RELIGACIÓN
REVISTA

Diseño de un sistema de seguridad de la información aplicando al área de TIC del GAD Municipal Santa Rosa

Design of an Information Security System Applied to the ICT Area of the Municipal GAD of Santa Rosa

Jorge Luis González Crespin, Daniel Jacobo Andrade Pesántez

Resumen

El presente trabajo de investigación tiene como objetivo diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) para al área de Tecnologías de la Información y Comunicación (TIC) del Gobierno Autónomo Descentralizado Municipal de Santa Rosa, ubicado en la provincia de El Oro, Ecuador. Ante el incremento de las amenazas cibernéticas y la creciente necesidad de proteger los activos de información en el sector público, se propone una solución fundamentada en los lineamientos de la norma ISO/IEC 27001:2022. Mediante la aplicación de la metodología MAGERIT, el ciclo de calidad PHVA (Planificar, Hacer, Verificar y Actuar), se efectuó un diagnóstico de la situación actual de seguridad, identificando riesgos, vulnerabilidades y oportunidades de mejora en la gestión de la información institucional. Los resultados obtenidos permitieron establecer controles y políticas que fortalecen la confidencialidad, integridad y disponibilidad de los datos, mejorando la eficiencia de los procesos tecnológicos. Se concluye que el diseño implementado contribuirá a la creación de una cultura organizacional orientada a la ciberseguridad y mejora continua, asegurando la protección de la información y la continuidad operativa del Gobierno Autónomo Descentralizado Municipal

Palabras clave: Seguridad de la información; Gestión del riesgo; Ciberseguridad; Tecnologías de la información; Administración pública

Jorge Luis González Crespin
Universidad Católica de Cuenca | Cuenca | Ecuador | jorge.gonzalez.67@est.ucacue.edu.ec
https://orcid.org/0009-0001-2186-4516
Daniel Jacobo Andrade Pesántez
Universidad Católica de Cuenca | Cuenca | Ecuador | dandradep@ucacue.edu.ec
https://orcid.org/0000-0003-0586-4038

http://doi.org/10.46652/rgn.v11i49.1597
ISSN 2477-9083
Vol. 11 No. 49, enero-marzo, 2026, e2601597
Quito, Ecuador

Enviado: julio 30, 2025
Aceptado: septiembre 04, 2025
Publicado: noviembre 27, 2025
Publicación Continua

Abstract

The protection of information has become a critical challenge for public institutions due to the increasing complexity of cyber threats and the need to safeguard essential technological assets. This research aims to design an Information Security Management System for the Information and Communication Technologies area of the municipal institution of Santa Rosa, located in the province of El Oro, Ecuador. The proposal is based on the guidelines of the ISO/IEC 27001:2022 standard and integrates the MAGERIT methodology together with the Plan–Do–Check–Act (PDCA) cycle to diagnose the current security conditions, identify risks and vulnerabilities, and determine opportunities for improvement in institutional information management. The analysis made it possible to establish controls and policies that reinforce data confidentiality, integrity, and availability while improving the efficiency of technological processes. The findings conclude that the proposed system contributes to the development of an organizational culture oriented toward cybersecurity and continuous improvement, ensuring stronger information protection and supporting the operational continuity of municipal services.

Keywords: Information security; Risk management; Cybersecurity; Information technology; Public administration

Introducción

Hoy en día la información se ha consolidado como uno de los activos más valiosos para cualquier organización, pues constituye un elemento esencial para la toma de decisiones y el sostenimiento institucional (Magnusson, 2025). En el sector público, proteger los datos y garantizar la continuidad de los servicios digitales es fundamental para mantener la transparencia, asegurar una gestión eficaz y preservar la confianza tanto del personal como de la ciudadanía (Hossain, 2025; Norris & Mateczun, 2023).

Por otro lado, las entidades públicas enfrentan amenazas crecientes relacionadas con riesgos cibernéticos como ransomware, cuyo propósito es cifrar o dañar la información con fines extorsivos, el phishing orientado a la suplantación de identidad y los accesos no autorizados, los cuales comprometen la confidencialidad, integridad y disponibilidad de los sistemas (Kitsios et al., 2023; Ruggiero, 2022). Los análisis recientes indican que estas instituciones son altamente vulnerables debido a la falta de recursos financieros y personal especializado, así como a niveles bajos de madurez en seguridad de la información (FQM, 2023; Public Sector Assurance, 2022).

Eventos como los ciberataques registrados en los municipios de Hackney, Reino Unido, y North Miami, Estados Unidos, evidencian las importantes repercusiones operativas y económicas que generan las brechas de seguridad en el sector público (Wired, 2023; Wall Street Journal, 2024). Frente a este escenario, la adopción de estándares internacionales como la norma ISO/IEC 27001:2022 constituye una estrategia clave para fortalecer la protección de los datos institucionales, gestionar riesgos y asegurar la continuidad operativa (Toapanta et al., 2020; ICCS-ISAC, 2023; ISO, 2022).

En este contexto, la institución municipal estudiada enfrenta desafíos significativos en la gestión y protección de la información que sustenta sus procesos administrativos y tecnológicos

(Vaca et al., 2021). El área de Tecnologías de la Información y Comunicación administra sistemas críticos como bases de datos, servidores de red y plataformas de atención ciudadana, los cuales presentan vulnerabilidades derivadas de riesgos físicos, tecnológicos y humanos (KPMG, 2024; ISO, 2022; URM Consulting, 2025). El diagnóstico realizado evidencia un nivel de madurez bajo, controles técnicos básicos y procedimientos administrativos aislados, a pesar de contar con un esquema formal de gestión de seguridad que integra políticas, roles y mecanismos de evaluación continua (López & Martínez, 2021; Suárez & Torres, 2022).

El análisis demuestra la necesidad de estructurar procesos de gestión del riesgo, fortalecer la gobernanza digital y fomentar una cultura institucional orientada a la ciberseguridad (ICCS-ISAC, 2023; Rahman et al., 2024). Este estudio se desarrolla bajo un enfoque cualitativo y descriptivo, aplicando la metodología MAGERIT y el ciclo PHVA para mejorar la seguridad del área TIC, sustentado además en las directrices de gestión del riesgo establecidas en la norma ISO/IEC 27005 (Stoltz, 2024; Lozada & Méndez, 2023). Estas metodologías permiten organizar de manera sistemática los activos, amenazas y vulnerabilidades, proporcionando un diagnóstico técnico que fundamenta el diseño del SGSI (NIST, 2020; Alhazmi et al., 2024).

De esta manera, el proyecto se alinea con las mejores prácticas internacionales en ciberseguridad y contribuye al fortalecimiento de los procesos institucionales, sentando las bases para la implementación, auditoría y mejora continua de un Sistema de Gestión de Seguridad de la Información en el área TIC (DHS, 2023; Wang & Chen, 2024).

Metodología

La investigación se desarrolla conforme a la metodología MAGERIT dentro del ciclo PHVA propuesto por la norma ISO/IEC 27001:2022, que guía la mejora continua de los sistemas de gestión y constituye el fundamento metodológico de esta investigación (ISO, 2022; Prasetyo, 2023). La metodología mencionada permite la planificación de las medidas de seguridad, así como la disminución de riesgos mediante un diseño de SGSI para el área de TIC, garantizando seguridad y confiabilidad para el GAD Municipal de Santa Rosa.

El estudio adoptó un enfoque cualitativo y descriptivo, sustentado en una Revisión Sistemática de Literatura (RSL) desarrollada según la metodología PRISMA 2020 (Stoltz, 2024). Se establecieron criterios de inclusión y exclusión descartando fuentes duplicadas o sin evidencia empírica. De los diez documentos revisados, ocho cumplieron los criterios establecidos, permitiendo fundamentar el diseño del SGSI.

Los resultados de la RSL demostraron la complementariedad entre las normas ISO/IEC 27001, ISO/IEC 27005 y la metodología MAGERIT, herramientas útiles para el análisis e identificación de activos, amenazas y vulnerabilidades (Lozada & Méndez, 2023). Con fundamento en dichos hallazgos, se aplicó un esquema metodológico adaptado al contexto del área TIC del GAD Municipal de Santa Rosa, conforme a las siguientes fases del ciclo PHVA. En la fase de Planificar

se identificaron y clasificaron los activos de información mediante criterios de criticidad e impacto definidos en ISO/IEC 27005 y MAGERIT. La información se obtuvo a través de observación directa y entrevistas semiestructuradas a los responsables del área TIC (Vaca et al., 2021).

En la fase Hacer, se aplicó la valoración de riesgos, se elaboró la matriz de riesgos y el Plan de Tratamiento (PTR), estableciendo medidas y responsables (Wired, 2023).

En la fase de Verificar se construye una Declaración de Aplicabilidad (SoA) y se definen indicadores de desempeño (KPIs) para medir la efectividad de los controles (Alhazmi et al., 2024).

Finalmente, en la fase de Actuar se propuso un plan de mejora continua que se centra en la actualización de políticas, capacitaciones y la revisión de auditorías, garantizando la seguridad del SGSI y su alineación con el ciclo PHVA (Prasetyo, 2023; Wang & Chen, 2024).

El alcance del estudio se limita al diseño del SGSI para el área TIC del GAD Municipal de Santa Rosa, sin abordar su implementación ni certificación formal. Además, el modelo propuesto servirá como guía para futuras auditorías internas y evaluaciones de madurez organizacional.

Figura 1. Ciclo PHVA en el área de Tics

Ciclo PDCA aplicado al diseño del Sistema de Gestión de Seguridad de la Información (SGSI) del GAD Municipal de Santa Rosa

Fuente: González (2025).

Resultados

Como parte del proceso de análisis se aplica la metodología MAGERIT la cual ayuda a valorar los riesgos de una forma más estructurada y práctica. Gracias a este método se evalúa

cada activo considerando los criterios de confidencialidad, integridad y disponibilidad (CID), lo que determina el impacto que tendría una falla o ataque sobre los sistemas del GAD. Además, se asignaron niveles de probabilidad e impacto a los incidentes más comunes, logrando una visión más clara de los puntos críticos y medidas prioritarias que deben implementarse para reducir los riesgos.

Dentro de la investigación se presenta la situación actual de la seguridad de la información para el área TIC del GAD Municipal de Santa Rosa mediante la aplicación del ciclo PHVA y el marco de análisis establecido por la norma ISO/IEC 27005, se identificó los activos más importantes, las amenazas principales, las vulnerabilidades frecuentes y los controles necesarios para fortalecer la protección de la información institucional.

En la fase Plan, se elaboró un inventario completo de los activos de información, como equipos de cómputo, sistemas administrativos, bases de datos, servidores y el personal técnico encargado de su gestión facilitando la identificación y clasificación de los activos mediante una observación directa, entrevistas con el personal especializado quienes corroboraron la importancia crítica que tiene cada elemento considerando su valor informativo y su impacto en las operaciones de la entidad pública.

Los activos con mayor nivel de riesgo se presentan en la figura 2, corresponden a las bases de datos y servidores de red de la entidad pública como contraseñas débiles, falta de auditorías y controles de acceso. También se detectaron amenazas físicas como fallas eléctricas, incendios y amenazas tecnológicas como infecciones por malware y accesos no autorizados que podrían poner en riesgo la integridad y la disponibilidad de la información.

Figura 2. Identificación de activos críticos del área TIC.

Identificación de los activos		
No.	**Activo**	**Tipo de activo**
1	Documentos físicos	Información
2	Datos e información	Información
3	Base de datos GIS	Información
4	Servidores	Hardware
5	Computadores/Laptos	Hardware
6	Impresoras	Hardware
7	GPS	Hardware
8	Personal Administrativo	Recursos Humanos
9	Personal Técnico	Recursos Humanos
10	Red de área local e inalámbrica	Infraestructura
11	Página Web	Servicio Subcontratados
12	Software / aplicaciones GIS	Software

Fuente: González (2025).

Se realiza la valoración de los activos aplicando los criterios de confidencialidad, integridad y disponibilidad definidos en la norma ISO/IEC 27005 siguiendo la metodología MAGERIT. Los resultados presentados en la figura 3, los activos con valores de alto nivel corresponden al servidor principal de base de datos y al sistema administrativo, considerados como críticos para la continuidad de los servicios del área TIC.

Figura 3. Valoración de Activos

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	VALORACIÓN ACT	AMENAZA Conseq	VULNERABILIDAD	APLICA	PROBABILIDAD	PUNTAJE	IMPACTO	PUNTAJE	ORACIÓN RIE	CLASIFICACIÓN	PRIORIDAD
Riesgo tecnológico	HARDWARE	Computadores/ Laptos	15,40	Acceso no autorizado	Puertas traseras activas no detectadas	SI	ALTA	4	ALTO	4	16	ALTO	246,4
Riesgo tecnológico				Deficiencias en la organización	Evaluación poco cuidadosa de la fuerza de trabajo	SI	ALTA	4	ALTO	4	16	ALTO	246,4
Riesgo tecnológico				Caídas del sistema por agotamiento de recursos	Cálculo no adecuado de consumo de energía	SI	ALTA	4	ALTO	4	16	ALTO	246,4
Riesgo tecnológico				Divulgación de información	Falta de políticas de seguridad, acuerdos de confidencialidad	SI	ALTA	4	ALTO	4	16	ALTO	246,4
Riesgo tecnológico				Deterioro físico en el equipo	Mantenimiento no adecuado de equipos	SI	ALTA	4	ALTO	4	16	ALTO	246,4
Riesgo tecnológico				Manipulación de la configuración	Deficiente administración de usuarios y permisos	SI	ALTA	4	ALTO	4	16	ALTO	246,4
Riesgo tecnológico				Abuso de privilegios de acceso	Deficiente administración de usuarios y permisos	SI	ALTA	4	ALTO	4	16	ALTO	246,4
Riesgo tecnológico				Difusión de software dañino	Poco conocimiento de reglamento interno	SI	ALTA	4	ALTO	4	16	ALTO	246,4
Riesgo tecnológico				Modificación de la información	Mala administración de accesos físicos y lógicos	SI	ALTA	4	ALTO	4	16	ALTO	246,4

Fuente: González (2025).

En la fase Hacer, se desarrolla un proceso de diagnóstico y tratamiento de riesgos sobre los activos identificados. A partir de la valoración se elabora una matriz de riesgos que permite clasificar las amenazas según su probabilidad e impacto determinando el nivel de riesgo de cada activo. Con base en este análisis se diseñó el Plan de Tratamiento del Riesgo (PTR), donde se definieron las acciones de mitigación, responsables, plazos y los indicadores de seguimiento.

Como se presenta en la figura 4, las amenazas priorizadas se relacionan principalmente con accesos no autorizados, malware y fallos eléctricos, donde se plantea medidas de control como la implementación de autenticación multifactor, el fortalecimiento de contraseñas, la segmentación de red y la automatización de respaldos. En la grafico 2 se presenta el mapa de calor de riesgos evidenciando los eventos de niveles medio y alto, confirmando la necesidad de monitorear constante y fortalecer la capacidad de respuesta institucional frente a amenazas o riesgos.

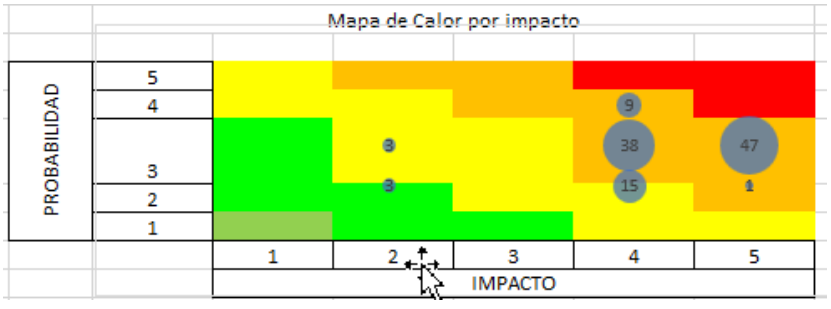
Los resultados del diagnóstico presentan un nivel de madurez bajo en la seguridad de la información del GAD Municipal de Santa Rosa, destacando fallos como controles de accesos, respaldo de información y auditorías. A pesar de ello, la aplicación del ciclo PHVA y las normas ISO/IEC 27001–27005 proporcionan un marco metodológico robusto para gestionar los riesgos y establecer controles apropiados para la situación municipal.

Figura 4. Identificación de amenazas y medidas de control

TIPO DE ACTIVO	ACTIVO	PROPIETARIO	CUSTODIO	VALOR DEL ACTIVO	AMENAZA	VULNERABILIDAD
INFORMACIÓN	Documentos físicos	DEPARTAMENTO TIC - GAD SANTA ROSA	GAD SANTA ROSA	14,96	Fuego	Edificación no apropiada y poco segura
					Daños por agua	Edificación no apropiada y poco segura
					Desastres naturales	Edificación no apropiada y poco segura
					Destrucción de la información	Corrupción
					Robo	Control de acceso insuficiente en el GAD
	Datos e información	DEPARTAMENTO TIC	GAD SANTA ROSA	14,96	Fuego	Edificación no apropiada y poco segura
					Daños por agua	Edificación no apropiada y poco segura
					Desastres naturales	Edificación no apropiada y poco segura
					Degradación de los soportes de almacenamiento de la información	Susceptibilidad de daño en almacenamiento de medios
					Errores de los usuarios	Entrenamiento de seguridad insuficiente
	Base de datos GIS	DEPARTAMENTO TIC	GAD SANTA ROSA	18,75	Vulnerabilidades de los programas	Instalación desinstalación no controlada
					Caídas del sistema por agotamiento de recursos	Cálculo no adecuado de consumo de energía
					Ataque destructivo	Mala administración de accesos físicos y lógicos
					Acceso no autorizado	Puertas traseras activas no detectadas
					Errores del administrador	Mantenimiento no adecuado de equipos
					Difusión de software dañado	Poco conocimiento de reglamento interno
HARDWARE	Servidores	GAD SANTA ROSA	GAD SANTA ROSA	18,75	Fuego	Edificación no apropiada y poco segura
					Daños por agua	Edificación no apropiada y poco segura
					Desastres naturales	Edificación no apropiada y poco segura
					Avería de origen físico o lógico	Mantenimiento no adecuado de equipos
					Errores de mantenimiento	Mantenimiento no adecuado de equipos
					Acceso no autorizado	Puertas traseras activas no detectadas
					Deficiencias en la organización	Evaluación poco cuidadosa de la fuerza de trabajo
					Caídas del sistema por agotamiento de recursos	Cálculo no adecuado de consumo de energía
					Divulgación de información	Falta de políticas de seguridad, acuerdos de confidencialidad
					Modificación de la información	Mala administración de accesos físicos y lógicos
					Robo	Escasa administración y monitoreo de recursos
	Computadores/Laptos	GAD SANTA ROSA	GAD SANTA ROSA	15,40	Fuego	Edificación no apropiada y poco segura
					Daños por agua	Edificación no apropiada y poco segura
					Desastres naturales	Edificación no apropiada y poco segura
					Errores de mantenimiento	Mantenimiento no adecuado de equipos
					Acceso no autorizado	Puertas traseras activas no detectadas
					Deficiencias en la organización	Evaluación poco cuidadosa de la fuerza de trabajo
					Abuso de privilegios de acceso	Deficiente administración de usuarios y permisos
					Difusión de software dañino	Poco conocimiento de reglamento interno
					Modificación de la información	Mala administración de accesos físicos y lógicos
	Impresoras	GAD SANTA ROSA	GAD SANTA ROSA	4,00	Fuego	Edificación no apropiada y poco segura
					Daños por agua	Edificación no apropiada y poco segura
					Desastres naturales	Edificación no apropiada y poco segura
					Errores de mantenimiento	Mantenimiento no adecuado de equipos
					Caídas del sistema por agotamiento de recursos	Cálculo no adecuado de consumo de energía
					Manipulación de la configuración	Deficiente administración de usuarios y permisos
	GPS	GAD SANTA ROSA	GAD SANTA ROSA	16,50	Daños por agua	Edificación no apropiada y poco segura
					Desastres naturales	Edificación no apropiada y poco segura
					Amenaza física	Edificación no apropiada y poco segura
					Robo	Escasa administración y monitoreo de recursos
RECURSOS HUMANOS	Personal Administrativo	GAD SANTA ROSA	GAD SANTA ROSA	15,40	Degradación de los soportes de	Susceptibilidad de daño en almacenamiento de medios
					Escapes de información	Falta de políticas de seguridad, acuerdos de confidencialidad
					Alteración de la información	Uso impropio/no controlado
					Destrucción de la información	Corrupción
					Divulgación de información	Falta de políticas de seguridad, acuerdos de confidencialidad
					Indisponibilidad del personal	Ausencia de personal
					Robo	Control de acceso insuficiente en el GAD
	Personal Técnico	GAD SANTA ROSA	GAD SANTA ROSA	15,40	Escapes de información	Falta de políticas de seguridad, acuerdos de confidencialidad
					Alteración de la información	Uso impropio/no controlado
					Destrucción de la información	Corrupción
					Divulgación de información	Falta de políticas de seguridad, acuerdos de confidencialidad
					Indisponibilidad del personal	Ausencia de personal
					Suplantación de la identidad del usuario	Ausencia de políticas de contraseñas
					Difusión de software dañado	Poco conocimiento de reglamento interno
					Modificación de la información	Mala administración de accesos físicos y lógicos
					Robo	Control de acceso insuficiente en el GAD
INFRAESTRUCTURA	Red de área local e inalámbrica	DEPARTAMENTO TIC - GAD SANTA ROSA	GAD SANTA ROSA	18,75	Fuego	Edificación no apropiada y poco segura
					Desastres naturales	Edificación no apropiada y poco segura
					Contaminación electromagnética	Líneas de comunicación no protegidas
					Corte del Suministro eléctrico	Fallos de hardware por voltaje inestable
					Fallo de servicios de comunicaciones	Acceso no autorizado a la red
					Errores de configuración	Entrenamiento de seguridad insuficiente
					Deterioro físico en el equipo	Mantenimiento no adecuado de equipos
					Acceso no autorizado	Puertas traseras activas no detectadas
					Ataque destructivo	Mala administración de accesos físicos y lógicos
SERVICIO SUBCONTRATADOS	Página Web	DEPARTAMENTO TIC - GAD SANTA ROSA	GAD SANTA ROSA	20,25	Vulnerabilidades de los programas	Instalación desinstalación no controlada
					Caídas del sistema por agotamiento de recursos	Cálculo no adecuado de consumo de energía
					Ataque destructivo	Mala administración de accesos físicos y lógicos
					Acceso no autorizado	Puertas traseras activas no detectadas
SOFTWARE	Software / aplicaciones GIS	DEPARTAMENTO TIC - GAD SANTA ROSA	GAD SANTA ROSA	18,75	Vulnerabilidades de los programas	Instalación desinstalación no controlada
					Caídas del sistema por agotamiento de recursos	Cálculo no adecuado de consumo de energía
					Ataque destructivo	Mala administración de accesos físicos y lógicos
					Acceso no autorizado	Puertas traseras activas no detectadas
					Errores del administrador	Mantenimiento no adecuado de equipos
					Difusión de software dañado	Poco conocimiento de reglamento interno
					Abuso de privilegios de acceso	Deficiente administración de usuarios y permisos
					Modificación de la información	Mala administración de accesos físicos y lógicos
					Destrucción de información	Corrupción
					Ingeniería social	Entrenamiento de seguridad insuficiente

Fuente: González (2025)

Figura 5. Mapa de calor de riesgos



Fuente: González, 2025

Se elabora la Declaración de Aplicabilidad (SoA) para los controles seleccionados del Anexo A de la norma ISO/IEC 27001:2022, justificando y recomendado cada control de riesgo identificado. La figura 6 presenta los riesgos y controles estableciendo una trazabilidad, vulnerabilidades y mecanismos de respuesta [27].

Figura 6. Declaración de aplicabilidad (extracto del SoA)

Se	Dominio, objetivos control y control	Aplicabilidad	Justificación	Recomendación implementación
6.1.1	Roles y responsabilidades para la seguridad de la Información.	Aplica	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	En el documento de políticas de seguridad y privacidad de la información debe ser revisada periódica como parte del mejoramiento continuo. (se sugiere una vez al año)
6.1.2	Separación de deberes.	Aplica	Roles y responsabilidades para la seguridad de la informacion	La separación de deberes se realiza de acuerdo al documento de roles y responsabilidades, así como en la segregación de funciones en seguridad de la información de cada proceso.
7.2.2	Concienciación, educación y capacitación en segur. de la informac.	Aplica	Se debe realizar actividades de concienciación, educación y capacitación en seguridad de la información a los usuarios de los sistemas	Con un personal capacitado habrá menos problemas de negligencia
7.3.1	Cese o cambio de puesto de trabajo.	Aplica	se deben implementar controles para el cese de personal o cambio de	Politicas de cambio de usuario y cese de labores
8.1.3	Uso aceptable de los activos	Aplica	Se deben identificar. documentar e implementar las reglas de uso acepiable de la información y de los activos asociados con los recursos para el tratamiento de la	Se tiene identificado y valorado los activos de información de la Institución de acuerdo con el alcance establecido del SGSI.Matriz de Riesgos.
8.3.3	Transferencia de medios físicos.	Aplica	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Se debe incorporar la seguridad de la información en el proceso transferencia documental para el traslado de medios físicos.
9.1.1	Política de control de acceso.	Aplica	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Se tiene definida la Política de control de acceso, se debe revisar y actualizar.
9.2.2	Suministro de acceso de usuarios.	Aplica	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y	Se ha incluido en la política de control de acceso de seguridad y privacidad de la Información.
9.2.3	Gestión de los derechos de acceso con privilegios especiales.	Aplica	Se debe revisar las funciones que se entregan a cada usuario dependiendo de su competencia.	Se debe revisar las funciones que se entregan a cada usuario dependiendo de su competencia.
9.2.5	Revisión de los derechos de acceso de los usuarios.	Aplica	Se debe implementar controles para la revisión de los derechos de acceso de los usuarios a los sistemas	Se debe implementar controles para la revisión de los derechos de acceso de los usuarios a los sistemas
9.2.6	Retirada o adaptación de los derechos de acceso	Aplica	Se debe retirar los accesos alos usuarios que ya hayan salido de la empresa o ya no necesiten acceso a funciones específicas del sistema.	Se debe retirar los accesos alos usuarios que ya hayan salido de la empresa o ya no necesiten acceso a funciones específicas del sistema.

Fuente: González (2025).

En la fase Verificar establece los criterios e indicadores de desempeño (KPIs) se encarga de evaluar que tan efectivos son los controles del SGSI, considerando métricas como el tiempo de detección en base a los incidentes, cumplimiento de políticas de acceso, tiempos de respaldos y continuidad de los servicios digitales. Los indicadores mencionados son importantes para ser consideradas en auditorías internas y en los procesos de mejora continua del sistema.

Figura 7. Evaluación de riesgo

TIPO DE RIESGO	TIPO DE ACTIVO	ACTIVO	VALORACIÓN ACT	AMENAZA Consec	VULNERABILIDAD	APLICA	PROBABILIDAD	PUNTAJE	IMPACTO	PUNTAJE	VALORACIÓN RIE	CLASIFICACIÓN	PRIORIDAD	CONTROL ISO 270	Solucion
Riesgo tecnológico	HARDWARE	Computadores/ Laptos	15,40	Acceso no autorizado	Puertas traseras activas no detectadas	SI	ALTA	4	ALTO	4	16	ALTO	246,4	9.1.1	Se deben realizar pruebas de funcionalidad durante el desarrollo de los sistemas en busca de posibles brechas de seguridad y documentar
Riesgo tecnológico				Deficiencias en la organización	Evaluación poco cuidadosa de la fuerza de trabajo	SI	ALTA	4	ALTO	4	16	ALTO	246,4	6.1.1	Se deben realizar pruebas de funcionalidad durante el desarrollo de los sistemas en busca de posibles brechas de seguridad y documentar
Riesgo tecnológico				Caídas del sistema por agotamiento de recursos	Cálculo no adecuado de consumo de energía	SI	ALTA	4	ALTO	4	16	ALTO	246,4	12.1.3	Se debe supervisar y ajustar la utilización de los recursos. asi corno realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido
Riesgo tecnológico				Divulgación de información	Falta de políticas de seguridad, acuerdos de confidencialidad	SI	ALTA	4	ALTO	4	16	ALTO	246,4	9.3.1	Se deben realizar pruebas de funcionalidad durante el desarrollo de los sistemas en busca de posibles brechas de seguridad y documentar
Riesgo tecnológico				Deterioro físico en el equipo	Mantenimiento no adecuado de equipos	SI	ALTA	4	ALTO	4	16	ALTO	246,4	8.3.1	Se deben realizar pruebas de funcionalidad durante el desarrollo de los sistemas en busca de posibles brechas de seguridad y documentar
Riesgo tecnológico				Manipulación de la configuración	Deficiente administración de usuarios y permisos	SI	ALTA	4	ALTO	4	16	ALTO	246,4	6.1.2	Se deben realizar pruebas de funcionalidad durante el desarrollo de los sistemas en busca de posibles brechas de seguridad y documentar
Riesgo tecnológico				Abuso de privilegios de acceso	Deficiente administración de usuarios y permisos	SI	ALTA	4	ALTO	4	16	ALTO	246,4	11.1.1	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de
Riesgo tecnológico				Difusión de software dañino	Poco conocimiento de reglamento interno	SI	ALTA	4	ALTO	4	16	ALTO	246,4	12.2.1	Se deben implementar controles para prevenir ataques externos por medio de software malicioso.
Riesgo tecnológico				Modificación de la información	Mala administración de accesos físicos y lógicos	SI	ALTA	4	ALTO	4	16	ALTO	246,4	9.2.2	Se deben realizar pruebas de funcionalidad durante el desarrollo de los sistemas en busca de posibles brechas de seguridad y documentar

Fuente: González (2025).

La figura 8 muestra la clasificación del riesgo identificada durante el diagnóstico: se suma la cantidad de riesgos identificados dividido al riesgo total de la evaluación donde el riesgo total es de 3,1612 de nivel alto. El resultado obtenido presenta la necesidad de reforzar los mecanismos de control preventivo, priorizando los activos críticos con mayor impacto.

Figura 8. Escala de Valoración

ESCALA DE VALORACIÓN						
Probabilidad	Impacto	Riesgo	Promedio	Clasificación	Cantidad	Riesgo Total
3	5	15	4	ALTO	47	188
2	5	10	3,5	ALTO	1	3,5
4	4	16	4	ALTO	9	36
3	4	12	3,5	ALTO	38	133
2	4	8	3	MEDIO	15	45
3	2	6	2,5	MEDIO	3	7,5
2	2	4	2	BAJO	3	6
3,612069	3,61206897				10	3,61206897
			Clasificación Riego Total			ALTO

Fuente: González (2025).

En la fase de Actuar presenta un sistema de retroalimentación para una mejora continua que contempla una revisión de políticas, revaluación de riesgos y actualización de controles en función de las auditorías internas. La figura 9 resume las acciones correctivas y preventivas recomendadas en base al ciclo PHVA.

Figura 9. Acciones de mejora continua y seguimiento

Cont	Actividad	Responsable	Registro	Tiemp	Recursos	Tratamiento del Riesgo
6.1.1	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Dirección de TIC	Documentación del SGSI	mes	Técnico (Cambio Sistema - Política)	Mitigar
6.1.2	Roles y responsabilidades para la seguridad de la informacion	Dirección de TIC	Documentación del SGSI	mes	Técnico (Cambio Sistema - Política)	Mitigar
7.2.2	Se debe realizar actividades de concienciación, educación y capacitación en seguridad de la información a los usuarios de los sistemas	Recursos Humanos - Dirección de TIC	Documentación del SGSI	mes	Humano (Capacitador)	Mitigar
7.3.1	se deben implementar controles para el cese de personal o cambio de puesto.	Recursos Humanos - Dirección de TIC	Documentación del SGSI	mes	Técnico (Cambio Sistema - Política)	Evitar
8.1.3	Se deben identificar. documentar e implementar las reglas de uso acepiable de la información y de los activos asociados con los recursos para el tratamiento de la información.	Activos Fijos - Dirección de TIC	Documentación de asignación de responsabilidad	mes	Técnico (Cambio Sistema - Política)	Mitigar
8.3.3	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Activos Fijos - Dirección de TIC	Documentación de asignación de responsabilidad	mes	Técnico (Cambio Sistema - Política)	Mitigar
9.1.1	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Dirección de TIC - Seguridad Movilidad y Riesgo	Documentación sobre descripción de los cargos	mes	Técnico (Cambio Sistema - Política)	Mitigar
9.2.2	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar	Dirección de TIC	Documentación sobre descripción de los cargos	mes		Mitigar

Fuente: González (2025).

Los resultados obtenidos en la valoración de riesgos y la aplicación del ciclo PHVA, se realiza un diseño de SGSI adaptado a las necesidades del área TIC del GAD Municipal de Santa Rosa. Este diseño se entiende como un sistema que está estructurado en procesos y roles permitiendo gestionar la seguridad de manera continua, medible y controlada.

El modelo propuesto se fundamenta en cuatro componentes principales:

Gobernanza y políticas: incluye la definición de una política institucional de seguridad de la información, aprobada por las autoridades del GAD, y la creación de un Comité de Seguridad de la Información encargado de supervisar el cumplimiento de los controles y coordinar auditorías internas.

“Gestión del riesgo: se compone del inventario de activos, la matriz de riesgos, el Plan de Tratamiento (PTR) y la Declaración de Aplicabilidad (SoA). Estos elementos permiten mantener la trazabilidad entre los activos, las amenazas y los controles aplicados”.

“Controles técnicos y operativos: abarca la implementación de medidas como autenticación multifactor, segmentación de red, copias de seguridad automatizadas, registro centralizado de eventos, endurecimiento de servidores y gestión de accesos por niveles”.

“Mejora continua: se basa en la revisión periódica de riesgos, la actualización del PTR y del SoA, así como en la evaluación de indicadores de desempeño (KPIs) para verificar la eficacia de los controles y proponer mejoras”.

El diseño presenta un proceso de análisis de todos los riesgos y vulnerabilidades garantizando una respuesta rápida ante cualquier amenaza y contemplarlas en el área de Tics.

Se establece una estructura de roles y responsabilidades, por el nivel de riesgo alto donde se debe aprobar y dar un seguimiento a los recursos y las políticas de seguridad, el personal de Tics ejecuta los controles técnicos, y el Comité de Seguridad realiza el seguimiento de cumplimiento y las auditorías.

En conjunto, el diseño del SGSI propuesto proporciona un marco organizativo y técnico que articula las fases del ciclo PHVA, asegurando la mejora continua, la protección de los activos de información e incidentes de ciberseguridad.

Discusión

Los resultados obtenidos reflejan que el GAD Municipal de Santa Rosa posee un nivel de riesgo alto (3,16) en la seguridad de la información, lo que coincide con investigaciones recientes desarrolladas en administraciones locales de América Latina, donde gran parte de los gobiernos municipales carecen de políticas consolidadas para la gestión del riesgo y el control de accesos (FQM, 2023; DHS, 2023). Este hallazgo, sustentado en la Tabla 1 y Tabla 2, demuestra que los activos más críticos, como las bases de datos y los sistemas administrativos, presentan los mayores niveles de vulnerabilidad, principalmente por la ausencia de controles formales y procedimientos documentados.

Los resultados obtenidos se relacionan directamente con la Revisión Sistemática de Literatura (RSL) desarrollada con la metodología PRISMA 2020, la cual permite identificar las principales debilidades en gobiernos locales. A partir de esta revisión, se observa que las instituciones públicas presentan problemas similares, como la falta de personal especializado y el incumplimiento de normas o estándares internacionales de seguridad (Stoltz, 2024).

Esta información fue clave para orientar el diseño del Sistema de Gestión de Seguridad de la Información, permitiendo adaptar las experiencias internacionales al contexto del GAD Municipal de Santa Rosa en el área de TIC. Los hallazgos de la RSL reforzaron las decisiones tomadas en las fases del ciclo PHVA, especialmente en la selección de controles y en la aplicación de la metodología MAGERIT para valorar los riesgos (DHS, 2023). El análisis sistemático sirvió como sustento teórico para justificar el diseño propuesto, asegurando que las acciones respondan a las necesidades del sector público (Suorsa, 2024).

La valoración de activos y la evaluación de riesgos que se presenta en la Tabla 4 con la normativa ISO/IEC 27005 establece una relación clara entre el impacto, las amenazas y la probabilidad, priorizando los recursos y esfuerzos técnicos según el nivel de exposición identificado. Tal como se visualiza en la grafico 2, el 74 % de los activos están expuestos en un nivel de riesgo alto, lo que sugiere la necesidad de crear controles operativos, ya que no existen procedimientos de supervisión o auditoría. Este hallazgo coincide con lo señalado por Alhazmi et al. (2024) y Lozada y Méndez

(2023), quienes destacan la importancia de aplicar metodologías basadas en la gestión del riesgo, especialmente en instituciones públicas que operan con presupuestos y personal limitado.

La aplicación del ciclo PHVA es una estrategia efectiva para la planificación, implementación, verificación y mejora de los controles de seguridad. En particular, la fase de Planificar realiza un inventario de activos y una trazabilidad de riesgos, mientras que la fase Hacer, como se visualiza en la Tabla 3, se relaciona con las amenazas identificadas y los controles técnicos basados en ISO/IEC 27001:2022, lo cual incluye el manejo de accesos, respaldos de información y el tratamiento de incidentes (ISO, 2022).

Asimismo, la integración de la metodología MAGERIT mejoró el análisis cualitativo del riesgo, permitiendo una comprensión más amplia e interconectada de los procesos institucionales y los activos tecnológicos. Este punto de vista concuerda con las propuestas de Vaca et al. (2021) y Rahman et al. (2024), que afirman que la combinación de metodologías complementarias y normas internacionales mejora la efectividad y sostenibilidad del SGSI en el sector público.

Tomando en cuenta la revisión sistemática de literatura basada en el método PRISMA 2020, los resultados de este caso se alinean con la evidencia que reconoce a ISO/IEC 27001 como una guía fundamental para la gestión de la información, la evaluación de riesgos y el fortalecimiento de una cultura institucional enfocada en la ciberseguridad (Toapanta et al., 2020; ICCS-ISAC, 2023; Stoltz, 2024). Por otro lado, los estudios que analizan entidades sin marcos estructurados evidencian tiempos de recuperación ante incidentes más prolongados y una capacidad menor para detectar amenazas (DHS, 2023).

Tal como se observa en la figura 7 y la figura 5, la implementación de acciones de mejora continua y el monitoreo de la vigilancia del riesgo permiten reducir las vulnerabilidades y fortalecer los activos institucionales. Este proceso de retroalimentación no solo garantiza que el SGSI siga vigente, sino también prepara a la entidad para una futura certificación bajo la norma ISO/IEC 27001, asegurando la continuidad operativa de los servicios municipales.

Finalmente, la sostenibilidad del SGSI dependerá de su actualización continua, la capacitación periódica del personal TIC y la integración del modelo en la planificación estratégica institucional, elementos que aseguran la continuidad operativa y el fortalecimiento progresivo del sistema de seguridad de la información.

Conclusión

El desarrollo de la investigación aplicando la metodología PHVA facilita el análisis y diseño de un modelo de SGSI orientado al área TIC del GAD Municipal de Santa Rosa. Los resultados confirman es un método eficaz para fortalecer la gobernanza digital en las instituciones públicas y la mejora continua en los procesos tecnológicos.

El análisis evidenció el nivel de madurez institucional en temas de seguridad de la información está en un nivel intermedio, con riesgos o amenazas relevantes relacionadas con el

control de accesos, la gestión de respaldos y la realización de auditorías internas. Sin embargo, la aplicación de las fases del ciclo PHVA permitió identificar los activos críticos, evaluar amenazas y vulnerabilidades y definir controles acordes a la normativa ISO/IEC 27001:2022 y la gestión del riesgo propuesta en la ISO/IEC 27005.

El análisis de riesgos presentado en la valoración de los activos en relación con el impacto y probabilidad como se visualiza en la Tablas 2 y 4, los activos más expuestos corresponden a los servidores de bases de datos y a los sistemas administrativos. Esto concluye la necesidad de aplicar medidas de protección, tales como la autenticación multifactor, los respaldos automatizados y la capacitación permanente del personal técnico.

De igual manera, la incorporación de la metodología MAGERIT fortalece la evaluación cualitativa de los riesgos a través de un enfoque basado en los principios de confidencialidad, integridad y disponibilidad (CID). Dicho enfoque resulta ser adecuado para el contexto de los gobiernos municipales o públicos, donde los recursos humanos y tecnológicos suelen ser limitados, pero la continuidad de los servicios digitales es vital.

Los resultados y el análisis comparativo presentado en el presente estudio, tomando en cuenta la revisión sistemática PRISMA 2020 no muestra lo importante de aplicar modelos estandarizados de ciberseguridad en las administraciones locales, ya que facilitan un proceso más eficiente de los recursos, asegurando la continuidad de los servicios digitales y fortaleciendo la confianza del personal y la ciudadanía en las instituciones públicas

En conclusión, la implementación del SGSI propuesto permitirá al GAD Municipal de Santa Rosa aumentar su estabilidad institucional y establecer una cultura organizacional orientada a la ciberseguridad a la mejora continua y la gobernanza digital, cumpliendo los estándares internacionales ISO/IEC 27001:2022 e ISO/IEC 27005.

Referencias

A-LIGN. (2025). *Everything you need to know about ISO 27001 certification*. A-LIGN Technical Brief.

Alhazmi, A., Shah, A., & Alghamdi, M. (2024). Enhancing information security management in public organizations using ISO 27001 framework. *IEEE Access, 12,* 8871–8885.

Baral, A., & Reynolds, T. (2024). Municipal cyber risk modeling using cryptographic computing to inform cyber policymaking. *arXiv Preprint*.

CISA. (2015). *Cybersecurity Information Sharing Act*.

Domestic Preparedness. (2024). Securing cities: The fight against local-level cyberthreats. *Domestic Preparedness Journal, 18*(4), 45–52.

Fédération Québécoise des Municipalités. (2023). *The economic impact of cyber attacks on municipalities*. FQM Report.

Figueroa, P. G., & González, J. L. (2024). Diagnóstico de la madurez en la gestión de la seguridad digital en gobiernos autónomos descentralizados. *Revista Científica UISRAEL, 9*(1), 92–104.

Hossain, S. T. (2025). Cybersecurity in local governments: A systematic review. *Government Information Quarterly, 42*(1), 55–72.

ICCS-ISAC. (2023). *Building a cybersecurity-aware culture in public sector organizations*. ICCS-ISAC Research Report.

ISO. (2022). *ISO/IEC 27001:2022 Information Security Management Systems — Requirements*. International Organization for Standardization.

Kitsios, F. (2023). The ISO/IEC 27001 Information Security Management: A critical examination. *Sustainability, 15*(7), 5828.

Kitsios, F., Kamariotou, M., & Douligeris, C. (2023). The ISO/IEC 27001 information security management system as a framework for improving organizational performance. *Sustainability, 15*(7), 5828–5845.

KPMG. (2024). *Cybersecurity considerations 2024: Government and public sector*. KPMG Global Insights.

Lozada, M. C., & Méndez, F. C. (2023). Gestión de riesgos informáticos en gobiernos locales: Enfoque basado en ISO 27001. *Revista Tecnológica ESPOL, 36*(1), 23–34.

Magnusson, L. (2025). Information security governance in the public sector: Investigations, approaches, measures, and trends. *International Journal of Information Security, 24*.

National Institute of Standards and Technology. (2020). *Special Publication 800-53 Rev. 5: Security and Privacy Controls for Federal Information Systems and Organizations*.

Norris, D. F., & Mateczun, L. K. (2023). *Cybersecurity in local government: A primer*. University of Maryland, Public Policy Center.

Prasetyo, A. O. (2023). An evaluation of the PHVA cycle in information security systems based on ISO 27001:2022. *Procedia Computer Science, 229,* 260–269.

Public Sector Assurance. (2022). *Public sector organizations use ISO/IEC 27001 to manage data securely*. International Accreditation Forum.

Rafiq, M. S., & Asif, H. (2024). Risk management practices in information security governance: A case study on municipal ICT systems. *International Journal of Information Security Science, 13*(1), 55–67.

Rahman, A., Islam, A., & Haque, N. (2024). Developing a cybersecurity culture through ISO 27001 implementation in local governments. *Journal of Information Security and Applications, 75*.

Ruggiero, A. F. (2022). Ransomware in local government: Risk factors and effects. *Issues in Information Systems, 23*(3), 103–112.

Santillán, J. J., & Vera, E. M. (2023). Evaluación de la madurez de la seguridad de la información en entidades públicas ecuatorianas. *Revista Ecuatoriana de Ciencia y Tecnología, 16*(2), 41–49.

Stoltz, M. (2024). The road to compliance: Executive federal agencies and the NIST risk management framework. *arXiv Preprint*.

Suárez, M., & Torres, E. (2022). Modelo de madurez para sistemas de gestión de seguridad de la información en gobiernos locales. *Revista Colombiana de Tecnologías de la Información, 13*(2), 51–63.

Suorsa, M. (2024). ISO/IEC 27001:2013 controls ranked based on GDPR compliance. *Journal of Cybersecurity and Privacy, 4*(2), 85–101.

Toapanta, S. M. T., Almeida, A. J., & Villavicencio, V. R. (2020). An approach of national and international cybersecurity laws and standards to mitigate information risks in public organizations of Ecuador. *ACM Digital Library*, (6), 61-66.

U.S. Department of Homeland Security. (2023). *Cyber Resilience Review (CRR): Method Description*.

URM Consulting. (2025). *ISO 27001:2022 – A.5 organisational controls*. URM Consulting.

Vaca, C., Alulema, D., & Jiménez, J. (2021). Evaluación de la seguridad informática en GADs del Ecuador. *Revista Ecuatoriana de Ciencia y Tecnología, 14*(2), 67–75.

Wall Street Journal. (2024). *Hack on North Miami tests ransom-payment bans.*

Wang, M. J., & Chen, L. (2024). Improving public sector cyber resilience through ISO 27001: Lessons from municipal deployments. *Government Information Quarterly, 41*(2).

Wired. (2023). *The untold story of a crippling ransomware attack: Hackney Council.*

Autores

Jorge Luis González Crespin. Ingeniero en Sistemas con experiencia en desarrollo e implementación de soluciones tecnológicas. Docente y Coordinador de TIC en el Instituto Ismael Pérez Pazmiño desde 2019. Participó en proyectos de transformación digital como el Sistema ATENEA y la Página Web Administrativa.

Daniel Jacobo Andrade Pesántez. Universidad Católica de Cuenca.

Declaración

Conflicto de interés

No tenemos ningún conflicto de interés que declarar.

Financiamiento

Sin ayuda financiera de partes externas a este artículo.

Nota

El artículo es original y no ha sido publicado previamente.