriptivo. Se utilizan diversas técnicas de recolección de datos con el objetivo de determinar e identificar amenazas, riesgos y vulnerabilidades en las diferentes áreas funcionales de la empresa. El proyecto permite detallar los procesos de gestión de la información en cada área funcional, así como la creación de inventarios de activos y la identificación de flujos de datos. A través de matrices y gráficos de calor, se representan los impactos y riesgos asociados a estos activos. Con estos elementos, se procede a la elaboración de un documento que contiene el plan del SGSI. Este documento incluye políticas, estrategias y acciones específicas diseñadas para promover la seguridad de la información en la empresa, siempre guiadas por el estándar ISO/IEC 27001.

ABSTRACT: *The investigation is centered around implementing an Information Security Management System (ISMS) at SP Sistemas Palacios LTDA, located in the city of Pasto. To carry out this process, ISO/IEC 27001 standards and the Magerit methodology are employed, adopting a quantitative, analytical, and descriptive approach. Various data collection techniques are utilized to determine and identify threats, risks, and vulnerabilities in different functional areas of the company. The project allows for a detailed understanding of information management processes in each functional area, including the creation of asset inventories and the identification of data flows. Impacts and risks associated with these assets are visually represented through matrices and heat maps. Using these elements, a document outlining the ISMS plan is developed. This document encompasses policies, strategies, and specific actions designed to foster information security within the company, always guided by the ISO/IEC 27001 standard.*

CONCLUSIONES: La investigación basada en estándares y metodologías que buscan identificar los procesos de gestión de información en el entorno organizacional de SP Sistemas Palacios LTDA., es una herramienta importante ya que, a través del análisis de las diferentes áreas funcionales, permitió identificar los flujos de información, las prácticas existentes y las áreas. Se reconoció la importancia de una gestión eficiente de la información para respaldar la toma de decisiones y la operación de la empresa, lo que sirvió para la elaboración del inventario de activos.

La identificación de amenazas, riesgos y vulnerabilidades a la información de SP Sistemas Palacios LTDA utilizando el estándar MAGERIT reveló una visión integral de las posibles vulnerabilidades en su entorno. Al evaluar amenazas y riesgos específicos para cada área administrativa, se obtuvo una comprensión profunda de los desafíos que enfrenta la empresa en términos de seguridad de la información. Estos hallazgos proporcionan una base sólida para la implementación de medidas de mitigación y la elaboración de estrategias para proteger la información sensible y crítica de la organización.

La falta de medidas adecuadas en el control dentro de las instalaciones del cliente, así como en los sistemas corporativos y el acceso a datos es otro factor crítico que requiere atención. La carencia tanto en políticas claras como en personal encargado del mantenimiento documental, junto con una falta de controles adecuados en vehículos y protecciones digitales en dispositivos móviles amplía aún más el rango amplio e importante riesgos a considerar.

CONCLUSIONS: *The Investigation, grounded in standards and methodologies aimed at identifying information management processes within the organizational environment of SP Sistemas Palacios LTDA., is a crucial tool. Through the analysis of various functional areas, it facilitated the identification of information flows, existing practices, and specific areas. The significance of efficient information management*

was acknowledged for supporting decision-making and the overall operation of the company. This recognition played a pivotal role in crafting the asset inventory.

The identification of threats, risks and vulnerabilities to the information of SP Sistemas Palacios LTDA using the MAGERIT standard revealed a comprehensive vision of the possible vulnerabilities in its environment. By evaluating specific threats and risks for each administrative area, a deep understanding of the challenges facing the company in terms of information security was obtained. These findings provide a solid foundation for implementing mitigation measures and developing strategies to protect the organization's sensitive and critical information.

The lack of adequate control measures within customer facilities, as well as corporate systems and data access, is another critical factor that requires attention. The lack of both clear policies and personnel in charge of document maintenance, together with a lack of adequate controls in vehicles and digital protections on mobile devices, further expands the wide range and important risks to be considered.

RECOMENDACIONES: Dado el análisis detallado de amenazas y vulnerabilidades, en consecuencia, se recomienda utilizar esta investigación como referencia para el análisis de amenazas y vulnerabilidades en la empresa SP Sistemas Palacios LTDA en cuestión.

De acuerdo con la propuesta del Sistema de Gestión de Seguridad de la Información (SGSI), asimismo, se propone considerar los estándares de la ISO/IEC 27001 para implementar y controlar el sistema de seguridad de la información.

Considerando la necesidad de fortalecer la seguridad de la información, por lo tanto, se sugiere iniciar la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en los estándares de la ISO/IEC 27001, teniendo en cuenta los puntos anteriores.

RECOMENDATIONS: *Considering the in-depth analysis of threats and vulnerabilities, it is advisable to utilize this research as a benchmark for conducting a thorough examination of potential risks and weaknesses within the SP Sistemas Palacios LTDA company.*

In accordance with the proposal of the Information Security Management System (ISMS), it is also proposed to consider the ISO/IEC 27001 standards to implement and control the information security system.

Considering the need to strengthen information security, therefore, it is suggested to begin the implementation of the Information Security Management System (ISMS) based on the ISO/IEC 27001 standards, taking into account the previous points.