

UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

FACULTAD DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

DISEÑO DE UN MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL DEPARTAMENTO DE TI DEL GADICC, BASADO EN LA NORMA ISO/IEC 27001:2022.

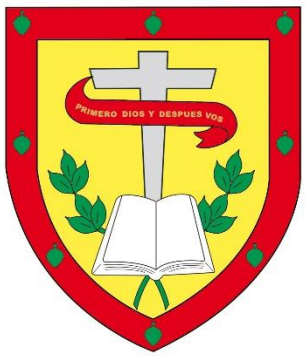
AUTOR: EMMANUEL DAVID VEGA ARCENTALES.

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILES.

CAÑAR - ECUADOR

2026

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

FACULTAD DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

DISEÑO DE UN MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL DEPARTAMENTO DE TI DEL GADICC, BASADO EN LA NORMA ISO/IEC 27001:2022.

PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

AUTOR: EMMANUEL DAVID VEGA ARCENTALES.

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILES.

CAÑAR - ECUADOR

2026

DECLARATORIA DE AUDITORÍA Y RESPONSABILIDAD

Yo, Emmanuel David Vega Arcentales portador de la cédula de ciudadanía N°**0302949011** Declaro ser la autora de la obra: **"Diseño de un manual de políticas de seguridad de la información para el departamento de TI del GADICC, basado en la norma ISO/IEC 27001:2022"** sobre la cual me hago responsable de las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cañar, 29 de septiembre 2026



Emmanuel David Vega Arcentales

C.I. 0302949011

CERTIFICADO DEL TUTOR

Certifico que el presente trabajo denominado "**Diseño de un manual de políticas de seguridad de la información para el departamento de TI del GADICC, basado en la norma ISO/IEC 27001:2022**" realizado por **Emmanuel David Vega Arcentales** con documento de identidad No. **0302949011**, previo a la obtención del título profesional de Ingeniero en Sistemas de Información, ha sido asesorado, supervisado y desarrollado bajo mi tutoría en todo su proceso, cumpliendo con la reglamentación pertinente que exige la Universidad Católica de Cuenca y los requisitos que determina la investigación científica.

Cañar, 29 de septiembre 2026

Ing. Cristhian Humberto Flores Urgiles

DIRECTOR DEL TRABAJO INVESTIGATIVO

UNIVERSIDAD CATÓLICA DE CUENCA EXTENSIÓN CAÑAR

DEDICATORIA

Dedico este trabajo de titulación, con profundo amor y gratitud, a mis padres, quienes han sido un pilar fundamental a lo largo de mi vida y, especialmente, durante los cuatro años de mi formación universitaria.

A ellos, por su apoyo incondicional, por la confianza depositada en mí y por acompañarme en cada etapa de este camino. Gracias por sus consejos, sus enseñanzas y por brindarme la fortaleza necesaria para continuar incluso en los momentos difíciles. Su presencia y respaldo han sido fundamentales para alcanzar esta meta, que representa no solo la culminación de una etapa académica, sino también el fruto de un esfuerzo compartido.

Este logro es también suyo, pues detrás de cada paso que he dado se encuentra su amor, sus sacrificios y el deseo de verme crecer personal y profesionalmente. Por todo lo que han hecho por mí, y por ser una fuente constante de inspiración en mi vida, les dedico este trabajo con todo mi cariño, respeto y eterna gratitud.

AGRADECIMIENTO

Quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi vida y a toda mi familia por estar siempre presentes.

A la Universidad Católica de Cuenca, Extensión Cañar, y de manera particular a la Carrera de Ingeniería de Sistemas de Información, por los conocimientos, experiencias y valores adquiridos durante mi formación académica.

Al Ing. Jhovany Santacruz Espinoza, subdirector de la Carrera, por su gestión, apoyo y constante disposición para atender las necesidades de los estudiantes durante nuestro proceso formativo. Extiendo mi gratitud al cuerpo docente, que con su dedicación, profesionalismo y vocación compartió sus conocimientos y contribuyó a mi crecimiento académico y personal, así como al personal administrativo, por su amabilidad, colaboración y oportuna atención en cada uno de los trámites y requerimientos a lo largo de la carrera.

De manera especial, expreso mi agradecimiento al Ing. Cristhian Flores Urgiles, director de este trabajo de investigación, por su orientación, acompañamiento, paciencia y rigurosidad académica. Sus valiosas observaciones y recomendaciones fueron fundamentales para el desarrollo y culminación de la presente investigación.

RESUMEN

El Gobierno Autónomo Descentralizado Intercultural del Cantón Cañar (GADICC) gestiona información institucional y ciudadana sin políticas formales de seguridad, lo que expone sus activos a riesgos operativos y normativos. La presente investigación tuvo como objetivo diseñar un manual de políticas de seguridad de la información para el departamento de Tecnologías de la Información del GADICC, basado en la norma ISO/IEC 27001:2022. Se aplicó un enfoque mixto de predominancia cualitativa, con nivel descriptivo-propositivo y diseño no experimental transversal, bajo la modalidad de proyecto factible. El diagnóstico se realizó mediante una encuesta de 63 ítems alineados a los controles de la norma ISO/IEC 27002:2022, análisis documental y un análisis de riesgos con la metodología MAGERIT v3. Los resultados evidenciaron un cumplimiento general del 69,8 %, con las mayores brechas en los dominios de seguridad física y ambiental (37,5 %), aspectos organizativos (50,0 %) y gestión de activos (60,0 %). De los 50 activos inventariados, 25 alcanzaron un valor global muy alto o crítico, siendo el riesgo más severo las condiciones ambientales inadecuadas del cuarto de servidores. A partir de estos hallazgos se estructuró un manual con catorce políticas organizadas en los dominios organizacional, de personas, físico y tecnológico, cada una con objetivo, alcance, directrices, procedimiento de implementación, responsable y mecanismo de revisión. Se concluye que el manual constituye un instrumento normativo aplicable que fortalece la confidencialidad, integridad y disponibilidad de los activos de información institucionales.

Palabras clave: seguridad de la información, ISO/IEC 27001:2022, políticas de seguridad, análisis de riesgos, MAGERIT.

ABSTRACT

The Decentralized Intercultural Autonomous Government of the Cañar Canton (GADICC) manages institutional and citizen information without formal security policies, which exposes its assets to operational and regulatory risks. This research aimed to design an information security policy manual for the GADICC Information Technology Department, based on the ISO/IEC 27001:2022 standard. A mixed-methods approach with a predominantly qualitative focus was applied, using a descriptive-propositional level and a non-experimental cross-sectional design, within the framework of a feasibility project. The diagnosis was conducted using a 63-item survey aligned with the controls in the ISO/IEC 27002:2022 standard, documentary analysis, and a risk analysis using the MAGERIT v3 methodology. The results showed an overall compliance rate of 69.8%, with the largest gaps in the areas of physical and environmental security (37.5%), organizational aspects (50.0%), and asset management (60.0%). Of the 50 assets inventoried, 25 received an overall rating of very high or critical, with the most severe risk being inadequate environmental conditions in the server room. Based on these findings, a manual was developed containing fourteen policies organized into the organizational, human resources, physical, and technological domains, each with an objective, scope, guidelines, implementation procedure, designated person in charge, and review mechanism. It is concluded that the manual constitutes an applicable policy framework that strengthens the confidentiality, integrity, and availability of institutional information assets.

Keywords: information security, ISO/IEC 27001:2022, security policies, risk analysis, MAGERIT.

INDICE

CONTENIDO

Declaratoria de auditoría y responsabilidad ..... **¡Error! Marcador no definido.**
CERTIFICADO DEL TUTOR..... **¡Error! Marcador no definido.**
DEDICATORIA IV
AGRADECIMIENTO VI
Resumen VII
ABSTRACT VIII
INDICE IX
INDICE DE TABLAS XIII
INDICE DE ILUSTRACIONES XIV
INTRODUCCIÓN XV
CAPÍTULO I 1
1.1. Planteamiento del problema 1
1.1.1. Formulación del problema 3
1.2. Antecedentes de la Investigación 4
1.3. Justificación de la investigación 6
1.4. Objetivos 6
1.1.2. Objetivo General 6
1.1.3. Objetivos Específicos 7
1.5. Limitaciones 8
1.6. Delimitaciones 8
CAPÍTULO II 9
2. MARCO TEÓRICO 9
2.1. Seguridad de la información 9
1.1.4. Concepto e importancia de la seguridad de la información 9
1.1.5. Principios fundamentales de la seguridad de la información 10
2.2. Sistema de Gestión de Seguridad de la Información (SGSI) 12
2.2.1. Concepto del SGSI 12
2.2.2. Objetivos de un SGSI 12
2.2.3. Beneficios de implementar un SGSI 13
2.2.4. Ciclo de mejora continua PHVA aplicado al SGSI 13
2.3. Norma ISO/IEC 27001:2022 14

2.3.1. Estructura de la norma ISO/IEC 27001:2022 14
2.3.2. Requisitos del Sistema de Gestión de Seguridad de la Información 15
2.4. Políticas de seguridad de la información 19
2.4.1. Definición de políticas de seguridad 19
2.4.2. Importancia de un manual de políticas de seguridad 19
2.4.3. Características de una política de seguridad efectiva 19
2.4.4. Componentes de un manual de políticas de seguridad 21
2.5. Controles de seguridad de la información según ISO/IEC 27002:2022 22
2.5.1. Controles organizacionales 22
2.5.2. Controles relacionados con personas 22
2.5.3. Controles físicos 23
2.5.4. Controles tecnológicos 23
2.6. Gestión de riesgos de seguridad de la información 23
2.6.1. Concepto de riesgo 23
2.6.2. Amenazas 24
2.6.3. Vulnerabilidades 24
2.6.4. Activos de información 24
2.6.5. Tratamiento del riesgo 25
2.7. Metodologías para análisis y gestión de riesgos 25
2.7.1. ISO/IEC 27005 25
2.7.2. MAGERIT 29
2.7.3. NIST Cybersecurity Framework 32
2.8. Contextualización del GADICC 35
CAPÍTULO III 36
3. MARCO METODOLÓGICO 36
3.1. Enfoque de la investigación 36
3.2. Nivel de la investigación 36
3.3. Diseño de la investigación 37
3.4. Población y muestra 37
3.5. Técnicas e instrumentos de recolección de datos 37
3.6. Interpretación de resultados 38
3.7. Análisis de la norma ISO 27001:2022 46
3.7.1. Dominio Políticas de la seguridad de la información 46

3.7.2. Dominio Aspectos organizativos de la seguridad de la información 47
3.7.3. Dominio Seguridad ligada a los recursos humanos 48
3.7.4. Dominio Gestión de activos 49
3.7.5. Dominio Control de accesos 50
3.7.6. Dominio Seguridad física y ambiental 51
3.7.7. Dominio Seguridad en la operativa 52
3.7.8. Dominio Seguridad en las telecomunicaciones 53
3.7.9. Dominio Gestión de incidentes de seguridad de la información 54
3.7.10. Dominio Cumplimiento 55
3.7.11. Análisis general de la encuesta 56
3.8. Selección de la metodología 57
CAPÍTULO IV 58
4. PROPUESTA 58
4.1. Introducción 58
4.2. Determinación del riesgo con MAGERIT 59
4.2.1. Identificación de Activos de Información 59
4.2.2. Valoración de los activos 63
4.2.3. Identificación de las Amenazas 66
4.2.4. Evaluación de Impacto y Probabilidad 67
4.2.5. Cálculo del riesgo 68
4.2.6. Controles de Seguridad 70
4.2.7. Resumen de la matriz de riesgo 71
4.3. Directrices o políticas para la seguridad de la información 72
4.3.1. Políticas del dominio organizacional 72
4.3.2. Políticas del dominio de personas 80
4.3.3. Políticas del dominio físico 81
4.3.4. Políticas del dominio tecnológico 84
Conclusiones 88
recomendaciones 90
Referencias 92
ANEXOS 97
Anexo 1: Protocolo de Investigación 97
Anexo: Formato del Anteproyecto. 97

Bibliografía 109

INDICE DE TABLAS

Tabla 1. Requisitos de la ISO/IEC 27001:2022: Fuente: Elaborado en base a la (nqa, 2026)..... 16
Tabla 2. Matriz de respuestas obtenidas con la norma ISO/IEC 27001:2022..... 39
Tabla 3. Inventario de activos de información del departamento de TI del GADICC... 60
Tabla 4. Escala de valoración de activos MAGERIT..... 63
Tabla 5. Valoración de los activos de información del departamento de TI del GADICC. D = Disponibilidad; I = Integridad; C = Confidencialidad; A = Autenticidad; T = Trazabilidad; VG = Valor global (máximo de las cinco dimensiones). Escala 0-10. 64
Tabla 6. Catálogo de amenazas MAGERIT aplicable a los activos prioritarios 67
Tabla 7. Escala de calificación del impacto. 67
Tabla 8. Escala de calificación de la probabilidad. 68
Tabla 9. Escala de interpretación del nivel de riesgo 68
Tabla 10. Matriz de riesgo de los activos prioritarios del departamento de TI del GADICC 69
Tabla 11. Controles de seguridad aplicables a los riesgos prioritarios identificados en el departamento de TI del GADICC..... 70

INDICE DE ILUSTRACIONES

Ilustración 1. Seguridad de la información. Fuente: Elaborado por (Conect LTDA, 2024) 9
Ilustración 2. Norma ISO/IEC 27001:2022. Fuete: (drmunozcl, 2025) 14
Ilustración 3. Componentes de un manual de políticas de seguridad. Fuente: Elaboración en base (nqa, 2026) 21
Ilustración 4. Fases de la metodología. Fuente: (Ortiz-Lazo y Vizñay-Duran , 2019) .. 27
Ilustración 5. Ventajas de la ISO/IEC 27005. Fuente: Elaboración Propia. 28
Ilustración 6. Desventajas de la ISO/IEC 27005. Fuente: Elaboración Propia. 29
Ilustración 7. Fases de la metodología. Fuente: (Sánchez, 2026) 31
Ilustración 8. Ventajas y Desventajas de la metodología MAGERIT. Fuente: Elaboración propia. 32
Ilustración 9.Fases de la metodología NIST. Fuente: (NIST, 2024) 34
Ilustración 10. Ventajas y desventajas de NIST. Fuente: Elaboración en base a (Díaz, 2023) 35

INTRODUCCIÓN

La información constituye hoy uno de los activos más valiosos de las instituciones públicas. En los gobiernos autónomos descentralizados del Ecuador, la transformación digital ha incrementado el volumen de datos institucionales y ciudadanos que se gestionan, y con ello la exposición a amenazas como accesos no autorizados, fugas de información, fallos técnicos y ataques informáticos. Garantizar la confidencialidad, integridad y disponibilidad de esos datos ya no es únicamente una preocupación técnica, sino una obligación normativa y una condición para la continuidad de los servicios y la confianza de la ciudadanía.

El Gobierno Autónomo Descentralizado Intercultural del Cantón Cañar (GADICC) administra, a través de su departamento de Tecnologías de la Información, los sistemas de gestión institucional, las bases de datos ciudadanas, la red interna, la infraestructura de servidores y los servicios digitales municipales. Sin embargo, la gestión de la seguridad de la información en este departamento se realiza de manera informal: no existen políticas documentadas, controles formalizados ni procedimientos definidos para la clasificación de la información, el control de accesos o la respuesta ante incidentes. Esta situación se produce en un contexto en el que la Ley Orgánica de Protección de Datos Personales y el Esquema Gubernamental de Seguridad de la Información exigen al sector público contar con mecanismos de seguridad alineados a estándares internacionales.

Frente a esta problemática, la presente investigación tiene como objetivo diseñar un manual de políticas de seguridad de la información para el departamento de TI del GADICC, basado en la norma ISO/IEC 27001:2022 y en los controles del Anexo A de la norma ISO/IEC 27002:2022. Para ello se adopta un enfoque mixto de predominancia cualitativa, con nivel descriptivo-propositivo y diseño no experimental transversal, bajo la modalidad de proyecto factible. El diagnóstico se sustenta en una encuesta de

cumplimiento aplicada al departamento, en el análisis documental de la normativa aplicable y en un análisis de riesgos desarrollado con la metodología MAGERIT v3, que permite identificar y valorar los activos de información, sus amenazas y el nivel de riesgo asociado.

El documento se organiza en cuatro capítulos. El Capítulo I presenta el planteamiento del problema, los antecedentes, la justificación, los objetivos y el alcance de la investigación. El Capítulo II desarrolla el marco teórico sobre seguridad de la información, el Sistema de Gestión de Seguridad de la Información, la norma ISO/IEC 27001:2022, los controles de la ISO/IEC 27002:2022 y las metodologías de análisis de riesgos ISO/IEC 27005, MAGERIT y NIST. El Capítulo III describe el marco metodológico y expone los resultados del diagnóstico de cumplimiento por dominio de control. El Capítulo IV contiene la propuesta: la determinación del riesgo con MAGERIT y las políticas de seguridad definidas. Finalmente, se presentan las conclusiones, las recomendaciones y, como anexo, el manual de políticas de seguridad de la información resultante.

CAPÍTULO I

1.1. Planteamiento del problema

En la actualidad, la información se ha consolidado como uno de los activos estratégicos más valiosos para las organizaciones públicas y privadas. Su gestión adecuada, en términos de confidencialidad, integridad y disponibilidad, resulta indispensable para garantizar la continuidad operativa, el cumplimiento normativo y la confianza ciudadana en los servicios gubernamentales (Podrecca, Culot, Nassimbeni , & Sartor, 2022). La transformación digital de los gobiernos locales ha incrementado significativamente el volumen de datos institucionales gestionados y, con ello, la exposición a amenazas como accesos no autorizados, fugas de información, errores humanos y ataques informáticos.

El Gobierno Autónomo Descentralizado Intercultural del Cantón Cañar (GADICC) es un organismo público que gestiona los recursos y servicios municipales y administra las operaciones del cantón. El departamento de Tecnologías de la Información del GADICC administra los sistemas de gestión institucional, bases de datos ciudadanas, red e infraestructura, computación personal y servicios digitales. Sin embargo, la gestión de la seguridad de la información por parte de este departamento se realiza de manera informal, sin políticas documentadas, controles formalizados ni procedimientos para incidentes de seguridad (Villarreal Morales, Coro Villarreal, Fernández Sánchez, & Cueva Martinez, 2024).

La Ley Orgánica Ecuatoriana para la Protección de Datos Personales (LOPDP) exige que el sector público cuente con protocolos de seguridad que cumplan con estándares internacionales. El Esquema de Seguridad de la Información Gubernamental (EGSI) v2.0 se basa en la norma ISO/IEC 27001, continuando desde 2021. Esto establece estándares mínimos de seguridad que todas las instituciones públicas en

Ecuador y los gobiernos autónomos descentralizados deben adoptar. Si no se cumplen estos estándares, puede haber consecuencias administrativas, el público puede perder confianza en los servicios digitales del GADICC y se puede perder información crítica (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021).

La infraestructura tecnológica del departamento de TI de GADICC incluye servidores, sistemas financieros y administrativos, bases de datos ciudadanas, una red interna, computadoras y sistemas de acceso remoto. Estos bloques no cuentan con controles de seguridad formales documentados, lo que genera algunas vulnerabilidades. No existen formas expresas de clasificar y gestionar la información institucional. Los sistemas empresariales y las bases de datos tienen un control inconsistente del acceso y privilegios de los usuarios. No hay formas documentadas expresas para identificar y responder a problemas de seguridad. Además, no existen controles de seguridad formales documentados relacionados con el uso aceptable de los recursos de TI y no hay formas expresas de realizar copias de seguridad y recuperación de datos.

Sin un manual de política de seguridad de la información, el departamento de TI parece manejar sus propios problemas de seguridad y tomar decisiones relacionadas con la seguridad de manera improvisada e individual. Manejar los problemas de seguridad de esta manera pone en riesgo las operaciones del servicio público, así como la integridad de los registros institucionales y la privacidad de los datos de los ciudadanos en GADICC.

La norma ISO/IEC 27001:2022 propone un enfoque sistemático para la gestión de la seguridad de la información que incluye la definición de políticas, objetivos de seguridad, controles y un ciclo de mejora continua, constituyendo el marco de referencia idóneo para el diseño del manual propuesto (International Organization for Standardization; International Electrotechnical Commission, 2022).

Esta situación plantea la siguiente pregunta de investigación: ¿Cómo diseñar un manual de políticas de seguridad de la información, basado en la norma ISO/IEC 27001:2022, que permita al departamento de TI del GADICC establecer lineamientos formales y controles adecuados para la protección de los activos de información institucional?

1.1.1. *Formulación del problema*

Actualmente, el departamento de Tecnologías de la Información del Gobierno Autónoma Descentralizado Intercultural del Cantón Cañar no cuenta con un manual de políticas de seguridad de la información, lo que significa que no existen estrategias documentadas oficialmente para salvaguardar los activos gubernamentales, como sistemas de administración, bases de datos y redes y servicios de TIC. Debido a la ausencia de estrategias documentadas, la seguridad de los sistemas de información se gestiona de manera informal. Como el departamento no tiene políticas documentadas, no se implementa ningún medio formal de control de seguridad, ni existen medios establecidos para la clasificación y seguridad de la información, seguridad de acceso y del usuario, copias de seguridad y restauración de la información y los sistemas, y gestión de incidentes. Esto expone al departamento y a los servicios gubernamentales a los riesgos de acceso no autorizado a la información, pérdida de información, alteración de la información, filtraciones de información, y el deterioro resultante de los servicios del gobierno en relación con las obligaciones legales y de servicio, especialmente en lo que respecta a la confianza del público en la gestión digital de los servicios gubernamentales del GADICC.

¿Cómo puede el departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado Intercultural del Cantón Cañar desarrollar un manual de políticas de seguridad de la información basado en la norma ISO/IEC 27001:2022 para diseñar

marcos de políticas y controles de seguridad formales y adecuados que protejan la información gubernamental?

1.2. Antecedentes de la Investigación

Silva et al, (2023), en su investigación titulada *"A worldwide overview on the information security posture of online public services"*, realizaron un análisis global sobre estado de la seguridad de la información dentro de los servicios públicos digitales fue examinado minuciosamente. Dentro de esta evaluación de plataformas gubernamentales en línea, se analizaron aspectos como la comunicación segura, los certificados digitales y las exposiciones a vulnerabilidades conocidas. Utilizando un método cuantitativo, este análisis abarcó 3,068 dominios gubernamentales de los estados miembros de la ONU. A partir del análisis, se determinó que, incluso con la expansión de los servicios públicos digitales, muchas instituciones gubernamentales aún carecen de un nivel adecuado de adopción de marcos internacionales, junto con estándares de seguridad y mejores prácticas. Tal situación representa un riesgo para la protección de datos de los ciudadanos, así como para la continuidad de los servicios públicos. Considerando estos problemas, surge la necesidad de establecer marcos formales de gestión de la seguridad de la información dentro de las instituciones públicas, una necesidad que está específicamente relacionada con el desarrollo del diseño del manual de políticas para el departamento de TI de GADICC.

Domínguez et al. (2023), en el estudio denominado *"Evaluation of an information security management system at a Mexican higher education institution"*, en el estudio "Evaluación de un sistema de gestión de seguridad de la información en una institución de educación superior mexicana" en conjunto con la norma ISO/IEC 27001. Este estudio se centró en el grado de conocimiento de la dirección, el nivel de capacitación del personal

y la eficiencia de los procesos relacionados con la gestión de riesgos de seguridad. La investigación fue cuantitativa y utilizó instrumentos de encuesta para la muestra de 81 individuos. Estos individuos eran miembros del personal administrativo y técnico del área de tecnología de la información. Los resultados identificaron brechas en la capacitación del personal, la gestión de riesgos de seguridad y la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). La investigación describió los riesgos de incidentes de seguridad derivados de una estructura organizacional poco clara. Esta investigación amplía la comprensión de la necesidad de contar con información documentada, responsabilidades definidas y procedimientos formales. Estos son algunos de los elementos sugeridos en el manual de seguridad para GADICC.

Flores & Perugachi (2023), investigadores de la Escuela Politécnica Nacional del Ecuador, desarrollaron el estudio "A GDPR-compliant Risk Management Approach based on Threat Modelling and ISO 27005". El enfoque basado en riesgos propuesto aquí incorpora consideraciones de protección de datos personales en la interacción de ISO 27005 como marco de gestión de riesgos, junto con los controles de ISO 27001 y ISO 27002. Esto es relevante para el presente estudio porque demuestra cuán importante es la identificación de amenazas y evaluación de riesgos, así como la selección de controles de seguridad, en el diseño de políticas institucionales.

El Ministerio de Telecomunicaciones y de la Sociedad de la Información (2023), establece regulaciones nacionales sobre telecomunicaciones, tecnologías de la información y seguridad de la información. Este documento describe el papel del ministerio en el desarrollo de políticas, directrices y planes para el sector público. Esto también es importante para el proyecto y las instituciones públicas trabajantes, ya que GADICC es una institución pública y necesita directrices de políticas formales para mejorar la seguridad de los activos informativos.

1.3. Justificación de la investigación

El presente proyecto tiene como finalidad diseñar un manual de políticas de seguridad de la información para el departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado Intercultural del Cantón Cañar (GADICC), tomando como referencia la norma ISO/IEC 27001:2022, los controles de la ISO/IEC 27002:2022 y los lineamientos del Esquema Gubernamental de Seguridad de la Información (EGSI). Para ello, se realizará un diagnóstico del estado actual de la gestión de seguridad mediante entrevistas al personal técnico, revisión documental y evaluación de controles existentes, permitiendo identificar activos críticos, riesgos, vulnerabilidades y brechas relacionadas con la confidencialidad, integridad y disponibilidad de la información institucional.

A partir de los resultados obtenidos, se definirán políticas de seguridad alineadas con los controles aplicables de la norma ISO/IEC 27002:2022, considerando aspectos como gestión de accesos, protección de datos, copias de seguridad, respuesta a incidentes, continuidad operativa y asignación de responsabilidades. Como resultado, se estructurará un manual que incluirá directrices, responsables, controles asociados y mecanismos de revisión, proporcionando al departamento de TI del GADICC un instrumento normativo para fortalecer la gestión de seguridad de la información. El proyecto se limita al diseño del manual y no contempla su implementación operativa, adquisición de herramientas tecnológicas, pruebas técnicas de seguridad ni auditorías de certificación.

1.4. Objetivos

1.1.2. *Objetivo General*

Diseñar un manual de políticas de seguridad de la información para el departamento de TI del GADICC, basado en la norma ISO/IEC 27001:2022, mediante el diagnóstico de la situación actual de seguridad, la identificación de controles aplicables

del Anexo A de la norma ISO/IEC 27002:2022 y la definición de políticas formales alineadas al estándar internacional, con el fin de fortalecer la confidencialidad, integridad y disponibilidad de los activos de información institucional.

1.1.3. *Objetivos Específicos*

- Construir el marco teórico sobre seguridad de la información, políticas de seguridad organizacional y la norma ISO/IEC 27001:2022, mediante la revisión sistemática de literatura científica, normativa vigente y marcos de referencia internacionales, para fundamentar el diseño del manual de políticas de seguridad del departamento de TI del GADICC.

- Diagnosticar el estado actual de la gestión de seguridad de la información en el departamento de TI del GADICC, mediante entrevistas al personal técnico, análisis documental y evaluación de los controles de seguridad existentes frente a los requerimientos de la norma ISO/IEC 27001:2022, con el fin de identificar las principales brechas y áreas de mejora.

- Definir las políticas de seguridad de la información alineadas a los controles del Anexo A de la norma ISO/IEC 27002:2022, a través del análisis de riesgos y de las brechas identificadas en el diagnóstico, para establecer lineamientos formales y apropiados que protejan los activos de información del departamento de TI del GADICC.

- Estructurar el manual de políticas de seguridad de la información del departamento de TI del GADICC, mediante la integración de las políticas definidas, los procedimientos de implementación, los roles y responsabilidades, y los mecanismos de revisión y actualización, para proveer un instrumento normativo que oriente la gestión segura de la información institucional.

1.5. Limitaciones

- El acceso a más información institucional será más difícil, ya que algunos documentos o datos técnicos pueden estar clasificados como reservados o confidenciales.
- La disponibilidad de personal de TI puede afectar la recopilación de información como parte de las entrevistas y la evaluación de la situación existente.
- La disponibilidad de tiempo no será el suficiente para completar los objetivos con total eficacia.

1.6. Delimitaciones

- El estudio será solo sobre el departamento de Tecnologías de la Información de GADICC y no analizará ningún otro departamento o las áreas operativas de la institución.
- Esta investigación analizará la creación de políticas de seguridad de la información. El marco de referencia será la norma ISO/IEC 27001:2022.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Seguridad de la información

Figura 1

Seguridad de la información.



Nota. Fuente: Elaborado por (Conect LTDA, 2024)

1.1.4. *Concepto e importancia de la seguridad de la información*

La seguridad de la información se refiere a las medidas empleadas para salvaguardar los datos y recursos de información de una organización contra amenazas que provienen del interior y del exterior de la organización. La seguridad de la información tiene como objetivo preservar el valor de la información de la organización durante su creación, almacenamiento, procesamiento, transmisión y eliminación. Esto se logra mediante la definición de varias políticas, controles, procedimientos y responsabilidades. Los marcos y estándares de seguridad permiten estructurar la gestión de riesgos, control y los requisitos de protección de la organización (Taherdoost, 2022).

1.1.5. *Principios fundamentales de la seguridad de la información*

Los principios fundamentales de la seguridad de la información establecen las bases para determinar el grado necesario de protección de los activos organizacionales. Tradicionalmente, estos componentes se agrupan en confidencialidad, integridad y disponibilidad. Sin embargo, con la evolución de los sistemas, las organizaciones priorizan la inclusión de autenticidad, responsabilidad y no repudio, ya que los sistemas y las organizaciones modernas están obligados a identificar a los usuarios, registrar acciones y mostrar la responsabilidad en la disposición de la información (Stallings & Brown, 2021).

a. Confidencialidad

La confidencialidad de la información consiste en proteger los datos confidenciales del acceso, difusión o uso no autorizado. Este principio exige la aplicación de múltiples mecanismos como la autenticación, gestión de privilegios, encriptación, clasificación de la información y contratos de confidencialidad. La violación de este principio puede resultar en filtraciones de datos, exposición de información institucional, pérdida de confianza y consecuencias legales (Whitman & Mattord, 2022)

b. Integridad

La integridad garantiza que la información sea completa y precisa, y que permanezca inalterada por individuos no autorizados a acceder a ella durante toda la vida útil de la información. Este principio aborda la fiabilidad de los registros institucionales, bases de datos, estados financieros, documentos administrativos y sistemas de transacciones. Para protegerlo, se implementan diversos controles como validación de datos, registros de auditoría, control de cambios, firmas digitales, copias de seguridad y segregación de funciones (Joint Task Force, 2020).

c. Disponibilidad

La disponibilidad significa el grado en que la información y los servicios de tecnología de la información pueden ser accedidos por usuarios autorizados. Este principio está alineado con la continuidad de las operaciones, el mantenimiento de los sistemas, las copias de seguridad, la redundancia, la recuperación ante incidentes y la defensa contra interrupciones. El ransomware, los ataques de denegación de servicio (DoS) y las fallas en la infraestructura son algunas de las amenazas a la disponibilidad. Todos estos son actualmente algunos de los riesgos altos identificados en relación con el estado de la ciberseguridad (European Union Agency for Cybersecurity., 2024).

d. Autenticidad

La autenticidad denota el grado en que un usuario, sistema, proceso o documento es genuino y representativo de sus afirmaciones. En el contexto de la seguridad de la información, la aplicabilidad de este principio es amplia. Satisface la necesidad de la validación de identidades. Ayuda en la protección de transacciones, la regulación de sesiones y la garantía de que las acciones realizadas en un sistema sean llevadas a cabo por sujetos y procesos legítimos. Los mecanismos empleados para garantizar este principio de seguridad son, en la mayoría de los casos, el uso de credenciales seguras, autenticación multifactor, certificados digitales y firmas electrónicas (Anderson, 2020).

e. Trazabilidad y no repudio

La trazabilidad permite la documentación y reconstrucción de las operaciones realizadas en sistemas, datos o recursos tecnológicos. La no repudio, por otro lado, elimina la posibilidad de que un usuario niegue sus acciones pasadas. Los conceptos de Trazabilidad y el no repudio son similares en su uso de registros, marcas de tiempo, registros de auditoría, firmas digitales y una variedad de mecanismos de monitoreo. Son vitales para realizar investigaciones exhaustivas de incidentes, atribuir responsabilidades

y proporcionar evidencia tanto en auditorías internas como externas (Joint Task Force, 2020).

2.2. Sistema de Gestión de Seguridad de la Información (SGSI)

2.2.1. Concepto del SGSI

Un SGSI establece las políticas y procedimientos de una empresa para la identificación y clasificación de sus recursos de información, evaluación de los riesgos relativos a esos recursos y costos de y métodos para la aplicación de la mitigación de riesgos, así como el avance continuo de la seguridad de la información dentro de la empresa. A diferencia de muchos sistemas de seguridad de la información, un SGSI integra los aspectos técnicos, humanos y organizativos de la seguridad de la información. Un SGSI está destinado a proteger la información de manera que sea coherente con el entorno en el que opera la empresa, los objetivos del negocio, el estado de la ley y las preocupaciones de las partes interesadas de la empresa (Domínguez-Domínguez, Flores-Laguna, & Valle-López, 2023).

2.2.2. Objetivos de un SGSI

Los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI) se orientan a salvaguardar la privacidad de los datos, la gestión de riesgos, el cumplimiento de leyes, la seguridad de las operaciones comerciales y la construcción de confianza entre las partes interesadas. Además, permite la implementación de controles documentados relacionados con la seguridad, roles definidos y estrategias de evaluación que ayudan en las decisiones relacionadas con la seguridad. La implementación de sistemas de gestión de seguridad está relacionada con la mejora de los sistemas y operaciones y con el valor añadido para las partes interesadas (Podrecca, Culot, Nassimbeni , & Sartor, 2022)

2.2.3. Beneficios de implementar un SGSI

El SGSI construye marcos para la formalización de políticas. Ayuda a reducir riesgos, mejorar la respuesta a incidentes, asignar responsabilidades, cumplir con las regulaciones y proteger los activos críticos. Con un SGSI en marcha, se pueden integrar y documentar diferentes formas de control de acceso, sistemas de respaldo, seguridad física, sistemas para la gestión de incidentes y sistemas para acciones correctivas. La mejora de un SGSI puede medirse con responsabilidades definidas y marcos procedimentales modificables (Ali, 2026).

2.2.4. Ciclo de mejora continua PHVA aplicado al SGSI

El SGSI está sujeto a un monitoreo continuo y a un perfeccionamiento activo cuando se utiliza el ciclo PDCA (Planificar, Hacer, Verificar, Actuar). La planificación implica la identificación de riesgos, objetivos y el control de los mismos. La siguiente fase, Hacer, implica la puesta en práctica de las políticas y procedimientos pertinentes. En la fase Verificar, se evalúa el rendimiento mediante auditorías, métricas o revisiones. En la fase Final, Actuar, se llevan a cabo las acciones correctivas necesarias. El uso de esta metodología fomenta la mejora del nivel de madurez necesario para abordar las brechas identificadas en las evaluaciones de seguridad (Kurniawan, Riadi, Irmawan, & Arusani, 2022)

2.3. Norma ISO/IEC 27001:2022

Figura **2**

Norma ISO/IEC 27001:2022.



Nota. Fuete: (drmunozcl, 2025)

ISO/IEC 27001 es el Marco de Estándar Internacional para los Sistemas de Gestión de la Seguridad de la Información (SGSI). Este marco describe las prácticas y requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema para gestionar riesgos relacionados con la seguridad de la información. La mejora continua, basada en riesgos protege la información que una organización posee y, mediante el cumplimiento, protege la información que una organización procesa (ISO, 2026).

2.3.1. Estructura de la norma ISO/IEC 27001:2022

ISO/IEC 27001:2022 adopta la mayor parte de la estructura de las normas de sistemas de gestión. Estas incluyen el contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del rendimiento y mejora. Tener esta estructura simplifica la integración del SGSI con otros sistemas de gestión en la

organización y ayuda a organizar las funciones y procesos, así como la evidencia necesaria para gestionar la seguridad de la información. También permite la elaboración de políticas y procedimientos con controles alineados y verificables (nqa, 2026).

2.3.2. Requisitos del Sistema de Gestión de Seguridad de la Información

Los requisitos del SGSI crean el marco para establecer un sistema de gestión de seguridad formal en toda la organización que tenga en cuenta el compromiso de la gestión, los riesgos, los recursos disponibles y el funcionamiento del control. También se consideran las evaluaciones de desempeño y la naturaleza iterativa del sistema. Estos requisitos protegen la seguridad ya que no es únicamente responsabilidad del departamento de TI. En cambio, el departamento de TI, las personas y los procesos involucrados son todos responsables de la seguridad (Ali, 2026).

La norma ISO/IEC 27001:2022 establece requisitos para los componentes de un Sistema de Gestión de la Seguridad de la Información que, desde la perspectiva institucional, permiten organizar la seguridad teniendo en cuenta el contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del rendimiento y procesos de mejora. Estos requisitos y su relación con el diseño del manual de políticas de seguridad de la información se describen en la Tabla 1.

Tabla 1

Requisitos de la ISO/IEC 27001:2022:

Requisito del SGSI	Descripción	Elementos principales	Aplicación en el manual de políticas
Contexto de la organización	Consiste en identificar factores internos y externos que pueden afectar la seguridad de la información. También permite reconocer las necesidades de las partes interesadas y delimitar el alcance del SGSI.	Factores internos y externos, partes interesadas, alcance del SGSI, activos, procesos, usuarios, proveedores y servicios.	Permite definir qué activos, procesos y servicios del departamento de TI deben ser protegidos mediante políticas formales.
Liderazgo	Requiere que la alta dirección demuestre compromiso con la seguridad de la información mediante la aprobación de políticas, asignación de responsabilidades, provisión de recursos y supervisión del desempeño.	Compromiso directivo, aprobación de políticas, asignación de roles, recursos y seguimiento.	Establece responsables para aprobar, cumplir, supervisar y actualizar las políticas de seguridad de la información.

Requisito del SGSI	Descripción	Elementos principales	Aplicación en el manual de políticas
Planificación	Se orienta a identificar riesgos y oportunidades, definir objetivos de seguridad y establecer acciones para alcanzarlos. Relaciona amenazas, vulnerabilidades y activos críticos con controles adecuados.	Riesgos, oportunidades, objetivos de seguridad, amenazas, vulnerabilidades, activos críticos y controles.	Facilita la selección de políticas prioritarias según los riesgos identificados en el departamento de TI.
Soporte	Comprende los recursos, competencias, comunicación e información documentada necesarios para implementar y mantener el SGSI. Incluye capacitación, documentación y disponibilidad de personal técnico.	Recursos, competencias, comunicación, documentación, formación y personal técnico.	Define los documentos, responsables, medios de comunicación y evidencias necesarias para aplicar el manual.
Operación	Corresponde a la ejecución de los procesos planificados para gestionar riesgos y aplicar controles de seguridad. Incluye evaluación y tratamiento de riesgos, control de accesos, respaldos, gestión de incidentes, seguridad física y monitoreo.	Evaluación de riesgos, tratamiento del riesgo, control de acceso, copias de seguridad, incidentes, seguridad física y monitoreo.	Permite transformar las políticas en procedimientos operativos aplicables y verificables dentro del área de TI.

Requisito del SGSI	Descripción	Elementos principales	Aplicación en el manual de políticas
Evaluación del desempeño	Permite medir la eficacia del SGSI mediante indicadores, auditorías internas, revisiones por la dirección y análisis de cumplimiento. Determina si los controles funcionan y si las políticas son aplicadas correctamente.	Indicadores, auditorías internas, revisión por la dirección, análisis de cumplimiento y medición de controles.	Establece mecanismos para revisar el cumplimiento y efectividad de las políticas incluidas en el manual.
Mejora continua	Permite corregir desviaciones, actualizar políticas, fortalecer controles y adaptar el SGSI frente a cambios tecnológicos, regulatorios o institucionales. Evita que la seguridad sea estática.	Acciones correctivas, actualización documental, fortalecimiento de controles, brechas y mejora progresiva.	Define la periodicidad y criterios para revisar, ajustar y mejorar el manual de políticas de seguridad.

Nota. Fuente: Elaborado en base a la (nqa, 2026)

2.4. Políticas de seguridad de la información

2.4.1. Definición de políticas de seguridad

Una política de seguridad articula las expectativas que una organización tiene para sus usuarios de información y los controles de seguridad y comportamiento que la organización considera necesarios para mitigar el riesgo a su información. Una política de seguridad utiliza reglas de acceso, restricciones de uso del sistema, reglas de protección de datos, reglas de respaldo y respuesta a incidentes, y constructos de confidencialidad y responsabilidad para establecer expectativas. La efectividad de una política depende de que el personal comprenda la política, perciba que la política es aplicable y reciba instrucciones sobre cómo cumplir con la política (Haney & Lutters, 2023).

2.4.2. Importancia de un manual de políticas de seguridad

Consolidar las directrices institucionales de protección de información, un manual de políticas de seguridad es fundamental para contener la dispersión regulatoria, decisiones improvisadas y proporcionar una base común a usuarios, técnicos y personal administrativo. También ofrece un vínculo de controles, funciones y evidencias. Las encuestas sobre conciencia de seguridad indican que las políticas y programas de seguridad ya no deben ser formalidades, sino diseñados para influir en el comportamiento real del personal (Hielscher & Parkin, 2024).

2.4.3. Características de una política de seguridad efectiva

Las características según Haney y Lutters (2023) son las siguientes:

- El documento debe ser fácil de leer y usar. Se deben eliminar las ambigüedades que afecten la usabilidad del documento. Además, los programas de seguridad deben abordar el desafío de ir más allá del cumplimiento formal hacia cambios sustantivos en las actitudes y comportamientos.

- Debe relacionarse con las prácticas reales de la organización, considerando sus sistemas, usuarios, recursos y actividades. Los desafíos de seguridad ocurren tanto por deficiencias técnicas como por políticas y procesos articulados de manera inadecuada.
- Las responsabilidades deben delinearse claramente para gerentes, personal técnico, usuarios y terceros. Esto indicará quién aprueba, ejecuta, supervisa y cumple con cada disposición, y mostrará que la colaboración, la comprensión colectiva y la participación impactan en el cumplimiento de las políticas de seguridad.
- Los protocolos y regulaciones de seguridad deben ser específicos y medibles para informar y guiar a los usuarios respecto a comportamientos que puedan mantenerlos seguros. En lugar de campañas breves de concienciación sobre seguridad, la comunicación a los empleados debe ser frecuente y más atractiva; debe incorporar acciones de concienciación.
- La evaluación de políticas implica reconocer la medida del cumplimiento de los controles presidiarios, la evidencia de verificación e identificar brechas. Debe prever la verificación del cumplimiento mediante evidencia, registros y controles relacionados o auditorías internas.
- Debe cumplir con controles, estándares y prácticas establecidas para que sus disposiciones no sean, como en muchos de los sistemas cuasi-legales, empíricas, y que la automatización de la defensa y la política de aplicación se integren con la capacidad de implementar contramedidas específicas.
- Además, debe ser evaluada y revisada de forma rutinaria a la luz de nuevos desafíos y cambios en tecnología, legislación, incidentes, etc. La evolución de la seguridad debe llevar a la organización más allá del simple cumplimiento

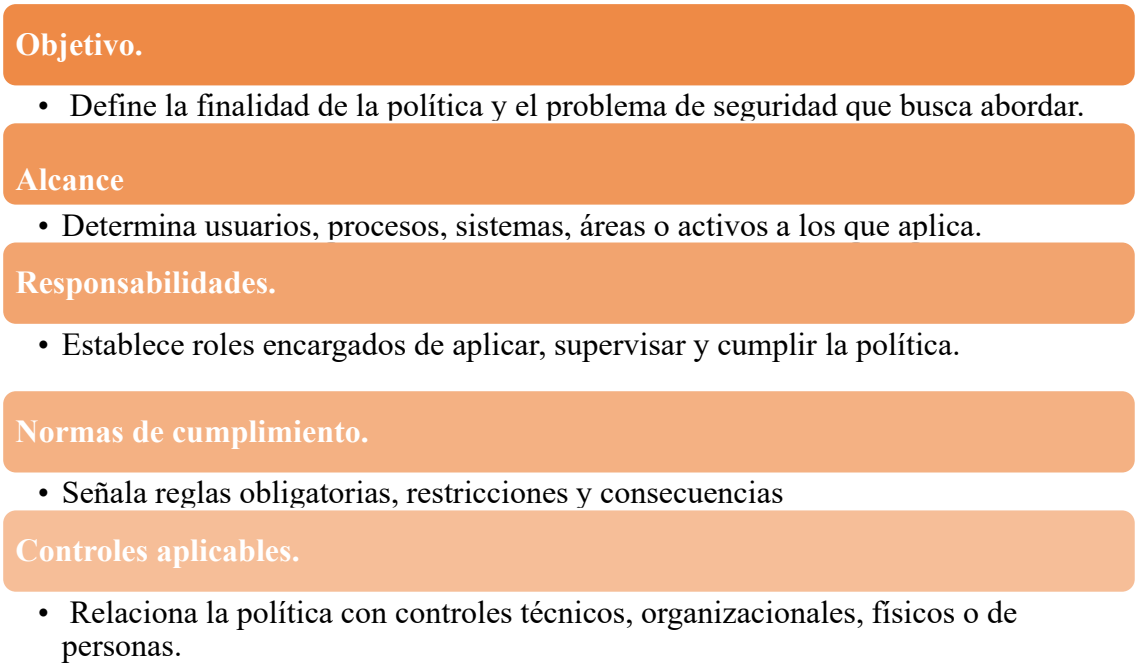
formal y hacia prácticas con efectos observables en relación con el personal (Hielscher & Parkin, 2024).

2.4.4. Componentes de un manual de políticas de seguridad

Para comprender, implementar y validar las políticas de seguridad individuales, un manual de políticas de seguridad debe contener los elementos mínimos necesarios. Estos incluyen el propósito, la aplicabilidad, las responsabilidades integradas, los mecanismos de cumplimiento y los controles pertinentes. También debe describir la evidencia, la frecuencia de las revisiones y la conexión con los riesgos descritos. La investigación sobre el cumplimiento de las políticas de seguridad sugiere que la intención de los usuarios de cumplir se ve afectada por la clarificación de responsabilidades, la participación del personal y la presencia de mecanismos de monitoreo (Condoy & Vizñay, 2021).

Figura 3

Componentes de un manual de políticas de seguridad.



Nota. Fuente: Elaboración en base (nqa, 2026)

2.5. Controles de seguridad de la información según ISO/IEC 27002:2022

Los procedimientos de control de seguridad de la información permiten tomar acciones específicas con las medidas de seguridad para mitigar riesgos a los activos de la compañía. En el caso de la ISO/IEC 27002:2022, los controles de seguridad pueden clasificarse en cuatro categorías: controles relacionados con la organización, las personas, el edificio y la tecnología. Esta política ayuda a facilitar el diseño de la defensa de seguridad, ya que ayuda a resumir los riesgos en procedimientos para proporcionar medidas de seguridad a los procesos, personas, edificios y sistemas (International Organization for Standardization; International Electrotechnical Commission, 2022).

2.5.1. Controles organizacionales

Los controles organizativos abordan la gobernanza de la seguridad, la asignación de responsabilidades, la gestión de activos, la clasificación de la información, las relaciones con proveedores, la continuidad y la respuesta a incidentes. Estos controles proporcionan la base que dirige y coordina las medidas técnicas que se pueden implementar dentro del marco de una institución. Al integrar controles de seguridad en los sistemas de gestión, se ilustra el papel dominante de la gobernanza y la asignación de responsabilidades para mantener un esquema de seguridad duradero (Enríquez, 2024).

2.5.2. Controles relacionados con personas

Los controles relacionados con los empleados aseguran que el personal y otros con relaciones laborales con la empresa desarrollen una comprensión de sus derechos y responsabilidades antes, durante y después de su relación con la empresa. La concienciación, la educación, los acuerdos de confidencialidad, los términos de empleo y los procesos de salida representan algunos de estos controles. Los empleados causan la mayoría de los incidentes relacionados con la seguridad ya sea por cometer errores o por

desconocimiento y no cumplimiento de las reglas y prácticas establecidas (Enríquez, 2024).

2.5.3. Controles físicos

Los controles físicos protegen varios activos al limitar el acceso a ciertas áreas y equipos. Los controles físicos consisten en sistemas de acceso de seguridad, sistemas de videovigilancia, seguridad ambiental, seguridad del equipo y procedimientos para visitantes. El objetivo de estos controles es proteger los sistemas que almacenan y procesan la información sensible de la institución contra pérdida, daño, robo y acceso no autorizado (Enríquez, 2024)

2.5.4. Controles tecnológicos

Los controles tecnológicos salvaguardan diversos componentes y capas de sistemas y servicios, incluyendo la infraestructura y la protección de identidades y comunicaciones. Algunos de los controles son autenticación y controles de acceso, gestión de vulnerabilidades, protección de copias de seguridad, monitoreo y encriptación. Al considerar también la protección mediante configuraciones seguras, actualizaciones y la gestión de vulnerabilidades, las tecnologías de protección deben mantenerse a lo largo de todo el ciclo de vida del software y la infraestructura relacionada (Enríquez, 2024)

2.6. Gestión de riesgos de seguridad de la información

La gestión de riesgos es el proceso de identificar, evaluar y abordar cualquier riesgo financiero, legal, estratégico y de seguridad para una organización (IBM, 2026).

2.6.1. Concepto de riesgo

El riesgo se refiere a un evento que puede ocurrir y que sería perjudicial para una empresa y sus objetivos. En cuanto a la seguridad de la información, el riesgo ocurre cuando una amenaza explota una vulnerabilidad con impacto en la confidencialidad, integridad o disponibilidad de un activo. Una evaluación es la capacidad de determinar el

impacto de un evento de riesgo (si ocurre), la probabilidad/riesgo y las medidas de control que se deben adoptar respecto al riesgo (Finn & Downie, 2026).

2.6.2. Amenazas

Las amenazas se refieren a aquellos eventos agentes que pueden dañar los sistemas de información y las redes. Las amenazas pueden ser intencionales: ransomware, phishing, robo de credenciales, no intencionales: error humano o incluso ambientales cortes de energía, desastres naturales. Los informes de incidentes de seguridad muestran que las credenciales comprometidas, los errores humanos y los ataques a aplicaciones son algunas de las causas más comunes de violaciones de seguridad (Rios, 2024).

2.6.3. Vulnerabilidades

Las vulnerabilidades se refieren a debilidades explotables de un sistema u organización. Estas debilidades técnicas, humanas o estructurales pueden manifestarse en software sin supervisar, obsoleto o mal configurado, procedimientos de seguridad o privilegios de usuario. La gestión de vulnerabilidades generalmente consiste en reconocer y describir aspectos de un sistema que pueden ser potencialmente dañados y desarrollar métodos para mitigarlos (Rios, 2024).

2.6.4. Activos de información

Los activos de información deben ser protegidos porque proporcionan a una o varias organizaciones un recurso importante. Las listas completas de activos de información pueden incluir sistemas, documentos, bases de datos, servidores, software de aplicaciones, sistemas de credenciales, equipos, redes, servicios digitales y conocimientos. Además, la identificación y clasificación de los activos implican la protección del ciclo de vida de los activos de información, ya que proporcionan la definición de controles y niveles de criticidad y criticidad del activo, así como de sus propietarios (Ortiz, 2022).

2.6.5. Tratamiento del riesgo

El tratamiento del riesgo consiste en seleccionar acciones para reducir, aceptar, transferir o evitar los riesgos identificados. En seguridad de la información, el tratamiento suele materializarse mediante políticas, controles, procedimientos, capacitación, respaldo, monitoreo y mejoras tecnológicas. La selección de controles debe considerar el nivel de riesgo, el costo, la viabilidad y el impacto sobre los procesos institucionales (Ortiz, 2022).

2.7. Metodologías para análisis y gestión de riesgos

2.7.1. ISO/IEC 27005

ISO/IEC 27005:2022 es una guía para gestionar los riesgos de seguridad de la información específicamente para la ayuda en la implementación, mantenimiento y desarrollo gradual de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001. Este enfoque ayuda a identificar, analizar, evaluar, tratar y/o comunicar de manera sistemática los riesgos que puedan poner en peligro la confidencialidad, integridad y/o disponibilidad de la información. Algunos enfoques crean métodos estrictos, pero el enfoque de ISO/IEC 27005 es adaptable a las necesidades, tamaño, contexto y fase de desarrollo de la organización. También tiene una relación con la norma ISO 31000, ofreciendo sus principios generales de gestión de riesgos y abordando la seguridad de la información (International Organization for Standardization, 2022)

a. Características

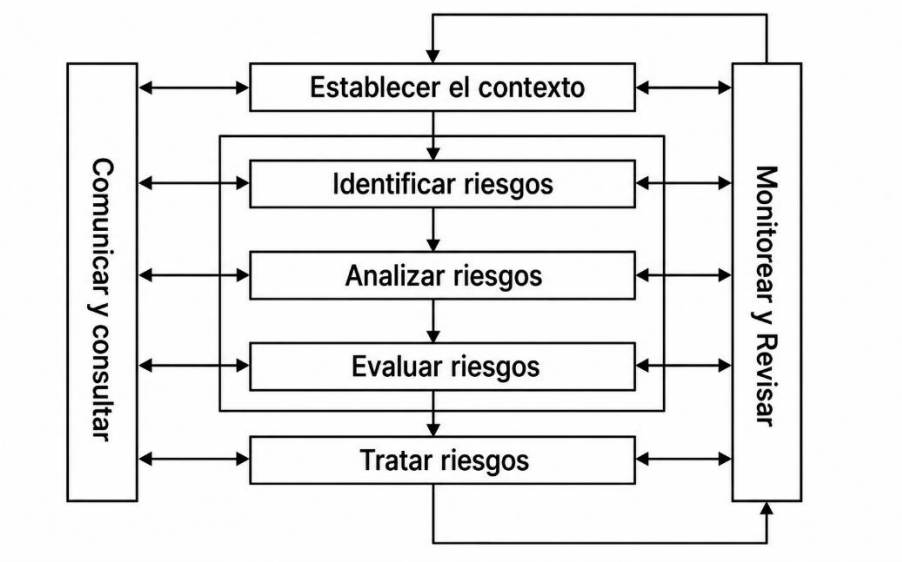
La metodología ISO/IEC 27005 es popular para la gestión del riesgo de seguridad de la información, por buenas razones lo afirma el Ministerio de Tecnologías de la Información y las Comunicaciones (2025):

- Esta metodología permite la identificación de amenazas y la evaluación de la probabilidad de vulnerabilidad a incidentes de seguridad de los activos de información.
- Esta metodología ayuda a cumplir con el requisito de la ISO/IEC 27001 para la evaluación y tratamiento de riesgos, mientras proporciona el establecimiento e implementación de un SGSI.
- Esta norma considera la gestión del riesgo como un ejercicio continuo de revisión y revisión de riesgos y de ajuste continuo a medida que cambian las condiciones internas y externas de la organización.
- ISO/IEC 27005 ofrece a la organización la opción de usar técnicas cualitativas, cuantitativas o una combinación de ambas para la evaluación de riesgos, y no prescribe una metodología particular.
- El marco de evaluación de riesgos de ISO/IEC 27005 es aplicable a organizaciones de cualquier tipo y tamaño, incluyendo las del sector público y privado.
- Esta norma ayuda a determinar el grado de exposición a riesgos de la organización para dirigir los recursos en la implementación de controles de seguridad**.**

b. Fases de la metodología

Figura 4

Fases de la metodología.



Nota. Fuente: (Ortiz-Lazo y Vizñay-Duran , 2019)

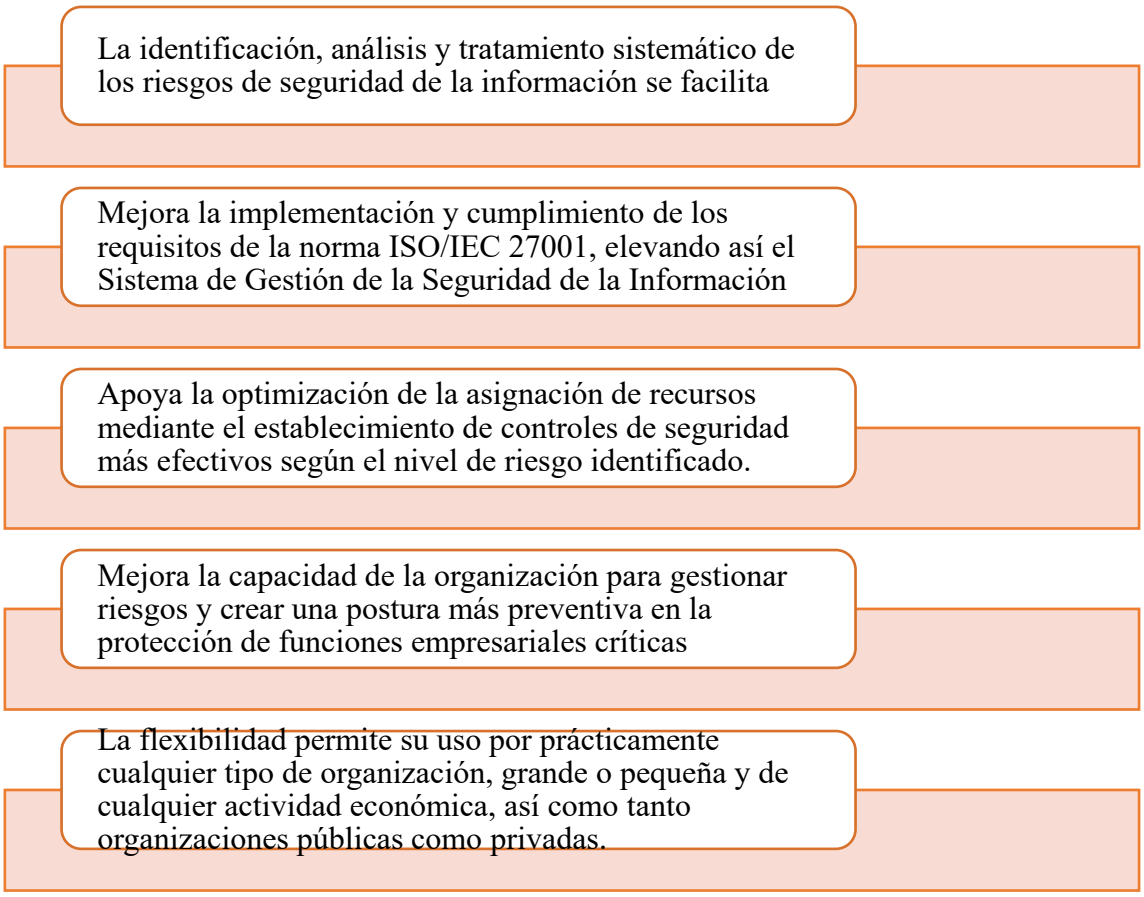
La metodología de gestión de riesgos es un proceso continuo que comienza con el establecimiento del contexto, donde se definen los objetivos, el alcance y los criterios de evaluación; posteriormente se identifican los posibles riesgos, se analizan según su probabilidad e impacto y se evalúan para determinar cuáles requieren atención prioritaria. Después se seleccionan acciones para evitarlos, reducirlos, transferirlos o aceptarlos. Durante todas las etapas se debe mantener una comunicación constante con las partes interesadas y realizar un monitoreo y revisión periódicos, con el fin de verificar la eficacia de los controles, detectar cambios y actualizar las medidas necesarias para asegurar el cumplimiento de los objetivos.

c. Ventajas y desventajas

Los siguientes son algunos de los beneficios clave de la metodología:

Figura 5

Ventajas de la ISO/IEC 27005.

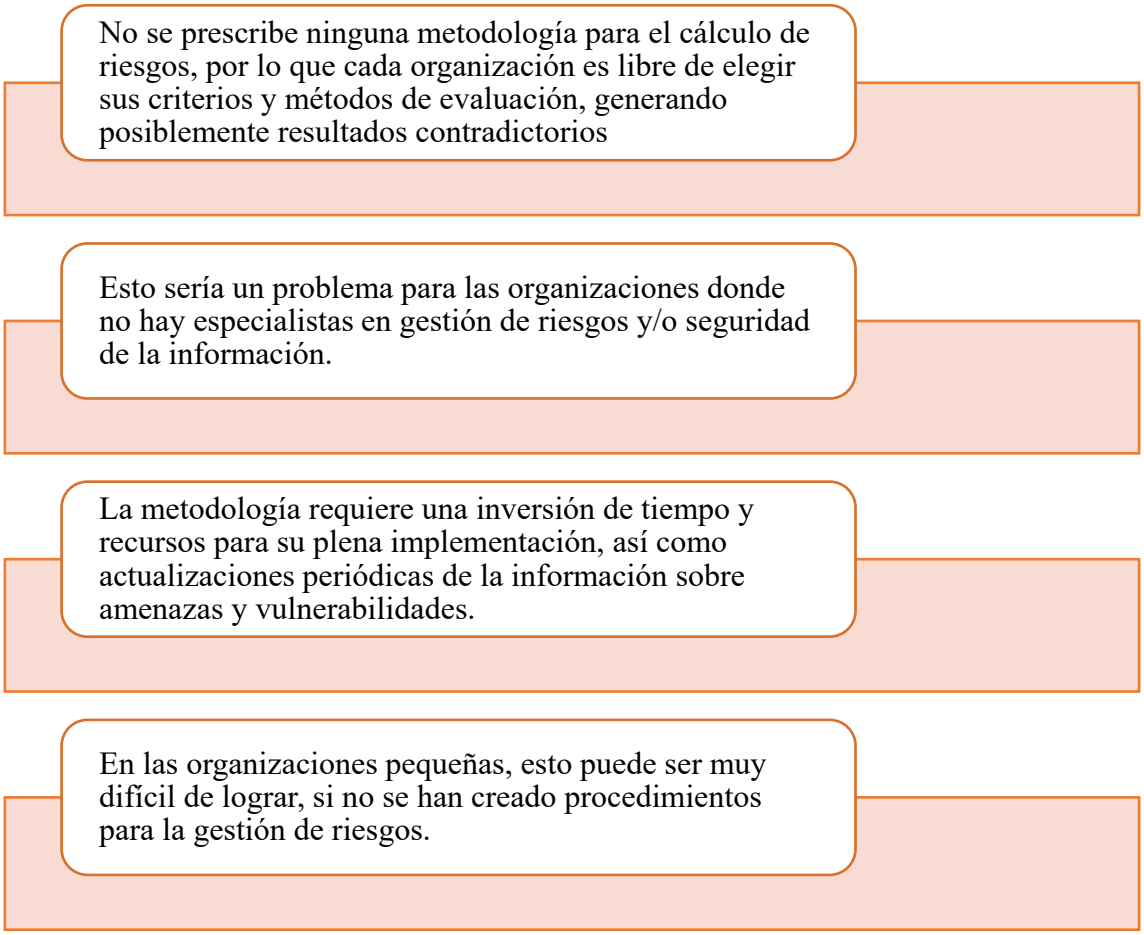


Nota. Fuente: Elaboración Propia.

Incluso con las ventajas que aporta esta metodología, describe ciertas limitaciones:

Figura 6

Desventajas de la ISO/IEC 27005.



Nota. Fuente: Elaboración Propia.

2.7.2. MAGERIT

El objetivo de la metodología Magerit es reconocer, evaluar y controlar de forma coherente estas posibles amenazas a los datos relativas a la seguridad de la información a las que una organización puede enfrentarse. La metodología MAGERIT está estructurada: comienza definiendo un inventario de activos y de sistemas de información. Con base en este registro, se realiza una evaluación y análisis de riesgos que permite identificar las amenazas y vulnerabilidades que, en caso de incidentes o desastres que afecten a la información, afectan a la organización. Posteriormente, se clasifica el riesgo por su severidad. Esto permite definir y poner en marcha planes de mitigación, así como

procesos de seguimiento y control necesarios para la gestión eficaz de estos riesgos (Morillo, 2024).

a. Características

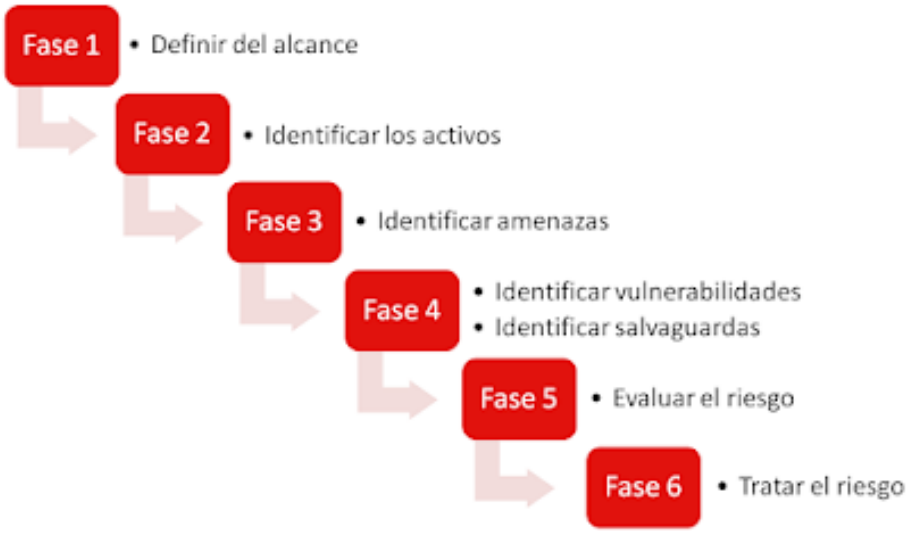
Las principales características de MAGERIT son las siguientes según (Rodríguez, 2025):

- La metodología comienza identificando y evaluando cuáles de los activos de información son valiosos para la organización.
- Examina los eventos que pueden tener impactos en los activos y en las vulnerabilidades (debilidades) que pueden explotarse afectando la seguridad.
- Define las consecuencias que produciría la materialización aceptable de una amenaza para la organización, permitiéndonos calcular su nivel de riesgo.
- La metodología permite identificar el riesgo residual que permanece en el sistema, después de que se hayan implementado las salvaguardas.
- Puede combinarse con normas como ISO/IEC 27001 e ISO/IEC 27002 para mejorar aún más la seguridad de la gestión de la información.

b. Fases de la metodología

Figura 7

Fases de la metodología.

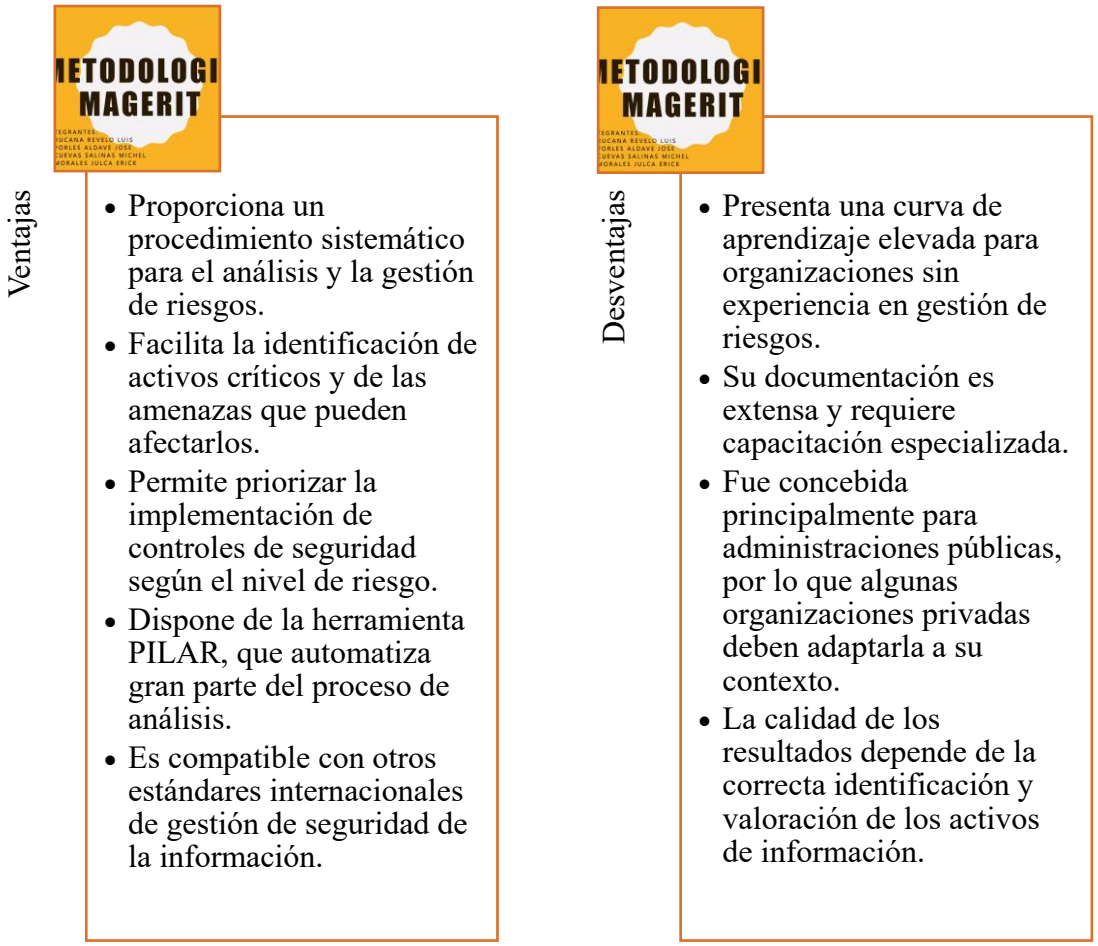


Nota. Fuente: (Sánchez, 2026)

c. Ventajas y desventajas

Figura 8

Ventajas y Desventajas de la metodología MAGERIT.



Nota. Fuente: Elaboración propia.

2.7.3. NIST Cybersecurity Framework

Marco de Ciberseguridad del NIST (CSF) El CSF del NIST es un conjunto de directrices, estándares y buenas prácticas que el Instituto Nacional de Estándares y Tecnología desarrolló para ayudar a las organizaciones a gestionar mejor y reducir el riesgo de ciberseguridad. La ISO 27001 es lo suficientemente flexible como para

adaptarse y desplegarse en organizaciones de cualquier tamaño o sector para proteger la información, mejorar la postura de seguridad y reforzar la gestión del riesgo (IBM, 2026).

a. Características

- Un marco de gestión del riesgo que te permite identificar, analizar y mitigar las amenazas cibernéticas.
- Ahora, flexibilidad y adaptabilidad para cualquier organización: grande o pequeña, privada o pública, joven o madura.
- De acuerdo con la normalización internacional y las mejores prácticas.
- Fomenta la mejora continua de los procesos y controles actuales de ciberseguridad.
- Permite proteger los activos de información con las funciones de Identificar, Proteger, Detectar, Responder y Recuperar.
- Compatible con otros marcos de gestión de seguridad de la información como ISO/IEC 27001, COBIT, CIS Controls, etc
- Proporciona una estructura para la gestión de la seguridad de la información y la resiliencia frente a incidentes cibernéticos de una manera más organizada (NIST, 2024).

b. Fases de la metodología

Figura 9

Fases de la metodología NIST.



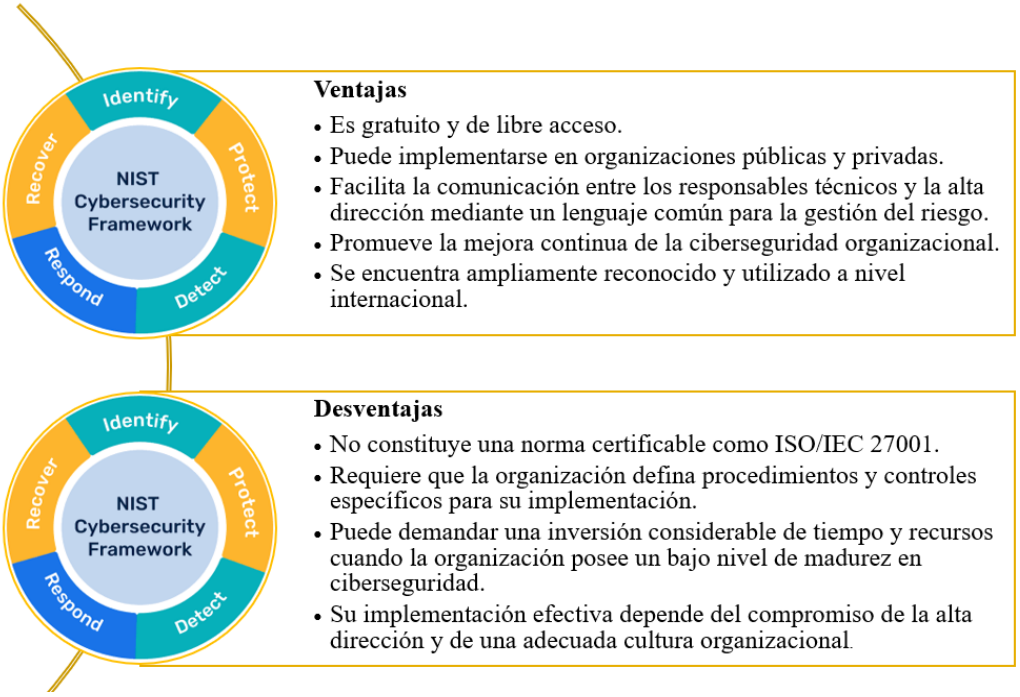
Nota. Fuente: (NIST, 2024)

c. Ventajas y desventajas

El Marco de Ciberseguridad del NIST ofrece una guía estructurada para ayudar a las organizaciones a gestionar el riesgo de ciberseguridad. Sin embargo, como cualquier otra metodología, existen limitaciones y desafíos al momento de adoptarlo, por lo que debe considerarse con cautela. A continuación, Díaz (2023) da a conocer sus principales pros y contras.

Figura 10

Ventajas y desventajas de NIST.



Nota. Fuente: Elaboración en base a (Díaz, 2023)

2.8. Contextualización del GADICC

El Gobierno Autónomo Descentralizado Intercultural del Cantón Cañar (GADICC) es la institución pública encargada de la atención a las personas adultas mayores, los servicios ciudadanos y proyectos específicos para el cantón Cañar, en la provincia del mismo nombre. Con base en las competencias establecidas en la Constitución de la República del Ecuador y en el Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD), sus funciones principales son planificar el desarrollo territorial; brindar servicios públicos, planificación urbana y gestión ambiental; y promover el desarrollo económico, social y cultural a nivel cantonal. La gestión de su territorio es participativa, intercultural, con inclusión ciudadana y una gobernanza llena de procesos de planificación para la toma de decisiones (GADICC CAÑAR, 2026).

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1. Enfoque de la investigación

La investigación adopta un enfoque mixto, de predominancia cualitativa con soporte cuantitativo. El componente cualitativo se expresa en la interpretación del estado de la gestión de la seguridad de la información del departamento de TI, en el análisis documental de la normativa institucional y nacional aplicable y en la valoración técnica de los activos de información identificados. El componente cuantitativo se materializa en la medición del nivel de cumplimiento por dominio de control, obtenida a partir de la encuesta diagnóstica aplicada, y en la valoración numérica de los activos según las cinco dimensiones de seguridad establecidas por MAGERIT.

Esta combinación resulta pertinente porque el objeto de estudio requiere, por una parte, cuantificar de manera objetiva las brechas existentes frente a los requisitos normativos y, por otra, comprender el contexto organizacional, técnico y operativo en el que dichas brechas se producen, condición indispensable para que las políticas propuestas resulten aplicables en la realidad institucional del GADICC.

3.2. Nivel de la investigación

El estudio corresponde a un nivel descriptivo-propositivo. Es descriptivo porque caracteriza sistemáticamente el estado actual de la gestión de la seguridad de la información del departamento de TI del GADICC, identificando sus prácticas vigentes, sus activos de información y las brechas existentes respecto de los controles establecidos en la norma ISO/IEC 27002:2022. Es propositivo porque, a partir de dicha caracterización, formula un instrumento normativo (el manual de políticas de seguridad de la información) orientado a subsanar las deficiencias detectadas y a alinear la gestión

institucional con los requisitos de la norma ISO/IEC 27001:2022 y con el Esquema Gubernamental de Seguridad de la Información (EGSI).

3.3. Diseño de la investigación

El diseño es no experimental y de corte transversal, dado que no se manipulan deliberadamente variables y la información se recolecta en un único momento temporal, correspondiente al segundo semestre del año 2026. La investigación se desarrolla, además, bajo la modalidad de proyecto factible aplicado a un caso de estudio institucional único: el departamento de Tecnologías de la Información del GADICC. El alcance se circunscribe al diseño del manual; no comprende su implementación operativa, la adquisición de herramientas tecnológicas, la ejecución de pruebas técnicas de seguridad ni procesos de auditoría de certificación.

3.4. Población y muestra

La población de estudio está constituida por el personal técnico y administrativo del departamento de Tecnologías de la Información del GADICC, así como por la máxima autoridad administrativa institucional, en tanto responsable de la aprobación y el respaldo de las políticas de seguridad de la información.

La muestra se dirige principalmente al responsable del departamento de TI del GADICC quien concentra las funciones de administración de sistemas, seguridad de la información y comunicaciones y a la máxima autoridad administrativa institucional, con el propósito de conocer, desde la perspectiva técnica y desde la perspectiva directiva, las necesidades y el estado actual de la seguridad de la información de la institución.

3.5. Técnicas e instrumentos de recolección de datos

Para recolectar la información necesaria se utilizará una encuesta estructurada, aplicada al responsable del departamento de TI y a la máxima autoridad administrativa del GADICC. El instrumento consta de sesenta y tres (63) preguntas cerradas,

organizadas en diez dominios de control derivados de la norma ISO/IEC 27002:2022, con opciones de respuesta Sí, No y En proceso. Este proceso tiene como objetivo obtener una visión integral de las prácticas actuales de seguridad de la información en el GADICC, identificar las brechas y los avances en curso frente a los controles de la norma, y fundamentar el desarrollo del manual de políticas de seguridad de la información.

3.6. Interpretación de resultados

En este apartado se presentan e interpretan los resultados obtenidos mediante la encuesta aplicada al responsable del departamento de TI y a la máxima autoridad administrativa del GADICC. El análisis se organiza en tres niveles complementarios: primero, el detalle ítem por ítem de las respuestas obtenidas en cada uno de los diez dominios de control de la norma ISO/IEC 27002:2022. Esta interpretación no busca únicamente cuantificar el cumplimiento normativo, sino identificar de manera diferenciada qué controles están consolidados, cuáles se encuentran en proceso de implementación y cuáles constituyen brechas que el manual de políticas propuesto en el Capítulo IV deberá subsanar.

Para evaluar la seguridad de la información en el GADICC, se aplicó una encuesta al responsable del departamento de TI y a la máxima autoridad administrativa institucional parcialmente implementados o en curso de formalización, lo cual permite conocer en el estado actual de la seguridad en el Gadicc.

Tabla 2

Matriz de respuestas obtenidas con la norma ISO/IEC 27001:2022

N.º	Pregunta	Sí	No	En proceso
	Dominio Políticas de la seguridad de la información (5 ítems)			
1	¿Existe un documento aprobado que contenga las políticas de seguridad de la información?	X		
2	¿El documento de políticas ha sido comunicado al personal técnico del departamento de TI?	X		
3	¿Las políticas de seguridad son coherentes con los objetivos y necesidades institucionales del GADICC?	X		
4	¿La política de seguridad de la información ha sido aprobada formalmente por la máxima autoridad institucional?			X
5	¿El documento de políticas de seguridad de la información se revisa periódicamente o ante la ocurrencia de eventos significativos?		X	
	2. Dominio Aspectos organizativos de la seguridad de la información (6 ítems)			

N.º	Pregunta	Sí	No	En proceso
6	¿Se han asignado responsabilidades específicas relacionadas con la seguridad de la información dentro del departamento de TI?	X		
7	¿La alta dirección del GADICC respalda las iniciativas de seguridad de la información?	X		
8	¿Existen mecanismos de contacto con autoridades competentes en materia de seguridad de la información?	X		
9	¿Existe un comité de gestión de seguridad de la información que impulse y dé seguimiento a las iniciativas de seguridad?		X	
10	¿Se realizan auditorías independientes que evalúen la gestión de la seguridad de la información?		X	
11	¿Se establecen contratos o cláusulas formales de seguridad con terceros y proveedores de TI?		X	
3. Dominio Seguridad ligada a los recursos humanos (5 ítems)				
12	¿Se realiza verificación de antecedentes al personal antes de su contratación?	X		
13	¿Se incluyen cláusulas de confidencialidad y seguridad de la información en los contratos del personal?	X		
14	¿Se aplican procedimientos disciplinarios ante incumplimientos de seguridad de la información?	X		

N.º	Pregunta	Sí	No	En proceso
15	¿Se retiran oportunamente los accesos del personal que finaliza su relación laboral?	X		
16	¿El personal conoce los procedimientos establecidos para reportar incidentes y debilidades de seguridad?		X	
4. Dominio Gestión de activos (5 ítems)				
17	¿Se mantiene un inventario actualizado de los activos de información?	X		
18	¿Cada activo de información cuenta con un responsable o propietario designado?	X		
19	¿Existen normas sobre el uso aceptable de los activos de información?	X		
20	¿Existen directrices institucionales para la clasificación de la información según su nivel de criticidad?		X	
21	¿Están definidos los procedimientos de etiquetado y manejo de los activos de información?		X	
5. Dominio Control de accesos (10 ítems)				
22	¿Existe una política formal de control de accesos?	X		
23	¿Se gestiona el acceso de usuarios mediante un proceso formal de altas, modificaciones y bajas?	X		
24	¿Se revisan periódicamente los derechos de acceso otorgados a los usuarios?	X		

N.º	Pregunta	Sí	No	En proceso
25	¿Se restringe y controla el acceso a la información y a las aplicaciones institucionales?	X		
26	¿Se utilizan mecanismos de autenticación para el acceso a los sistemas de información?	X		
27	¿Se gestionan de manera segura las contraseñas del personal técnico?	X		
28	¿Se controlan y monitorizan los accesos privilegiados de administración?	X		
29	¿Se restringe el acceso al código fuente de las aplicaciones desarrolladas internamente?	X		
30	¿Se controla el acceso remoto mediante mecanismos seguros como VPN?	X		
31	¿Existe una política formal para el uso de controles criptográficos en la protección de la información?		X	
6. Dominio Seguridad física y ambiental (8 ítems)				
32	¿Se cuenta con un cuarto de servidores de acceso restringido?	X		
33	¿Se dispone de sistemas de control ambiental (climatización) en el cuarto de servidores?	X		
34	¿Se protegen los racks de comunicaciones frente a accesos no autorizados?	X		
35	¿Se dispone de sistemas de protección física ante desastres, ataques o accidentes que puedan afectar la infraestructura tecnológica?		X	

N.º	Pregunta	Sí	No	En proceso
36	¿Se controlan y restringen los puntos de acceso físico a las instalaciones institucionales?		X	
37	¿El equipamiento de TI se encuentra adecuadamente protegido frente a amenazas ambientales?		X	
38	¿Existen procedimientos para la corrección oportuna de fallas o daños en el cableado de datos?		X	
39	¿Se dispone de áreas o sitios seguros designados para el desarrollo de actividades que requieren protección especial?		X	
7. Dominio Seguridad en la operativa (9 ítems)				
40	¿Existen procedimientos documentados para la operación de los sistemas de información?	X		
41	¿Se realizan copias de respaldo periódicas de la información institucional?	X		
42	¿Se prueba periódicamente la restauración de las copias de respaldo?	X		
43	¿Se cuenta con protección contra software malicioso en los equipos y servidores?	X		
44	¿Se gestionan y protegen adecuadamente los registros (logs) de actividad del sistema?	X		
45	¿Existen procedimientos formales de gestión de cambios en la infraestructura tecnológica?	X		

N.º	Pregunta	Sí	No	En proceso
46	¿Se separan los entornos de desarrollo, pruebas y producción del Sistema Integrado Municipal?	X		
47	¿Se gestionan de manera oportuna las vulnerabilidades técnicas identificadas?	X		
48	¿Se restringe la instalación de software no autorizado en los equipos institucionales?			X
8. Dominio Seguridad en las telecomunicaciones (5 ítems)				
49	¿La red institucional se encuentra segmentada para limitar el acceso a recursos críticos?	X		
50	¿Se protege la información transmitida a través de las redes institucionales?	X		
51	¿Se dispone de un cortafuegos perimetral que controle y filtre el tráfico de red?	X		
52	¿Se supervisan las comunicaciones de red para detectar actividades sospechosas?	X		
53	¿Se actualizan y gestionan adecuadamente los dispositivos de red?			X
9. Dominio Gestión de incidentes de seguridad de la información (5 ítems)				
54	¿Existen procedimientos documentados para la gestión de incidentes de seguridad de la información?	X		
55	¿Se registran los incidentes de seguridad ocurridos en la institución?	X		
56	¿Se toman medidas correctivas para evitar la recurrencia de incidentes de seguridad?	X		

N.º	Pregunta	Sí	No	En proceso
57	¿Se informa a la alta dirección sobre los incidentes de seguridad significativos?			X
58	¿Se realiza la valoración de los eventos de seguridad para determinar su clasificación como incidentes?		X	
10. Dominio Cumplimiento (5 ítems)				
59	¿La institución cumple con la normativa nacional aplicable en materia de protección de datos personales?	X		
60	¿Se identifican los requisitos legales y regulatorios aplicables a la seguridad de la información?	X		
61	¿Se revisa el cumplimiento técnico de los sistemas frente a las políticas de seguridad establecidas?	X		
62	¿Se llevan a cabo auditorías externas de seguridad de la información?	X		
63	¿Se actualizan las políticas de seguridad para reflejar cambios en las regulaciones y estándares?			X

Nota. Elaboración propia (2026), a partir de los resultados de la encuesta aplicada al responsable de TI y a la máxima autoridad administrativa del GADICC.

Tras la aplicación de la encuesta al responsable del departamento de TI y a la máxima autoridad administrativa del GADICC, se llevó a cabo el análisis respectivo de los resultados obtenidos, tomando como referencia los controles de la norma ISO/IEC 27002:2022, según se muestra en las tablas anteriores.

3.7. Análisis de la norma ISO 27001:2022

3.7.1. Dominio Políticas de la seguridad de la información

Figura 11

Dominio Políticas de la seguridad de la información.



Nota. Autoría propia.

Con base en los resultados obtenidos en el dominio de Políticas de la Seguridad, como se observa en el Gráfico N.º 1, se evidencia que el 60,0 % de las políticas de seguridad de la información del departamento de TI del GADICC están documentadas e implementadas. Un 20,0 % adicional se encuentra en proceso, correspondiente a la aprobación formal del documento por parte de la máxima autoridad institucional, mientras que el 20,0 % restante corresponde a la ausencia de un proceso de revisión periódica del documento de políticas, brecha vinculada al control 5.1 Políticas de seguridad de la información del Anexo A de la norma ISO/IEC 27002:2022. Este

resultado subraya la importancia de formalizar tanto la aprobación como el ciclo de revisión del documento de políticas.

3.7.2. Dominio Aspectos organizativos de la seguridad de la información

Figura 12

Dominio Aspectos organizativos de la seguridad de la información.



Nota. Autoría propia.

Como se observa en el Gráfico N.º 2, en el dominio de Aspectos organizativos de la Seguridad de la Información el 50,0 % de las prácticas evaluadas se encuentran implementadas, mientras que el otro 50,0 % no lo está. El departamento no dispone de un comité de gestión de seguridad de la información, no somete sus prácticas a auditorías independientes y no ha formalizado contratos ni cláusulas de seguridad con terceros y proveedores de TI, brechas vinculadas a los controles 5.2, 5.35 y 5.19 a 5.22 del Anexo A. Este resultado evidencia una de las debilidades estructurales más relevantes del diagnóstico y resalta la necesidad de fortalecer la gobernanza de la seguridad de la información dentro de la institución.

3.7.3. Dominio Seguridad ligada a los recursos humanos

Figura 13

Dominio Seguridad ligada a los recursos humanos.



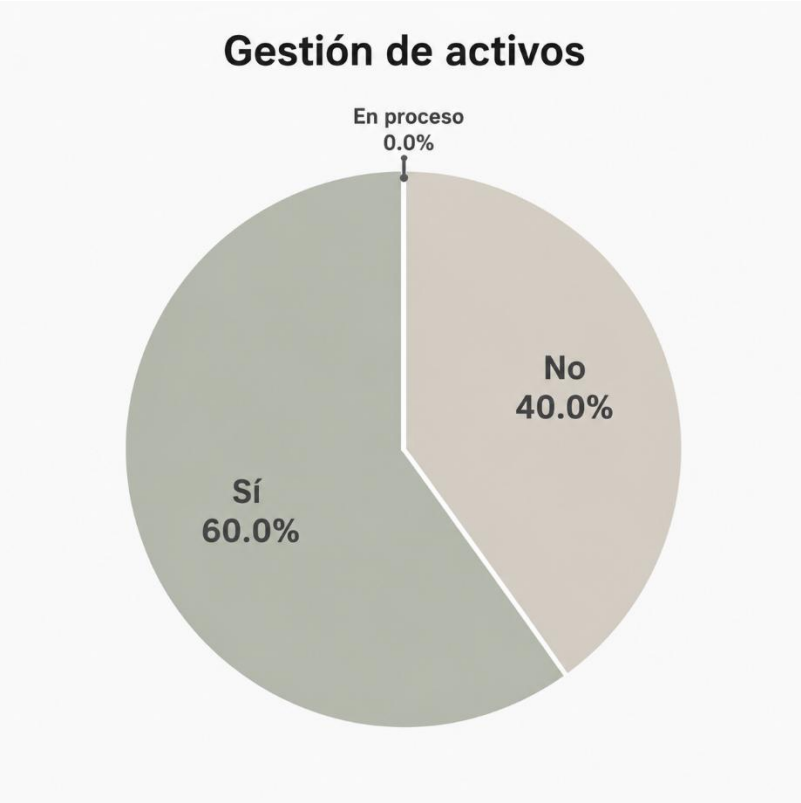
Nota. Autoría propia.

De acuerdo con el Gráfico N.º 3, en el dominio de Seguridad Ligada a los Recursos Humanos el 80,0 % de las prácticas están adecuadamente implementadas, entre ellas la verificación de antecedentes, las cláusulas de confidencialidad y el retiro oportuno de accesos al personal saliente. El 20,0 % restante corresponde al desconocimiento, por parte del personal técnico, de los procedimientos para reportar incidentes y debilidades de seguridad, brecha vinculada al control 6.8 Reporte de eventos de seguridad. Este resultado pone de manifiesto que la formalización de procedimientos no ha sido acompañada de una difusión suficiente hacia el personal.

3.7.4. Dominio Gestión de activos

Figura 14

Dominio Gestión de activos.



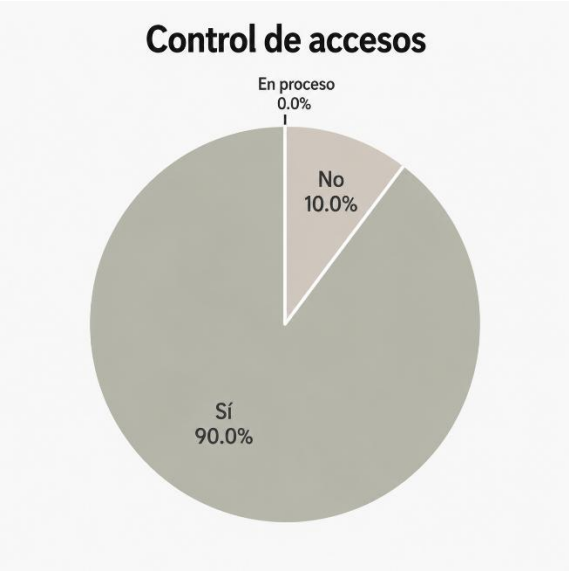
Nota. Autoría propia.

Según el Gráfico N.º 4, en el dominio de Gestión de Activos el 60,0 % de las actividades y controles relacionados están implementados, mientras que el 40,0 % restante se encuentra ausente. El departamento mantiene un inventario actualizado de sus activos, con responsables designados; sin embargo, no existen directrices para la clasificación de la información según su nivel de criticidad ni procedimientos definidos de etiquetado y manejo, brechas asociadas a los controles 5.12 y 5.13 del Anexo A.

3.7.5. Dominio Control de accesos

Figura 15

Dominio Control de accesos.



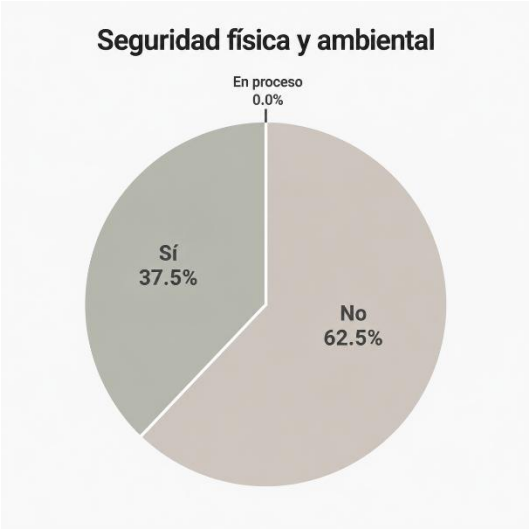
Nota. Autoría propia.

En el Gráfico N.º 5 se observa que el dominio de Control de Accesos alcanzó el segundo nivel de cumplimiento más alto del diagnóstico, con un 90,0 % de las medidas y procedimientos implementados satisfactoriamente. El departamento gestiona formalmente el ciclo de vida de los accesos de usuario, revisa periódicamente los derechos otorgados y protege el acceso remoto mediante VPN. El 10,0 % restante corresponde a la ausencia de una política formal para el uso de controles criptográficos, vinculada al control 8.24 Uso de criptografía del Anexo A. Este resultado enfatiza la importancia de completar este último control para asegurar la protección adecuada de la información crítica.

3.7.6. Dominio Seguridad física y ambiental

Figura 16

Dominio Seguridad física y ambiental.



Nota. Autoría propia.

El Gráfico N.º 6 muestra que el dominio de Seguridad Física y Ambiental constituye el hallazgo más crítico del diagnóstico: solo el 37,5 % de las medidas evaluadas están implementadas de manera adecuada, mientras que el 62,5 % restante se encuentra ausente. El departamento no dispone de sistemas de protección física ante desastres, ataques o accidentes, no controla adecuadamente los puntos de acceso a las instalaciones, el equipamiento no está protegido frente a amenazas ambientales, no existen procedimientos de corrección oportuna de fallas en el cableado de datos y no se dispone de áreas o sitios seguros para el desarrollo de actividades, brechas vinculadas a los controles 7.5, 7.2, 7.8, 7.12 y 7.3 del Anexo A. Este resultado subraya la importancia de completar y consolidar todas las acciones relacionadas con la seguridad física y ambiental para garantizar la protección integral de los recursos físicos y tecnológicos de la institución.

3.7.7. Dominio Seguridad en la operativa

Figura 17

Dominio Seguridad en la operativa.



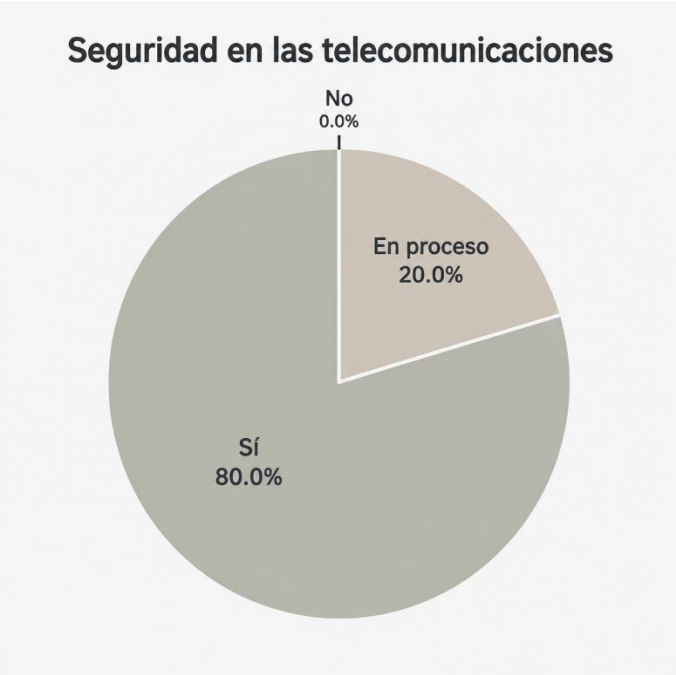
Nota. Autoría propia.

De acuerdo con los resultados obtenidos en el dominio de Seguridad en la Operativa, presentados en el Gráfico N.º 7, se observa que el 88,9 % de las medidas y procedimientos operativos de seguridad están implementados de manera adecuada: procedimientos documentados de operación, copias de respaldo periódicas y verificadas, protección contra software malicioso, gestión de registros de actividad, control de cambios y separación de entornos. El 11,1 % restante corresponde a la restricción de instalación de software no autorizado, control que se encuentra actualmente en proceso de implementación. Este resultado evidencia que las prácticas técnico-operativas del departamento de TI del GADICC se encuentran en gran medida consolidadas, aunque con algunos aspectos aún por completar.

3.7.8. Dominio Seguridad en las telecomunicaciones

Figura 18

Dominio Seguridad en las telecomunicaciones.



Nota. Autoría propia.

Según el Gráfico N.º 8, el dominio de Seguridad en las Telecomunicaciones alcanzó un cumplimiento del 80,0 %. La segmentación de la red institucional en ocho VLAN, la protección de la información transmitida, la existencia de un cortafuegos perimetral y la supervisión de las comunicaciones constituyen controles ya implementados; el 20,0 % restante corresponde a la actualización y gestión de los dispositivos de red, proceso que se encuentra actualmente en curso. Este resultado indica un nivel aceptable de madurez en la protección de las telecomunicaciones institucionales.

3.7.9. Dominio Gestión de incidentes de seguridad de la información

Figura 19

Dominio Gestión de incidentes de seguridad de la información.



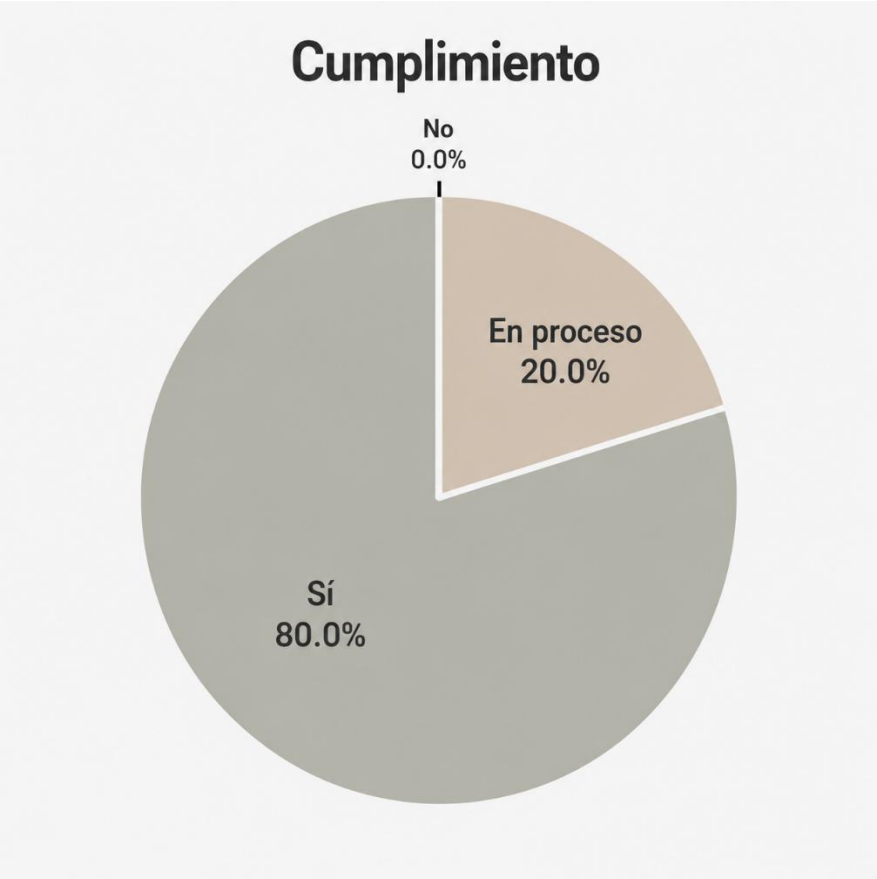
Nota. Autoría propia.

Como se muestra en el Gráfico N.º 9, el dominio de Gestión de Incidentes de Seguridad de la Información presenta un cumplimiento del 60,0 %. El departamento cuenta con procedimientos documentados, registra los incidentes ocurridos y toma medidas correctivas para evitar su recurrencia; sin embargo, el reporte de incidentes significativos a la alta dirección se encuentra en proceso de formalización (20,0 %), y no se efectúa la valoración de los eventos de seguridad para determinar su clasificación como incidentes (20,0 %), brecha vinculada al control 5.25 Evaluación y decisión sobre eventos de seguridad. Es esencial culminar estos procesos para fortalecer la gestión de incidentes en la institución.

3.7.10. Dominio Cumplimiento

Figura 20

Dominio Cumplimiento.



Nota. Autoría propia.

En el Gráfico N.º 10 se presenta el dominio de Cumplimiento, en el que el 80,0 % de las prácticas y procedimientos evaluados están implementados de manera adecuada: el departamento observa la normativa nacional aplicable, identifica los requisitos legales y regulatorios pertinentes, revisa el cumplimiento técnico de sus sistemas y realiza auditorías externas de seguridad. El 20,0 % restante corresponde a la actualización de las políticas de seguridad para reflejar cambios en las regulaciones y estándares, proceso que se encuentra actualmente en curso.

3.7.11. Análisis general de la encuesta

La encuesta aplicada al departamento de Tecnologías de la Información (TI) del GADICC evidencia la coexistencia de fortalezas técnico-operativas, procesos de mejora en desarrollo y brechas relacionadas con aspectos organizativos y físicos de la seguridad de la información. De los 63 ítems evaluados, 44 obtuvieron una respuesta afirmativa (69,8 %), 5 se encuentran en proceso de implementación (7,9 %) y 14 presentan incumplimientos (22,2 %). En términos generales, el nivel de cumplimiento alcanzado es del 69,8 %, valor que, de acuerdo con la escala establecida en el presente estudio, corresponde a un nivel insuficiente, debido a la existencia de controles que requieren fortalecimiento y formalización institucional.

Los dominios asociados a la gestión técnica y operativa presentan los mejores resultados, destacándose el control de accesos con un cumplimiento del 90,0 %, considerado satisfactorio, seguido de seguridad en la operativa, seguridad en las telecomunicaciones y cumplimiento, con porcentajes que oscilan entre el 80,0 % y 88,9 %. Estos resultados reflejan que el personal del área de TI posee capacidades técnicas consolidadas y que una parte significativa de los controles tecnológicos se encuentra implementada. No obstante, los dominios relacionados con la gestión organizativa y física presentan mayores oportunidades de mejora; específicamente, los aspectos organizativos (50,0 %), la gestión de activos (60,0 %) y la gestión de incidentes de seguridad de la información (60,0 %) evidencian niveles deficientes, mientras que la seguridad física y ambiental, con un 37,5 %, alcanza una condición crítica. De las 14 brechas identificadas, el 71,4 % se concentra en estos tres dominios prioritarios, por lo que representan los principales ejes de intervención para el desarrollo del manual de políticas de seguridad de la información propuesto.

En este contexto, los resultados obtenidos permiten determinar que las principales limitaciones del departamento de TI del GADICC no se relacionan con la capacidad técnica del personal, sino con la ausencia de mecanismos formales de gobernanza y gestión integral de la seguridad, tales como un comité especializado, auditorías independientes, procedimientos documentados y controles asociados a proveedores, infraestructura física y condiciones ambientales. Asimismo, la existencia de controles en proceso dentro de los diferentes dominios evaluados evidencia que la institución se encuentra en una etapa de transición hacia mayores niveles de madurez en seguridad de la información, lo que representa una oportunidad para fortalecer sus capacidades mediante la implementación de políticas, procedimientos y mecanismos de mejora continua.

3.8. Selección de la metodología

Luego del análisis de las metodologías de gestión y análisis de riesgos ISO/IEC 27005, MAGERIT v3 y NIST Cybersecurity Framework, se seleccionó MAGERIT como metodología para el análisis de riesgos del departamento de Tecnologías de la Información del GADICC. Esta elección se fundamenta en su enfoque estructurado, que permite identificar y valorar los activos de información, determinar las amenazas y vulnerabilidades asociadas, y estimar el nivel de riesgo mediante evaluaciones cualitativas y cuantitativas considerando dimensiones de seguridad como disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. Además, su capacidad para determinar el riesgo residual después de la aplicación de salvaguardas facilita la evaluación de la efectividad de los controles implementados y la definición de medidas de tratamiento adecuadas.

La selección de MAGERIT también se justifica por su reconocimiento institucional, disponibilidad de documentación técnica en español, catálogo normalizado de activos y compatibilidad con estándares internacionales como ISO/IEC 27001:2022, lo que garantiza su alineación con buenas prácticas de seguridad de la información. Su aplicación en el departamento de TI del GADICC permitirá identificar, clasificar y valorar los activos críticos, así como establecer los riesgos asociados, cuyos resultados servirán como base para la definición de políticas de seguridad y la elaboración del manual propuesto en el Capítulo IV, en cumplimiento de los objetivos específicos tercero y cuarto de la presente investigación.

CAPÍTULO IV

4. PROPUESTA

4.1. Introducción

En este capítulo se desarrolla la propuesta de la presente investigación: un manual de políticas de seguridad de la información para el departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado Intercultural del Cantón Cañar (GADICC), fundamentado en la norma ISO/IEC 27001:2022 y en los controles del Anexo A de la norma ISO/IEC 27002:2022. La propuesta parte del diagnóstico institucional presentado en el Capítulo III, en el que se identificó un nivel de cumplimiento general del 69,8 %, así como brechas prioritarias en los dominios de seguridad física y ambiental, aspectos organizativos y gestión de activos. A partir de estos hallazgos, se aplica la metodología MAGERIT v3 para determinar el riesgo asociado a los activos de

información críticos del departamento y, con base en dicho análisis, se establecen las directrices que estructurarán el manual de políticas.

4.2. Determinación del riesgo con MAGERIT

La metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), versión 3, es un enfoque sistemático para identificar, analizar y valorar los riesgos asociados a los activos de información de una organización, compatible con la norma ISO/IEC 27005 y con los estándares ISO/IEC 27001 e ISO/IEC 27002 (Amutio Gómez, Candau, & Mañas, 2012). Tal como se justificó en el Capítulo III, esta metodología fue seleccionada para el análisis de riesgos del departamento de TI del GADICC por su enfoque estructurado, su catálogo normalizado de activos y amenazas, y su compatibilidad con la norma ISO/IEC 27001:2022.

El desarrollo del análisis de riesgos comprende las siguientes fases: 1) identificación de los activos de información; 2) valoración de los activos según las cinco dimensiones de seguridad; 3) identificación de las amenazas asociadas a los activos de mayor valor; 4) evaluación del impacto y la probabilidad de ocurrencia; 5) cálculo del nivel de riesgo; y 6) determinación de los controles de seguridad aplicables. A continuación, se desarrolla cada una de estas fases con base en el levantamiento realizado en el departamento de TI del GADICC.

4.2.1. Identificación de Activos de Información

Se identificaron 50 activos de información en la infraestructura tecnológica del departamento de TI del GADICC, clasificados según el catálogo de tipos de activos de MAGERIT v3 (Libro II): datos e información, servicios, software, equipamiento (hardware), redes de comunicaciones, soportes de información, equipamiento auxiliar, instalaciones y personal. Para cada activo se registró el responsable y la ubicación dentro de la institución, como se detalla en la Tabla 15.

Tabla 3

Inventario de activos de información del departamento de TI del GADICC

Código	Tipo	Activo	Responsable	Ubicación
[D] Datos / Información				
ACT-D-01	files/int	Base de datos institucional del municipio	DBA (D. Andrade / A. Serrano / W. Lema)	Servidor de BD (VM)
ACT-D-02	backup	Copias de respaldo (BD y archivos)	TIC's	Data center municipal
ACT-D-03	conf	Datos de configuración de red	Adm. de comunicaciones (D. Andrade)	Switches / Firewall
ACT-D-04	password/auth	Credenciales y datos de autenticación	Adm. de seguridad (D. Andrade)	Servidor de BD
ACT-D-05	acl	Datos de control de acceso	Adm. de seguridad (D. Andrade)	Servidor de BD
ACT-D-06	log	Registros de actividad (logs)	TIC's	Servidores
ACT-D-07	source	Código fuente del SIM	Desarrolladores (Serrano / Guasco / Andrade)	Repositorio interno
[S] Servicios				
ACT-S-01	pub	Portal web SIM (público)	TIC's	Servicio web (Internet)
ACT-S-02	int	Sistema Integrado Municipal (SIM) y módulos internos	TIC's	Servidores institucionales
ACT-S-03	www	Servicios web publicados	TIC's	Servicio web (Internet)
ACT-S-04	telnet	Acceso remoto VPN	Adm. de comunicaciones (D. Andrade)	Firewall / red
ACT-S-05	email	Correo electrónico institucional	TIC's	Servidor de correo (CentOS 6)
ACT-S-06	edi	Servicios externos de pago / intercambio	TIC's / Financiero	Servicios externos
ACT-S-07	pki	Certificados digitales (PKI)	Adm. de seguridad (D. Andrade)	Servidores web
[SW] Software				
ACT-SW-01	prp	SIM, Sistema Integrado Municipal (in house)	Desarrolladores (Serrano / Guasco / Andrade)	Servidor de aplicaciones
ACT-SW-02	std.dbms	Gestores de base de datos (Oracle 11gR2 / MySQL 8)	DBA	Servidores de BD

Código	Tipo	Activo	Responsable	Ubicación
ACT-SW-03	std.app	Servidor de aplicaciones Glassfish	TIC's	VM avalúos/catastros
ACT-SW-04	std.www	Servidor web IIS	TIC's	VM de aplicaciones
ACT-SW-05	std.email_server	Servidor de correo Zimbra	TIC's	Servidor CentOS 6
ACT-SW-06	std.hypervisor	Virtualización VMware	TIC's	Servidores físicos
ACT-SW-07	std.os	Sistemas operativos	TIC's	Servidores y equipos
ACT-SW-08	std.av	Antivirus Kaspersky	Adm. de seguridad (D. Andrade)	Equipos y servidor AV
ACT-SW-09	std.office	Ofimática (LibreOffice)	TIC's	Equipos de usuario
ACT-SW-10	std.backup	Software de respaldo (Oracle 11gR2)	DBA	Servidor de BD
		[HW] Equipamiento (hardware)		
ACT-HW-01	host	Servidores físicos	TIC's	Data center municipal
ACT-HW-02	vhost	Máquinas virtuales (VMware)	TIC's	Servidores físicos
ACT-HW-03	pc	Equipo potenciado (servidor de antivirus)	TIC's	Data center
ACT-HW-04	network.switch	Switches Cisco (capa 3)	Adm. de comunicaciones (D. Andrade)	Racks de comunicaciones
ACT-HW-05	network.router	Routers de acceso y distribución	Adm. de comunicaciones (D. Andrade)	Racks de comunicaciones
ACT-HW-06	network.firewall	Firewall Sophos	Adm. de seguridad (D. Andrade)	Perímetro de red
ACT-HW-07	peripheral.print	Impresoras	TIC's / Administrativo	Departamentos
ACT-HW-08	peripheral.scan	Escáneres	TIC's / Administrativo	Departamentos
ACT-HW-09	pabx/ipphone	Telefonía IP (Elastix)	TIC's	Data center / oficinas
		[COM] Redes de comunicaciones		
ACT-COM-01	LAN	Red local (LAN) institucional	Adm. de comunicaciones (D. Andrade)	Sede municipal

Código	Tipo	Activo	Responsable	Ubicación
ACT-COM-02	Internet	Acceso a Internet	TIC's	Sede municipal
[Media] Soportes de información				
ACT-MEDIA-01	electronic.disk	Discos (HDD / SSD)	TIC's	Servidores / equipos
ACT-MEDIA-02	electronic.vdisk	Discos virtuales	TIC's	Plataforma VMware
ACT-MEDIA-03	electronic.dvd/cd	Medios ópticos (DVD / CD-RW)	TIC's	Data center
[AUX] Equipamiento auxiliar				
ACT-AUX-01	ups/power	UPS / SAI	TIC's / Administrativo	Data center
ACT-AUX-02	gen	Generador eléctrico	Administrativo	Instalaciones
ACT-AUX-03	cabling.fiber	Backbone de fibra óptica	Adm. de comunicaciones (D. Andrade)	Canalizaciones
ACT-AUX-04	cabling.wire	Cableado estructurado	TIC's	Instalaciones
[L] Instalaciones				
ACT-L-01	building/site	Edificio e instalaciones municipales	Administrativo	Sede municipal
ACT-L-02	local	Cuarto de servidores (data center)	TIC's	Sede municipal
ACT-L-03	shelter	Racks de comunicaciones	TIC's	Data center
[P] Personal				
ACT-P-01	adm/sec/com	Administrador de sistemas, seguridad y comunicaciones	Dirección TIC's	Departamento TIC's
ACT-P-02	dba	Administradores de bases de datos	Dirección TIC's	Departamento TIC's
ACT-P-03	des	Desarrolladores / programadores	Dirección TIC's	Departamento TIC's
ACT-P-04	op	Operadores	Dirección TIC's	Departamento TIC's
ACT-P-05	ui	Usuarios internos (funcionarios)	Cada área	Sede municipal

Nota. a escala se aplica a cada una de las cinco dimensiones de valoración de los activos: Disponibilidad (D), Integridad (I), Confidencialidad (C), Autenticidad (A) y Trazabilidad (T). El valor global (VG) de cada activo corresponde al máximo alcanzado entre sus cinco dimensiones. Elaboración propia con base en Amutio Gómez, Candau, & Mañas (2012)

4.2.2. Valoración de los activos

La valoración de los activos se realizó sobre cinco dimensiones de seguridad definidas por MAGERIT: disponibilidad (D), integridad (I), confidencialidad (C), autenticidad (A) y trazabilidad (T), utilizando una escala de 0 a 10 (Tabla 16). El valor global (VG) de cada activo corresponde al valor máximo alcanzado entre sus cinco dimensiones, criterio que MAGERIT recomienda para evitar que una dimensión poco relevante compense el riesgo real de la dimensión más crítica del activo.

Tabla 4

Escala de valoración de activos MAGERIT

Rango	Nivel de riesgo
1-4	Bajo
5-9	Medio
10-15	Alto
16-25	Crítico

Nota. Los rangos establecidos permiten clasificar el nivel de riesgo de los activos en cuatro categorías: bajo, medio, alto y crítico. La asignación de colores se utiliza como apoyo visual para facilitar la identificación de los activos que requieren mayor atención y la priorización de medidas de seguridad. Fuente: (Amutio Gómez et al., 2012)

La Tabla 17 presenta el resultado completo, organizado por tipo de activo. De los cincuenta activos valorados, 25 (50 %) obtuvieron un valor global de 9 o 10 (muy alto o crítico), concentrados principalmente en los datos institucionales, el Sistema Integrado Municipal (SIM), los gestores de base de datos y el firewall perimetral.

Tabla 5

Valoración de los activos de información del departamento de TI del GADICC.

Código	Activo	D	I	C	A	T	VG
[D] Datos / Información							
ACT-D-01	Base de datos institucional del municipio	9	10	9	9	9	10
ACT-D-02	Copias de respaldo (BD y archivos)	9	9	8	7	7	9
ACT-D-03	Datos de configuración de red	8	9	8	8	8	9
ACT-D-04	Credenciales y datos de autenticación	8	9	10	9	8	10
ACT-D-05	Datos de control de acceso	7	9	9	8	8	9
ACT-D-06	Registros de actividad (logs)	6	9	7	8	10	10
ACT-D-07	Código fuente del SIM	6	9	9	8	8	9
[S] Servicios							
ACT-S-01	Portal web SIM (público)	9	9	7	9	9	9
ACT-S-02	Sistema Integrado Municipal (SIM) y módulos internos	9	10	9	9	9	10
ACT-S-03	Servicios web publicados	8	8	6	8	8	8
ACT-S-04	Acceso remoto VPN	7	8	9	9	9	9
ACT-S-05	Correo electrónico institucional	8	8	8	8	8	8
ACT-S-06	Servicios externos de pago / intercambio	8	9	8	9	9	9
ACT-S-07	Certificados digitales (PKI)	7	9	8	10	8	10
[SW] Software							
ACT-SW-01	SIM, Sistema Integrado Municipal (in house)	9	10	9	9	9	10
ACT-SW-02	Gestores de base de datos (Oracle 11gR2 / MySQL 8)	9	10	9	8	8	10
ACT-SW-03	Servidor de aplicaciones Glassfish	8	9	8	8	8	9
ACT-SW-04	Servidor web IIS	8	8	6	7	7	8
ACT-SW-05	Servidor de correo Zimbra	8	8	8	8	8	8
ACT-SW-06	Virtualización VMware	9	9	8	8	7	9

Código	Activo	D	I	C	A	T	VG
ACT-SW-07	Sistemas operativos	8	8	7	7	7	8
ACT-SW-08	Antivirus Kaspersky	7	8	6	7	8	8
ACT-SW-09	Ofimática (LibreOffice)	5	6	6	4	4	6
ACT-SW-10	Software de respaldo (Oracle 11gR2)	8	9	8	7	7	9
[HW] Equipamiento (hardware)							
ACT-HW-01	Servidores físicos	9	9	8	8	7	9
ACT-HW-02	Máquinas virtuales (VMware)	9	9	8	8	7	9
ACT-HW-03	Equipo potenciado (servidor de antivirus)	7	7	6	6	6	7
ACT-HW-04	Switches Cisco (capa 3)	9	8	6	6	6	9
ACT-HW-05	Routers de acceso y distribución	8	7	6	7	6	8
ACT-HW-06	Firewall Sophos	9	9	9	9	9	9
ACT-HW-07	Impresoras	4	4	4	3	3	4
ACT-HW-08	Escáneres	4	4	4	3	3	4
ACT-HW-09	Telefonía IP (Elastix)	6	5	5	5	5	6
[COM] Redes de comunicaciones							
ACT-COM-01	Red local (LAN) institucional	9	8	7	6	6	9
ACT-COM-02	Acceso a Internet	8	6	5	6	6	8
[Media] Soportes de información							
ACT-MEDIA-01	Discos (HDD / SSD)	7	7	7	5	5	7
ACT-MEDIA-02	Discos virtuales	8	7	7	5	5	8

Código	Activo	D	I	C	A	T	VG
ACT-MEDIA-03	Medios ópticos (DVD / CD-RW)	3	4	4	3	3	4
[AUX] Equipamiento auxiliar							
ACT-AUX-01	UPS / SAI	8	3	2	2	2	8
ACT-AUX-02	Generador eléctrico	8	2	2	2	2	8
ACT-AUX-03	Backbone de fibra óptica	8	6	4	4	3	8
ACT-AUX-04	Cableado estructurado	6	3	2	2	2	6
[L] Instalaciones							
ACT-L-01	Edificio e instalaciones municipales	7	4	4	3	4	7
ACT-L-02	Cuarto de servidores (data center)	9	6	7	5	6	9
ACT-L-03	Racks de comunicaciones	7	5	5	4	4	7
[P] Personal							
ACT-P-01	Administrador de sistemas, seguridad y comunicaciones	8	8	9	8	8	9
ACT-P-02	Administradores de bases de datos	8	9	9	8	8	9
ACT-P-03	Desarrolladores / programadores	7	8	8	7	7	8
ACT-P-04	Operadores	7	7	7	6	6	7
ACT-P-05	Usuarios internos (funcionarios)	6	6	7	5	5	7

Nota. D = Disponibilidad; I = Integridad; C = Confidencialidad; A = Autenticidad; T = Trazabilidad; VG = Valor global (máximo de las cinco dimensiones). Escala 0-10. El valor global corresponde a la puntuación máxima obtenida en las cinco dimensiones de seguridad. Los porcentajes se calcularon sobre un total de 50 activos. Fuente: elaboración propia con base en MAGERIT. Fuente: (GADICC CAÑAR, 2026)

4.2.3. Identificación de las Amenazas

A partir del inventario valorado, se priorizaron para el análisis de amenazas los activos con valor global de 9 o 10, por representar el mayor impacto potencial para el

departamento de TI del GADICC en caso de materializarse un riesgo. La Tabla 18 presenta el catálogo de amenazas de MAGERIT aplicable a estos activos.

Tabla 6

Catálogo de amenazas MAGERIT aplicable a los activos prioritarios

Tipo de amenaza	Amenazas aplicables
[N] Desastres naturales	[N.1] Fuego
[I] De origen industrial	[I.6] Corte del suministro eléctrico · [I.7] Condiciones inadecuadas de temperatura o humedad
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios · [E.3] Errores de monitorización (log) · [E.19] Fugas de información · [E.28] Indisponibilidad del personal
[A] Ataques intencionados	[A.5] Suplantación de identidad · [A.6] Abuso de privilegios de acceso · [A.11] Acceso no autorizado · [A.14] Interceptación de información · [A.24] Denegación de servicio

Nota. Se presenta las amenazas MAGERIT aplicables a los activos prioritarios con valor global de 9 o 10. Fuente: (Amutio Gómez et al., 2012).

4.2.4. Evaluación de Impacto y Probabilidad

El impacto estima el daño que causaría la materialización de una amenaza sobre la dimensión de seguridad más afectada del activo, mientras que la probabilidad estima la posibilidad de que dicha amenaza se concrete, considerando las vulnerabilidades y los controles ya existentes en el departamento de TI del GADICC. Ambas se califican en una escala de 1 a 5 (Tablas 7 y 8).

Tabla 7

Escala de calificación del impacto.

Valor	Nivel de impacto
1	Muy bajo
2	Bajo
3	Medio
4	Alto
5	Muy alto

Nota. El impacto estima el daño que causaría la materialización de una amenaza sobre la dimensión de seguridad más afectada del activo.

Tabla 8

Escala de calificación de la probabilidad.

Valor	Nivel de probabilidad
1	Muy baja (poco probable)
2	Baja
3	Media
4	Alta
5	Muy alta (casi seguro)

Nota. La probabilidad estima la posibilidad de que una amenaza se concrete, considerando las vulnerabilidades y los controles de seguridad ya existentes en el departamento de TI del GADICC. Fuente: (Amutio Gómez et al., 2012)

4.2.5. Cálculo del riesgo

El riesgo se calcula multiplicando el valor de impacto por el valor de probabilidad, obteniéndose un resultado entre 1 y 25 que se interpreta según los rangos de la Tabla 9.

Tabla 9

Escala de interpretación del nivel de riesgo

Rango	Nivel de riesgo
1-4	Bajo
5-9	Medio
10-15	Alto
16-25	Crítico

Nota. El riesgo se calcula multiplicando el valor de impacto por el valor de probabilidad (Riesgo = Impacto × Probabilidad). El color de cada fila identifica el nivel de riesgo correspondiente.

La Tabla 10 presenta la matriz de riesgo resultante para los activos prioritarios del departamento de TI del GADICC, seleccionados por su valor global de 9 o 10 y por su vinculación directa con los dominios de mayor brecha detectados en el diagnóstico del Capítulo III: seguridad física y ambiental, aspectos organizativos y gestión de activos.

Tabla 10

Matriz de riesgo de los activos prioritarios del departamento de TI del GADICC

Código	Activo	Amenaza	Imp.	Prob.	Riesgo	Nivel
ACT-D-01	Base de datos institucional del municipio	[A.11] Acceso no autorizado	5	3	15	Alto
ACT-D-01	Base de datos institucional del municipio	[E.19] Fugas de información	5	3	15	Alto
ACT-D-04	Credenciales y datos de autenticación	[A.5] Suplantación de identidad	5	3	15	Alto
ACT-D-06	Registros de actividad (logs)	[E.3] Errores de monitorización (log)	5	3	15	Alto
ACT-S-02	Sistema Integrado Municipal (SIM)	[A.24] Denegación de servicio	4	3	12	Alto
ACT-S-07	Certificados digitales (PKI)	[A.6] Abuso de privilegios de acceso	4	3	12	Alto
ACT-L-02	Cuarto de servidores (data center)	[N.1] Fuego	5	3	15	Alto
ACT-L-02	Cuarto de servidores (data center)	[I.7] Condiciones inadecuadas de temperatura/humedad	4	4	16	Crítico
ACT-AUX-01	UPS / SAI	[I.6] Corte del suministro eléctrico	4	3	12	Alto
ACT-P-01	Adm. de sistemas, seguridad y comunicaciones	[E.28] Indisponibilidad del personal clave	4	3	12	Alto
ACT-S-04	Acceso remoto VPN	[A.14] Interceptación de información	4	2	8	Medio

Código	Activo	Amenaza	Imp.	Prob.	Riesgo	Nivel
ACT-HW-06	Firewall Sophos	[A.24] Denegación de servicio	4	2	8	Medio

Nota. Imp. = Impacto; Prob. = Probabilidad. Los activos se priorizaron por su valor global (VG) de 9 o 10 en la Tabla 17 y por su vinculación con las brechas de mayor criticidad del diagnóstico. Fuente. Elaboración porpia.

4.2.6. Controles de Seguridad

A partir de los riesgos calificados como "Alto" o "Crítico" en la Tabla 11, se identificaron los controles del Anexo A de la norma ISO/IEC 27002:2022 aplicables a cada caso. Estos controles coinciden con las brechas ya documentadas en el diagnóstico del Capítulo III, lo que confirma la coherencia entre el análisis de cumplimiento normativo (encuesta de 63 ítems) y el análisis de riesgo de activos (MAGERIT). La Tabla 23 resume esta correspondencia.

Tabla 11

Controles de seguridad aplicables a los riesgos prioritarios identificados en el departamento de TI del GADICC.

Activo(s)	Descripción	Riesgo asociado	Controles ISO/IEC 27002:2022 (Anexo A)
ACT-D-01 / ACT-D-04	Base de datos institucional / Credenciales de autenticación	Acceso no autorizado, fugas de información, suplantación de identidad	5.12 Clasificación de la información · 5.13 Etiquetado de la información · 8.5 Autenticación segura · 8.24 Uso de criptografía
ACT-D-06	Registros de actividad (logs)	Errores de monitorización	5.25 Evaluación y decisión sobre eventos de seguridad · 8.16 Actividades de monitoreo
ACT-S-02	Sistema Integrado Municipal (SIM)	Denegación de servicio	8.7 Protección contra código malicioso · 8.16 Actividades de monitoreo
ACT-S-07	Certificados digitales (PKI)	Abuso de privilegios de acceso	5.18 Derechos de acceso · 8.24 Uso de criptografía
ACT-L-02	Cuarto de servidores (data center)	Fuego, condiciones ambientales inadecuadas	7.5 Protección contra amenazas físicas y ambientales · 7.8 Emplazamiento y protección de equipos · 7.2 Entrada física

Activo(s)	Descripción	Riesgo asociado	Controles ISO/IEC 27002:2022 (Anexo A)
ACT-AUX-01	UPS / SAI	Corte del suministro eléctrico	7.11 Instalaciones de suministro · 7.5 Protección contra amenazas físicas y ambientales
ACT-P-01	Adm. de sistemas, seguridad y comunicaciones	Indisponibilidad del personal clave (concentración de funciones)	5.2 Roles y responsabilidades de seguridad · 6.8 Reporte de eventos de seguridad · 5.35 Revisión independiente
ACT-S-04	Acceso remoto VPN	Interceptación de información	8.24 Uso de criptografía
ACT-HW-06	Firewall Sophos	Denegación de servicio	8.20 Seguridad de las redes

Nota. Los controles corresponden al Anexo A de la norma ISO/IEC 27002:2022 y se seleccionaron a partir de los riesgos calificados como Alto o Crítico en la Tabla 22.

4.2.7. Resumen de la matriz de riesgo

Del inventario de 50 activos de información del departamento de TI del GADICC, 25 (50 %) obtuvieron un valor global de 9 o 10 (muy alto o crítico), concentrados principalmente en los datos institucionales (base de datos, credenciales, registros de actividad), el Sistema Integrado Municipal y sus componentes de software, y elementos críticos de red como el firewall perimetral. El análisis de riesgo aplicado a estos activos prioritarios evidencia que los niveles más altos no se concentran únicamente en los sistemas de información en sí mismos, sino también en las condiciones organizativas y físicas que rodean su operación: la ausencia de controles ambientales y de acceso físico en el cuarto de servidores calificada como riesgo crítico ante condiciones inadecuadas de temperatura o humedad, la falta de clasificación y etiquetado formal de la información institucional, y la concentración de funciones críticas de administración de sistemas, seguridad y comunicaciones en un número reducido de personas.

Estos hallazgos son consistentes con el diagnóstico del Capítulo III, en el que los dominios de seguridad física y ambiental (37,5 %) y aspectos organizativos (50,0 %)

presentaron los niveles de cumplimiento más bajos frente a la norma ISO/IEC 27002:2022. Los controles priorizados en la Tabla 11 clasificación y etiquetado de la información, protección física y ambiental del centro de datos, uso de criptografía en el acceso remoto y en las credenciales, y formalización de roles y responsabilidades de seguridad constituyen, en consecuencia, los ejes centrales sobre los que se estructurarán las políticas del manual propuesto en la sección 4.6.

4.3. Directrices o políticas para la seguridad de la información

Con base en el análisis de riesgo desarrollado en la sección 4.5 y en las brechas identificadas en el diagnóstico institucional del Capítulo III, a continuación, se presentan las políticas que integran el manual de seguridad de la información propuesto para el departamento de TI del GADICC. Las políticas se organizan según las cuatro categorías de controles del Anexo A de la norma ISO/IEC 27002:2022 organizacionales, de personas, físicos y tecnológicos y cada una especifica su objetivo, alcance, directrices concretas, responsable de aplicación y periodicidad de revisión, en coherencia con los requisitos de planificación, operación y mejora continua de la norma ISO/IEC 27001:2022.

4.3.1. Políticas del dominio organizacional

a. POL-01. Política general de seguridad de la información (Control 5.1)

Objetivo: Establecer el compromiso formal del GADICC con la seguridad de la información y el marco general que rige su gestión.

Alcance: Todo el personal, los activos de información y los sistemas del departamento de TI del GADICC (Tabla 3).

Directrices:

- La máxima autoridad administrativa del GADICC aprobará formalmente el presente manual y sus actualizaciones.
- El manual se difundirá a todo el personal del departamento de TI y a las áreas usuarias de los sistemas institucionales.
- El documento se revisará al menos una vez al año o ante cambios significativos en la infraestructura, la normativa o el nivel de riesgo institucional.

Procedimiento de implementación:

1. Elaborar el borrador del manual y presentarlo a la máxima autoridad administrativa (o al Comité de Seguridad, una vez constituido) para su revisión.
2. Obtener la aprobación formal mediante resolución o memorando institucional.
3. Publicar y distribuir el manual aprobado a todo el personal del departamento de TI y a las áreas usuarias, mediante correo institucional y una sesión informativa inicial.
4. Registrar la fecha de aprobación y programar la siguiente revisión en el calendario institucional.

Responsable: Máxima autoridad administrativa (aprobación); responsable de TI (elaboración y difusión).

Revisión: Anual.

b. POL-02. Roles, responsabilidades y comité de seguridad de la información (Controles 5.2, 5.35)

Objetivo: Formalizar las responsabilidades de seguridad y establecer un mecanismo de supervisión independiente, dado que las funciones de administración de sistemas, seguridad y comunicaciones se concentran actualmente en un número reducido de personal (activo ACT-P-01).

Alcance: La estructura organizativa del GADICC vinculada a la seguridad de la información.

Directrices:

- Se conformará un Comité de Seguridad de la Información integrado por la máxima autoridad, el responsable de TI y un delegado administrativo, que se reunirá al menos semestralmente.
- Se documentarán y asignarán formalmente los roles de administrador de sistemas, administrador de seguridad, administrador de comunicaciones y administrador de bases de datos.
- Se realizarán auditorías internas independientes al menos una vez al año, ejecutadas por personal distinto al que administra los sistemas evaluados.

Procedimiento de implementación:

1. Designar formalmente, mediante memorando de la máxima autoridad, a los integrantes del Comité de Seguridad de la Información.
2. Notificar por escrito a cada funcionario del departamento de TI el rol de seguridad que le corresponde.
3. Convocar y realizar la primera sesión del comité para aprobar el cronograma anual de auditorías internas.
4. Designar al personal, interno o externo al área de TI, que ejecutará la primera auditoría independiente.

Responsable: Comité de Seguridad de la Información.

Revisión: Semestral.

c. POL-03. Clasificación y etiquetado de la información (Controles 5.12, 5.13)

Objetivo: Establecer niveles de clasificación de la información institucional para proteger los activos de mayor criticidad (ACT-D-01, ACT-D-04, ACT-D-06, entre otros con valor global 9-10).

Alcance: Toda la información gestionada por el departamento de TI, en formato físico y digital.

Directrices:

- La información se clasificará en los niveles Pública, Interna, Confidencial y Crítica, según su impacto ante una divulgación no autorizada.
- Todo activo de información con valor global (VG) igual o mayor a 9 (Tabla 5) se clasificará, como mínimo, como Confidencial.
- Los documentos y bases de datos se etiquetarán, física o digitalmente, indicando su nivel de clasificación y su responsable.

Procedimiento de implementación:

1. Elaborar una guía de clasificación con los cuatro niveles definidos y ejemplos basados en los activos del inventario (Tabla 3).
2. Revisar la valoración de cada activo (Tabla 5) y asignarle el nivel de clasificación correspondiente.
3. Etiquetar los activos digitales y físicos conforme a la clasificación asignada.
4. Notificar al responsable de cada activo su nivel de clasificación y las restricciones de manejo aplicables.

Responsable: Responsable de TI, en coordinación con el propietario de cada activo.

Revisión: Anual, o al incorporarse nuevos activos al inventario.

d. POL-04. Gestión de accesos y derechos de acceso (Controles 5.18, 8.5)

Objetivo: Garantizar que el acceso a los sistemas y a la información institucional se otorgue únicamente al personal autorizado y conforme a sus funciones.

Alcance: Los sistemas SIM, gestores de base de datos, PKI y demás activos de tipo [SW] y [S] del inventario.

Directrices:

- Los derechos de acceso se otorgarán según el principio de mínimo privilegio y se revisarán al menos semestralmente.
- Los certificados digitales (ACT-S-07) y las credenciales de autenticación (ACT-D-04) se gestionarán mediante un procedimiento formal de emisión, renovación y revocación.
- El acceso remoto se realizará exclusivamente a través de la VPN institucional (ACT-S-04), con autenticación multifactor para roles administrativos.

Procedimiento de implementación:

1. Levantar un inventario de usuarios y perfiles de acceso vigentes en el SIM, los gestores de base de datos y la VPN.
2. Ajustar los permisos existentes al principio de mínimo privilegio, retirando los accesos innecesarios.
3. Habilitar la autenticación multifactor para los roles administrativos y el acceso remoto.
4. Programar y ejecutar la revisión semestral de los derechos de acceso otorgados.

Responsable: Administrador de seguridad.

Revisión: Semestral.

e. POL-05. Relaciones con proveedores y terceros (Controles 5.19, 5.20, 5.21, 5.22)

Objetivo: Formalizar los requisitos de seguridad de la información en los contratos con proveedores de tecnología y servicios externos (ACT-S-06).

Alcance: Todo proveedor o tercero con acceso a los sistemas o a la información del GADICC.

Directrices:

- Todo contrato con proveedores de TI incluirá cláusulas de confidencialidad y de cumplimiento de controles mínimos de seguridad.
- Se mantendrá un registro de proveedores con acceso a los sistemas institucionales y el alcance de dicho acceso.
- Se evaluará periódicamente el cumplimiento de los proveedores críticos, en particular los de alojamiento/hosting y de pagos e intercambio de información.

Procedimiento de implementación:

1. Identificar a todos los proveedores actuales con acceso a sistemas o información del GADICC (hosting, pagos, soporte técnico).
2. Incorporar cláusulas de confidencialidad y de seguridad de la información en los contratos vigentes y en los futuros.
3. Elaborar y mantener actualizado el registro de proveedores con el alcance de su acceso.
4. Programar la evaluación anual del cumplimiento de seguridad de los proveedores críticos.

Responsable: Responsable de TI, en coordinación con la unidad de contratación.

Revisión: Anual, o al renovar contratos.

f. POL-06. Gestión de incidentes y evaluación de eventos de seguridad (Controles 5.25, 8.16)

Objetivo: Establecer un procedimiento formal para la identificación, evaluación y reporte de eventos e incidentes de seguridad, subsanando la brecha detectada en el diagnóstico del Capítulo III sobre la valoración de eventos de seguridad.

Alcance: Todos los sistemas y registros de actividad del departamento de TI (ACT-D-06).

Directrices:

- Todo evento de seguridad detectado en los registros de actividad se evaluará dentro de las veinticuatro horas siguientes para determinar si constituye un incidente.
- Los incidentes se clasificarán por severidad y se reportarán a la máxima autoridad administrativa cuando afecten activos con valor global igual o mayor a 9.
- Se mantendrá un registro histórico de incidentes y de las acciones correctivas aplicadas.

Procedimiento de implementación:

1. Documentar el procedimiento de reporte, clasificación y escalamiento de incidentes.
2. Habilitar un canal de reporte accesible para todo el personal (correo institucional o formulario interno).
3. Capacitar al personal de TI en la evaluación de eventos dentro del plazo de veinticuatro horas establecido.
4. Implementar el registro (bitácora) de incidentes y de las acciones correctivas aplicadas.

Responsable: Responsable de TI.

Revisión: Continua; el procedimiento se revisará anualmente.

g. POL-07. Revisión y mejora continua del manual (relacionada con el Control 5.35 y la cláusula 10 de la ISO/IEC 27001:2022)

Objetivo: Asegurar que el manual y sus políticas se mantengan vigentes y efectivos frente a cambios tecnológicos, regulatorios u organizacionales.

Alcance: El conjunto de políticas del presente manual.

Directrices:

- El manual se revisará formalmente al menos una vez al año por el Comité de Seguridad de la Información.
- Toda auditoría interna o externa que identifique no conformidades generará un plan de acción con responsables y plazos definidos.
- Las actualizaciones del manual se documentarán con control de versiones y se comunicarán al personal afectado.

Procedimiento de implementación:

1. Incluir en el cronograma anual del Comité de Seguridad una sesión dedicada a la revisión del manual.
2. Recopilar los hallazgos de auditorías internas o externas y los incidentes registrados durante el periodo.
3. Actualizar las políticas afectadas y documentar los cambios con número de versión y fecha.
4. Comunicar las actualizaciones al personal correspondiente.

Responsable: Comité de Seguridad de la Información.

Revisión: Anual.

4.3.2. Políticas del dominio de personas

a. POL-08. Concienciación, formación y reporte de eventos de seguridad (Control 6.8)

Objetivo: Fortalecer el conocimiento del personal técnico y administrativo sobre sus responsabilidades de seguridad y los procedimientos de reporte de incidentes, atendiendo la brecha detectada en el Capítulo III.

Alcance: Todo el personal del departamento de TI y los usuarios internos (ACT-P-05) de los sistemas institucionales.

Directrices:

- Se impartirá una capacitación anual obligatoria sobre seguridad de la información a todo el personal del departamento de TI.
- Se difundirá un procedimiento simple y conocido por todo el personal para reportar eventos o sospechas de incidentes de seguridad.
- El personal nuevo recibirá una inducción de seguridad de la información antes de acceder a los sistemas institucionales.

Procedimiento de implementación:

1. Diseñar el contenido de la capacitación anual (políticas, clasificación de la información, reporte de incidentes).
2. Programar la capacitación obligatoria para todo el personal de TI y los usuarios clave de los sistemas institucionales.
3. Incorporar la inducción de seguridad de la información al proceso de ingreso de personal nuevo.
4. Evaluar la comprensión del personal mediante una prueba corta o encuesta posterior a la capacitación.

Responsable: Responsable de TI, en coordinación con Recursos Humanos.

Revisión: Anual.

4.3.3. Políticas del dominio físico

a. POL-09. Seguridad física del centro de datos (Controles 7.2, 7.3, 7.8)

Objetivo: Proteger el cuarto de servidores (ACT-L-02) y los equipos críticos (ACT-HW-01, ACT-HW-02) frente a accesos no autorizados, subsanando la brecha identificada como la más crítica del diagnóstico institucional (37,5 % de cumplimiento en el dominio de seguridad física y ambiental).

Alcance: Las instalaciones físicas del centro de datos municipal.

Directrices:

- El acceso al cuarto de servidores se restringirá mediante un mecanismo de control (llave, tarjeta o registro de acceso) y se limitará al personal autorizado de TI.
- Se mantendrá un registro de ingresos de personal propio y de terceros al centro de datos.
- Los equipos de red y servidores se ubicarán en racks cerrados (ACT-L-03), fuera del alcance de personal no autorizado.

Procedimiento de implementación:

1. Instalar un mecanismo de control de acceso en la puerta del cuarto de servidores (cerradura, tarjeta o registro manual).
2. Implementar y mantener el registro de ingresos de personal propio y visitantes.
3. Asegurar en racks cerrados los equipos que actualmente no cuenten con esta protección.
4. Realizar una inspección trimestral del cumplimiento de estos controles.

Responsable: Responsable de TI.

Revisión: Anual.

b. POL-10. Protección ambiental y continuidad eléctrica (Controles 7.5, 7.11)

Objetivo: Reducir el riesgo crítico identificado en la Tabla 10 condiciones inadecuadas de temperatura o humedad, riesgo 16 y garantizar la continuidad eléctrica del centro de datos (ACT-AUX-01, ACT-AUX-02).

Alcance: El cuarto de servidores y los sistemas de respaldo eléctrico del GADICC.

Directrices:

- Se instalará y mantendrá un sistema de climatización adecuado en el cuarto de servidores, con monitoreo de temperatura y humedad.
- El UPS y el generador eléctrico se someterán a mantenimiento preventivo periódico y pruebas de autonomía.
- Se instalarán detectores de humo o sistemas de mitigación de incendios acordes al riesgo identificado ([N.1] Fuego).

Procedimiento de implementación:

1. Evaluar el estado actual del sistema de climatización e instalar o ajustar el equipo necesario.
2. Programar el mantenimiento preventivo periódico del UPS y del generador, incluyendo pruebas de autonomía.
3. Instalar detectores de humo u otro sistema de mitigación de incendios en el cuarto de servidores.
4. Documentar los resultados de cada mantenimiento y prueba realizada.

Responsable: Responsable de TI, en coordinación con el área administrativa.

Revisión: Semestral.

c. POL-11. Seguridad del cableado estructurado (Control 7.12)

Objetivo: Proteger el cableado estructurado (ACT-AUX-04) y el backbone de fibra óptica (ACT-AUX-03) frente a daños o interceptación.

Alcance: La infraestructura de cableado de la red institucional.

Directrices:

- El cableado se instalará en canalizaciones protegidas y se mantendrá separado de fuentes de interferencia electromagnética.
- Se documentará el mapa de cableado y se etiquetarán los puntos de red.
- Toda intervención sobre el cableado se registrará y será autorizada por el administrador de comunicaciones.

Procedimiento de implementación:

1. Elaborar el mapa actualizado del cableado estructurado y del backbone de fibra óptica.
2. Verificar y corregir los tramos expuestos a interferencia electromagnética o daño físico.
3. Etiquetar los puntos de red conforme al mapa elaborado.
4. Establecer que toda intervención futura sobre el cableado quede registrada y autorizada por el administrador de comunicaciones.

Responsable: Administrador de comunicaciones.

Revisión: Anual.

4.3.4. Políticas del dominio tecnológico

a. POL-12. Uso de criptografía y autenticación segura (Controles 8.5, 8.24)

Objetivo: Proteger la confidencialidad de las credenciales (ACT-D-04), el acceso remoto (ACT-S-04) y los certificados digitales (ACT-S-07), subsanando la brecha de uso de controles criptográficos detectada en el diagnóstico del Capítulo III.

Alcance: Los sistemas de autenticación, acceso remoto y firma electrónica del GADICC.

Directrices:

- Las contraseñas y credenciales se almacenarán cifradas, y se aplicará autenticación multifactor para los accesos administrativos y remotos.
- La VPN institucional utilizará protocolos de cifrado vigentes y se auditará periódicamente su configuración.
- Los certificados digitales (PKI) se renovarán antes de su vencimiento y se revocarán de inmediato ante sospecha de compromiso.

Procedimiento de implementación:

1. Configurar el cifrado de las credenciales almacenadas y de las conexiones VPN conforme a protocolos vigentes.
2. Habilitar la autenticación multifactor para los accesos administrativos y remotos.
3. Establecer el procedimiento de emisión, renovación y revocación de los certificados digitales (PKI).
4. Auditar semestralmente la configuración criptográfica de los sistemas críticos.

Responsable: Administrador de seguridad.

Revisión: Semestral.

b. POL-13. Monitoreo de actividad y gestión de registros (Control 8.16)

Objetivo: Garantizar la trazabilidad de las acciones sobre los sistemas institucionales mediante el monitoreo de los registros de actividad (ACT-D-06), atendiendo la brecha de errores de monitorización identificada en el análisis de riesgo (Tabla 10).

Alcance: Los servidores, aplicaciones y equipos de red del departamento de TI.

Directrices:

- Los registros (logs) de los sistemas críticos se revisarán periódicamente y se conservarán por un periodo mínimo definido institucionalmente.
- Se establecerán alertas ante eventos anómalos en los sistemas de mayor criticidad (SIM, base de datos institucional, firewall).
- El acceso a los registros de actividad se restringirá al personal autorizado, para preservar su integridad como evidencia.

Procedimiento de implementación:

1. Configurar la generación y el almacenamiento centralizado de los registros de los sistemas críticos.
2. Definir el periodo mínimo de conservación de los registros conforme a las necesidades institucionales.
3. Configurar alertas automáticas para eventos anómalos en el SIM, la base de datos institucional y el firewall.
4. Restringir el acceso a los registros de actividad al personal autorizado.

Responsable: Responsable de TI.

Revisión: Semestral.

c. POL-14. Seguridad de las redes y protección perimetral (Controles 8.7, 8.20)

Objetivo: Proteger la red institucional (ACT-COM-01) y el firewall perimetral (ACT-HW-06) frente a accesos no autorizados y software malicioso.

Alcance: La red interna, la conexión a Internet y los sistemas de protección perimetral del GADICC.

Directrices:

- Se mantendrá la segmentación de la red institucional en VLAN según el criterio de criticidad de cada área o sistema.
- Las reglas del firewall perimetral se revisarán y actualizarán periódicamente, documentando los cambios realizados.
- El software antivirus (ACT-SW-08) se mantendrá actualizado en todos los equipos y servidores, con revisión periódica de su cobertura.

Procedimiento de implementación:

1. Revisar y documentar la segmentación actual de las VLAN institucionales.
2. Actualizar las reglas del firewall perimetral conforme a los riesgos identificados en la Tabla 22.
3. Verificar que el antivirus institucional esté actualizado en todos los servidores y equipos.
4. Programar revisiones semestrales de la configuración de red y del firewall.

Responsable: Administrador de comunicaciones / administrador de seguridad.

Revisión: Semestral.

Las catorce políticas presentadas constituyen el manual de políticas de seguridad de la información propuesto para el departamento de TI del GADICC. Cada política integra su objetivo, alcance, directrices, procedimiento de implementación, responsable

de aplicación y mecanismo de revisión, en cumplimiento del cuarto objetivo específico de la presente investigación.

CONCLUSIONES

En relación con el primer objetivo específico, se construyó el marco teórico sobre seguridad de la información, políticas de seguridad organizacional y la norma ISO/IEC 27001:2022 mediante la revisión sistemática de literatura científica, normativa vigente y marcos de referencia internacionales, lo que permitió fundamentar conceptualmente el diseño del manual de políticas y justificar la selección de MAGERIT v3 como metodología de análisis de riesgos frente a otras alternativas como ISO/IEC 27005 y NIST Cybersecurity Framework.

En relación con el segundo objetivo específico, el diagnóstico aplicado al departamento de TI del GADICC determinó un nivel de cumplimiento general del 69,8 % frente a los sesenta y tres controles de la norma ISO/IEC 27002:2022 evaluados, nivel insuficiente para sustentar un Sistema de Gestión de Seguridad de la Información formal. Las brechas más críticas se concentraron en los dominios de seguridad física y ambiental (37,5 %), aspectos organizativos (50,0 %) y gestión de activos (60,0 %), lo que evidenció que las principales debilidades del departamento no se relacionan con la capacidad técnica del personal, sino con la ausencia de mecanismos formales de gobernanza, clasificación de la información y protección física del centro de datos.

En relación con el tercer objetivo específico, el análisis de riesgo desarrollado mediante MAGERIT permitió identificar y valorar cincuenta activos de información del departamento de TI, de los cuales veinticinco (50 %) presentaron un valor global de 9 o 10 en la escala de 0 a 10. A partir de este análisis se determinó que el riesgo de mayor severidad corresponde a las condiciones ambientales inadecuadas del cuarto de servidores calificado como crítico, seguido de riesgos altos vinculados al acceso no autorizado a la base de datos institucional, la suplantación de identidad en las credenciales de autenticación y la concentración de funciones críticas en un número reducido de personal

técnico. Estos hallazgos permitieron definir las políticas de seguridad alineadas a los controles del Anexo A de la norma ISO/IEC 27002:2022 que efectivamente atienden dichos riesgos y brechas.

En relación con el cuarto objetivo específico, se estructuró el manual de políticas de seguridad de la información del departamento de TI del GADICC mediante la integración de catorce políticas organizadas en los cuatro dominios de la norma ISO/IEC 27002:2022 organizacional, personas, físico y tecnológico, cada una con su objetivo, alcance, directrices, procedimiento de implementación, responsable de aplicación y mecanismo de revisión. Esta estructura provee al departamento de TI un instrumento normativo completo y aplicable, y no únicamente un marco declarativo de intenciones.

En consecuencia, se concluye que el objetivo general de la investigación fue alcanzado: se diseñó un manual de políticas de seguridad de la información para el departamento de TI del GADICC, basado en la norma ISO/IEC 27001:2022, fundamentado en el diagnóstico de la situación actual, en la identificación de los controles aplicables del Anexo A de la norma ISO/IEC 27002:2022 y en la definición de políticas formales orientadas a fortalecer la confidencialidad, integridad y disponibilidad de los activos de información institucional.

RECOMENDACIONES

Se recomienda a la máxima autoridad del GADICC aprobar formalmente el manual de políticas de seguridad de la información mediante el acto administrativo correspondiente y disponer su difusión obligatoria a todo el personal institucional, dejando constancia documentada de su recepción. Sin aprobación formal, el instrumento carece de exigibilidad y su aplicación queda sujeta a la voluntad individual de los servidores públicos.

Se recomienda conformar el Comité de Seguridad de la Información y designar al Oficial de Seguridad de la Información como acción de ejecución inmediata y prioritaria, por tratarse del presupuesto organizativo del que depende la exigibilidad de las restantes políticas. La designación del Oficial debe recaer en un profesional distinto de quien administra la plataforma tecnológica, a fin de materializar la segregación de funciones que actualmente no existe.

Se recomienda priorizar la intervención sobre el dominio de seguridad física y ambiental, por registrar el nivel de cumplimiento más bajo del diagnóstico y por proteger los activos de hardware e instalaciones que soportan al resto del inventario. En particular, se sugiere gestionar la implementación de un sistema de detección y extinción de incendios apropiado para equipamiento eléctrico, el control de acceso con registro al cuarto de servidores y la documentación actualizada del cableado estructurado.

Se recomienda a la institución elaborar un plan de migración de los componentes tecnológicos que han alcanzado el fin de su ciclo de soporte, considerando que sobre ellos se sustentan el servicio de correo institucional y la base de datos institucional, ambos valorados con criticidad muy alta. Se sugiere acompañar el plan de una evaluación técnica y económica que permita a la administración adoptar una decisión informada respecto de la actualización o la migración de plataforma.

Se recomienda documentar un plan de sucesión para las funciones críticas concentradas en personal clave, así como incorporar en los perfiles de puesto y en los contratos del personal las responsabilidades específicas de seguridad de la información, medidas que reducen la dependencia institucional respecto de personas determinadas.

REFERENCIAS

Ali, R. (2026). Operationalising information security management: A procedural framework analysis of ISO/IEC 27001:2022 implementation in a financial-technology organisation. arXiv. https://arxiv.org/abs/2604.23230

Amutio Gómez, M. A., Candau, J., y Mañas, J. A. (2012). *MAGERIT – versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información*. Ministerio de Hacienda y Administraciones Públicas.

Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems*. Wiley.

Condoy, R. J., y Vizñay, J. K. (2021). Diseño de la estructura de un manual de políticas de seguridad de la información para la Unidad de Informática del Gobierno Autónomo Descentralizado Municipal del Cantón Camilo Ponce Enríquez. *Dominio de las Ciencias, 7*(4), 293-318. https://doi.org/10.23857/dc.v7i6.2332

Conect LTDA. (2024, 30 de mayo). *www.linkedin.com*. https://www.linkedin.com/pulse/la-seguridad-de-informaci%C3%B3n-una-prioridad-para-tu-empresa-xg18e/

Díaz, R. (2023). *repository.unad.edu.co*. https://repository.unad.edu.co/bitstream/handle/10596/60042/ANALISIS_DE_LOS_ESTANDARES_Y_BUENAS_PRACTICAS_DE_CIBERSEGURIDAD_UTILIZADOS_POR_LA_INDUSTRIA_COLOMBIANA.pdf?sequence=1&isAllowed=y

Domínguez-Domínguez, R., Flores-Laguna, O. A., y Valle-López, J. del. (2023). Evaluation of an information management system at a Mexican higher education institution. arXiv. https://doi.org/10.48550/arXiv.2306.11050

drmunozcl. (2025, 18 de mayo). *www.infoproteccion.com*. https://www.infoproteccion.com/iso-27001/principales-cambios-de-norma-iso-270012022/

Enríquez, E. G. (2024, 2 de junio). *repositorio.utn.edu.ec*. https://repositorio.utn.edu.ec/handle/123456789/16138

European Union Agency for Cybersecurity. (2024). *www.enisa.europa.eu*. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Finn, T., y Downie, A. (2026). *www.ibm.com/es-es*. https://www.ibm.com/es-es/think/topics/risk-mitigation

Flores, D., y Perugachi, R. (2023). A GDPR-compliant risk management approach based on threat modelling and ISO 27005. arXiv. https://arxiv.org/abs/2306.04783

GADICC CAÑAR. (2026). *www.canar.gob.ec*. https://www.canar.gob.ec/quienes-somos

Haney, J. M., y Lutters, W. (2023). From compliance to impact: Tracing the transformation of an organizational security awareness program. arXiv. https://arxiv.org/abs/2309.07724

Hielscher, J., y Parkin, S. (2024). "What keeps people secure is that they met the security team": Deconstructing drivers and goals of organizational security awareness. arXiv. https://arxiv.org/abs/2404.18365

IBM. (2026, 6 de enero). *www.ibm.com*. https://www.ibm.com/es-es/think/topics/risk-management

International Organization for Standardization. (2022). *www.iso.org*. https://www.iso.org/standard/80585.html

International Organization for Standardization, y International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity*

and privacy protection Information security management systems Requirements. International Organization for Standardization.

ISO. (2026, 4 de mayo). *www.iso.org*. https://www.iso.org/es/norma/27001

Joint Task Force. (2020). *Security and privacy controls for information systems and organizations*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Kurniawan, E., Riadi, I., Irmawan, A., y Arusani. (2022). Performance measurement of security academic information system using maturity level. arXiv. https://arxiv.org/abs/2204.09511

Ministerio de Tecnologías de la Información y las Comunicaciones. (2025). *gobiernodigital.mintic.gov.co*. https://gobiernodigital.mintic.gov.co/692/articles-418986_recurso_1.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2021). *Esquema Gubernamental de Seguridad de la Información (EGSI), versión 2.0*.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2023). *www.telecomunicaciones.gob.ec*. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2024/09/Politica-Publica-de-Telecomunicaciones-2023-2025.pdf

Morillo, D. (2024). *repositorio.puce.edu.ec*. https://repositorio.puce.edu.ec/server/api/core/bitstreams/c963af86-95ac-4066-b157-7e2136db3d2f/content

NIST. (2024, 24 de febrero). *nvlpubs.nist.gov*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

nqa. (2026, 18 de mayo). *www.nqa.com*. https://www.nqa.com/medialibraries/NQA/NQA-Media-

Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Ortiz, K. (2022). *dspace.ups.edu.ec*. https://dspace.ups.edu.ec/bitstream/123456789/23698/1/GT004012.pdf

Ortiz-Lazo, J. E., y Vizñay-Duran, J. K. (2019). Análisis de riesgo y vulnerabilidades de la red de datos, en un ISP, utilizando el estándar ISO/IEC 2007:2008. Caso de estudio: Empresa Sistelcel. *Ciencias de la Computación y Telecomunicaciones, 4*(7).

Podrecca, M., Culot, G., Nassimbeni, G., y Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*.

Rios, J. (2024). *oa.upm.es*. https://oa.upm.es/80516/1/TFG_JAVIER_RIOS_SERRANO.pdf

Rodríguez, S. (2025). *dspace.umh.es*. https://dspace.umh.es/handle/11000/37545

Sánchez, R. (2026). *ricardo-sb.blogspot.com*. https://ricardo-sb.blogspot.com/2017/11/gestion-de-riesgos-en-seguridad-de-la.html

Silva, J. M., Ribeiro, D., Ramos, L. F., y Fonte, V. (2023). A worldwide overview on the information security posture. arXiv. https://doi.org/10.48550/arXiv.2310.01200

Stallings, W., y Brown, L. (2021). *Computer security: Principles and practice*. Pearson.

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standardsA review and comprehensive overview. *Electronics, 11*(14), Artículo 2181. https://doi.org/10.3390/electronics11142181

Villarreal Morales, V., Coro Villarreal, K. E., Fernández Sánchez, E. G., y Cueva Martinez, J. P. (2024). Sistema gestión de seguridad de la información y su

impacto en el gobierno y gestión de las tecnologías de la información. *Ciencia Latina Revista Científica Multidisciplinar*.

Whitman, M. E., y Mattord, H. J. (2022). *Principles of information security*. Cengage.

ANEXOS

Anexo 1: Protocolo de Investigación

Anexo: Formato del Anteproyecto.

A. TÍTULO
Diseño de un manual de políticas de seguridad de la información para el departamento de TI del GADICC, basado en la norma ISO/IEC 27001:2022

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Tecnologías de Información y Comunicación	**Ciencias exactas, naturales y tecnológicas**	Inteligencia de Negocios	
		Sistemas de Información	
		Gobierno y administración de tecnologías de información	
		Auditoría Informática	
		Seguridad Informática	**x**
		Redes y comunicación	
		Arquitectura de Hardware	
		Arquitectura de desarrollo de software	
		Ingeniería de Software	
		Gestión y gobierno de proyectos de tecnología informática	
		Ingeniería de requerimientos	
		Algoritmos y programación	
		Ciencias exactas y naturales (Matemáticas, Física, Química, Biología, etc.)	
		Modelaje y simulación	

C. PLANTEAMIENTO DEL PROBLEMA

En la actualidad, la información se ha consolidado como uno de los activos estratégicos más valiosos para las organizaciones públicas y privadas. Su gestión adecuada, en términos de confidencialidad, integridad y disponibilidad, resulta indispensable para garantizar la continuidad operativa, el cumplimiento normativo y la confianza ciudadana en los servicios gubernamentales (Podrecca, Culot, Nassimbeni , & Sartor, 2022). La transformación digital de los gobiernos locales ha incrementado significativamente el volumen de datos institucionales gestionados y, con ello, la exposición a amenazas como accesos no autorizados, fugas de información, errores humanos y ataques informáticos.

El Gobierno Autónomo Descentralizado Intercultural del Cantón Cañar (GADICC) es un organismo público que gestiona los recursos y servicios municipales y administra las operaciones del cantón. El departamento de Tecnologías de la Información del GADICC administra los sistemas de gestión institucional, bases de datos ciudadanas, red e infraestructura, computación personal y servicios digitales. Sin embargo, la gestión de la seguridad de la información por parte de este departamento se realiza de manera informal, sin políticas documentadas, controles formalizados ni procedimientos para incidentes de seguridad (Villarreal Morales, Coro Villarreal, Fernández Sánchez, & Cueva Martinez, 2024).

La Ley Orgánica Ecuatoriana para la Protección de Datos Personales (LOPDP) exige que el sector público cuente con protocolos de seguridad que cumplan con estándares internacionales. El Esquema de Seguridad de la Información Gubernamental (EGSI) v2.0 se basa en la norma ISO/IEC 27001, continuando desde 2021. Esto establece estándares mínimos de seguridad que todas las instituciones públicas en Ecuador y los gobiernos autónomos descentralizados deben adoptar. Si no se cumplen estos estándares, puede haber consecuencias administrativas, el público puede perder confianza en los servicios digitales del GADICC y se puede perder información crítica (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021).

La infraestructura tecnológica del departamento de TI de GADICC incluye servidores, sistemas financieros y administrativos, bases de datos ciudadanas, una red interna, computadoras y sistemas de acceso remoto. Estos bloques no cuentan con controles de seguridad formales documentados, lo que genera algunas vulnerabilidades. No existen formas expresas de clasificar y gestionar la información institucional. Los sistemas empresariales y las bases de datos tienen un control inconsistente del acceso y privilegios

de los usuarios. No hay formas documentadas expresas para identificar y responder a problemas de seguridad. Además, no existen controles de seguridad formales documentados relacionados con el uso aceptable de los recursos de TI y no hay formas expresas de realizar copias de seguridad y recuperación de datos.

Sin un manual de política de seguridad de la información, el departamento de TI parece manejar sus propios problemas de seguridad y tomar decisiones relacionadas con la seguridad de manera improvisada e individual. Manejar los problemas de seguridad de esta manera pone en riesgo las operaciones del servicio público, así como la integridad de los registros institucionales y la privacidad de los datos de los ciudadanos en GADICC.

La norma ISO/IEC 27001:2022 propone un enfoque sistemático para la gestión de la seguridad de la información que incluye la definición de políticas, objetivos de seguridad, controles y un ciclo de mejora continua, constituyendo el marco de referencia idóneo para el diseño del manual propuesto (International Organization for Standardization; International Electrotechnical Commission, 2022).

Esta situación plantea la siguiente pregunta de investigación: ¿Cómo diseñar un manual de políticas de seguridad de la información, basado en la norma ISO/IEC 27001:2022, que permita al departamento de TI del GADICC establecer lineamientos formales y controles adecuados para la protección de los activos de información institucional?

D. OBJETIVO GENERAL

Diseñar un manual de políticas de seguridad de la información para el departamento de TI del GADICC, basado en la norma ISO/IEC 27001:2022, mediante el diagnóstico de la situación actual de seguridad, la identificación de controles aplicables del Anexo A de la norma ISO/IEC 27002:2022 y la definición de políticas formales alineadas al estándar internacional, con el fin de fortalecer la confidencialidad, integridad y disponibilidad de los activos de información institucional.

E. OBJETIVOS ESPECÍFICOS

1. Construir el marco teórico sobre seguridad de la información, políticas de seguridad organizacional y la norma ISO/IEC 27001:2022, mediante la revisión sistemática de literatura científica, normativa vigente y marcos de referencia internacionales, para fundamentar el diseño del manual de políticas de seguridad del departamento de TI del GADICC.
2. Diagnosticar el estado actual de la gestión de seguridad de la información en el departamento de TI del GADICC, mediante entrevistas al personal técnico, análisis documental y evaluación de los controles de seguridad existentes frente a los requerimientos de la norma ISO/IEC 27001:2022, con el fin de identificar las principales brechas y áreas de mejora.
3. Definir las políticas de seguridad de la información alineadas a los controles del Anexo A de la norma ISO/IEC 27002:2022, a través del análisis de riesgos y de las brechas identificadas en el diagnóstico, para establecer lineamientos formales y apropiados que protejan los activos de información del departamento de TI del GADICC.
4. Estructurar el manual de políticas de seguridad de la información del departamento de TI del GADICC, mediante la integración de las políticas definidas, los procedimientos de implementación, los roles y responsabilidades, y los mecanismos de revisión y actualización, para proveer un instrumento normativo que oriente la gestión segura de la información institucional.

F. JUSTIFICACIÓN

El presente proyecto comprende el diseño de un manual de políticas de seguridad de la información para el departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado Intercultural del Cantón Cañar (GADICC), tomando como referencia los requisitos de la norma ISO/IEC 27001:2022, los controles establecidos en la ISO/IEC 27002:2022 y las disposiciones aplicables del Esquema Gubernamental de Seguridad de la Información.

Para su desarrollo, se realizará un diagnóstico de la situación actual de la seguridad de la información en el departamento de TI, mediante entrevistas al personal técnico, revisión

documental y análisis de los controles existentes. Este análisis destacará tres componentes clave: las principales necesidades de protección de información, las amenazas y vulnerabilidades que enfrentan las instituciones, y las brechas en los mecanismos de protección.

El proyecto identificará y clasificará los activos de información críticos del departamento de TI y evaluará los riesgos en relación con su confidencialidad, integridad y disponibilidad. A partir de los hallazgos, se identificarán los controles de seguridad relevantes. La gestión de accesos, el uso aceptable de los recursos tecnológicos, la copia de seguridad y recuperación de información, la respuesta a incidentes, la protección de datos, la seguridad (tanto física como tecnológica), la continuidad operativa y la asignación de responsabilidades definirán los controles y políticas de seguridad establecidas.

El producto final incluirá un manual de políticas de seguridad de la información. Cada política incluirá el propósito de la política y el alcance de la misma, las partes responsables del cumplimiento de la política, las directrices institucionales relacionadas, los controles asociados y los mecanismos de revisión y actualización. Este documento ofrecerá al departamento de TI un marco regulatorio y metodológico para la gestión de la seguridad de la información y para la implementación de controles relacionados con las normas internacionales.

El alcance institucional se limita a los procesos, activos de información, infraestructura tecnológica y personal dentro del departamento de TI de GADICC. Por lo tanto, no se realizará una evaluación del resto de los departamentos o unidades municipales.

Asimismo, el proyecto no contempla la implementación operativa de las políticas diseñadas, la adquisición o instalación de herramientas tecnológicas, la ejecución de pruebas de penetración, la modificación de la infraestructura existente, la capacitación formal del personal ni la realización de una auditoría de certificación ISO/IEC 27001. Estas actividades podrán desarrollarse posteriormente, tomando como referencia el manual elaborado y las recomendaciones derivadas del diagnóstico.

G. ALCANCE

Este proyecto tiene como objetivo diagnosticar y diseñar un manual de políticas de seguridad de la información para el departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado Intercultural del Cantón Cañar (GADICC), basado en la norma ISO/IEC 27001:2022. Para ello, el desarrollo del proyecto contempla las siguientes etapas: primero, se diagnosticará la situación actual de la gestión de la seguridad de la información en el departamento de TI. A continuación, se identificarán y clasificarán los activos de información críticos. Posteriormente, se evaluarán los riesgos asociados a las amenazas y vulnerabilidades identificadas, considerando su probabilidad e impacto, y se analizarán las brechas existentes frente a los requisitos de la norma. Finalmente, se definirán las políticas, directrices, responsabilidades y procedimientos de seguridad de la información, en concordancia con los controles del Anexo A de la norma ISO/IEC 27001:2022 y las orientaciones de la ISO/IEC 27002:2022.

Este estudio se limita al diseño de un manual de políticas de seguridad de la información para el departamento de TI del GADICC y excluye su implementación operativa, la adquisición o instalación de herramientas e infraestructura tecnológica, la ejecución de pruebas técnicas de seguridad, la capacitación del personal y la realización de auditorías de certificación. El manual constituirá una base formal y estructurada que servirá como referencia para futuras fases de implementación, seguimiento, actualización y mejora continua de la seguridad de la información institucional.

H. CONCEPTOS RELACIONADOS

Seguridad de la información

La seguridad de la información se refiere a los principios, políticas y tecnologías que desarrollan las protecciones para la información en el contexto de amenazas a la confidencialidad, integridad y disponibilidad de dicha información. Dado el estado actual de la transformación digital, la seguridad de la información se ha convertido en un aspecto crítico para la sostenibilidad operativa de todas las organizaciones, especialmente aquellas que manejan información sensible y/o crítica (NIST, 2024).

ISO/IEC 27001:2022 afirma que se debe utilizar un método basado en riesgos para aplicar controles de seguridad de la información, donde una organización pueda comprender su exposición e incorporar las medidas de seguridad apropiadas contra los riesgos identificados (International Organization for Standardization; International

Electrotechnical Commission, 2022). Este método es flexible y puede emplearse en distintas operaciones organizativas y en diferentes entornos tecnológicos, y, como tal, se considera altamente efectivo.

Política de seguridad de la información

Una política de seguridad de la información es un documento formal que establece los objetivos, principios y reglas que una organización adopta para proteger sus activos de información. Las políticas de seguridad constituyen el fundamento del Sistema de Gestión de Seguridad de la Información (SGSI), ya que definen las expectativas de la dirección en materia de seguridad, establecen responsabilidades, orientan el comportamiento del personal y sirven como marco de referencia para la implementación de controles técnicos y organizativos. Según la norma ISO/IEC 27001:2022, la alta dirección debe establecer una política de seguridad de la información apropiada al propósito de la organización, que incluya objetivos de seguridad medibles y un compromiso explícito con la mejora continua del SGSI (International Organization for Standardization; International Electrotechnical Commission, 2022).

Manual de políticas de seguridad de la información

Un manual de políticas de seguridad de la información es un instrumento normativo que integra en un único documento el conjunto de políticas, procedimientos, directrices y controles que una organización establece para la gestión segura de su información. Su propósito es proporcionar al personal técnico y directivo una referencia consolidada y accesible que oriente la toma de decisiones en materia de seguridad. La estructuración de un manual basado en la norma ISO/IEC 27001:2022 y los controles del Anexo A de la ISO/IEC 27002:2022 permite alinear la gestión de la seguridad institucional con mejores prácticas internacionales, facilitando además el proceso de eventual certificación y la demostración de conformidad regulatoria (Ali, Operationalising Information Security Management: A Procedural Framework Analysis of ISO/IEC 27001:2022 Implementation in a Financial-Technology Organisation, 2026).

ISO/IEC 27001:2022

La norma ISO/IEC 27001:2022 detalla las expectativas internacionales para el desarrollo, la implementación y la mejora progresiva de un Sistema de Gestión de Seguridad de la Información (SGSI). Adoptando un enfoque basado en riesgos para los procesos de identificación, evaluación y tratamiento de amenazas, esta norma proporciona requisitos y estructuras para que las organizaciones los riesgos a sus activos de información de manera más sistemática y controlada (International Organization for Standardization; International Electrotechnical Commission, 2022).

ISO/IEC 27002:2022

La norma ISO/IEC 27002:2022 proporciona un conjunto de controles de mejores prácticas para la seguridad de la información, clasificados en cuatro categorías: controles organizativos (37 controles), controles de personas (8 controles), controles físicos (14 controles) y controles tecnológicos (34 controles). En el diseño de un manual de políticas de seguridad, la ISO/IEC 27002:2022 permite identificar los controles aplicables al

contexto del GADICC y estructurar las políticas correspondientes a cada dominio de seguridad (International Organization for Standardization; International Electrotechnical Commission, 2022).

Esquema Gubernamental de Seguridad de la Información (EGSI)

El Esquema Gubernamental de Seguridad de la Información (EGSI) es la normativa emitida por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) del Ecuador, que establece las directrices mínimas de seguridad de la información que deben adoptar las entidades del sector público ecuatoriano. El EGSI v2.0, vigente desde 2021, se basa en la norma NTE INEN-ISO/IEC 27001 e incorpora controles adaptados al contexto institucional ecuatoriano, incluyendo aspectos relacionados con la protección de datos personales en concordancia con la Ley Orgánica de Protección de Datos Personales (LOPDP). Para el GADICC, el cumplimiento del EGSI constituye una obligación normativa que refuerza directamente la pertinencia y necesidad del presente proyecto (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021).

Gestión de riesgos de seguridad de la información

La gestión de riesgos de seguridad de la información es el proceso mediante el cual una organización identifica, analiza, evalúa y trata los riesgos asociados a sus activos de información. Este proceso incluye la identificación de amenazas y vulnerabilidades, la valoración del impacto y la probabilidad de materialización de cada riesgo, y la selección de controles adecuados para su mitigación, transferencia, aceptación o eliminación. Según la norma ISO/IEC 27001:2022, la revisión de gestión de riesgos organizada, documentada y sensible a cambios es la base del SGSI dentro del manual de políticas de GADICC, la gestión de riesgos configura el orden en que se abordan las políticas, además de guiar la elección de controles a implementar en la institución (International Organization for Standardization; International Electrotechnical Commission, 2022).

Gobernanza de TI en el sector público

La gobernanza de TI en el sector público denota las estructuras y mecanismos a través de los cuales la organización gubernamental gestiona y rinde cuentas del uso de las tecnologías de la información para cumplir sus objetivos. En el campo de la seguridad de la información, la gobernanza de TI se refiere a la asignación de roles y responsabilidades específicas, la alineación de la seguridad con las misiones de la agencia y el establecimiento de mecanismos de control para hacer cumplir la normativa y el cumplimiento de los estándares (NIST, 2024).

I. TRABAJOS RELACIONADOS

Ali (2019) ofrece una visión global y procedimental sobre la ejecución de la norma ISO/IEC 27001:2022 en una organización fintech. Al describir las fases para la operacionalización de un Sistema de Gestión de Seguridad de la Información, Ali enfatiza

el papel de las políticas de seguridad documentadas como bloques de construcción del SGSI. El estudio muestra que la presencia de políticas articuladas mejora la implementación de los controles de seguridad y la respuesta a incidentes. Este estudio es útil para abordar las características y aspectos de un manual de políticas en el marco de ISO/IEC 27001:2022. Sin embargo, su organización contextual, una organización fintech del sector privado, está alejada de un Gobierno Autónomo Descentralizado. Los marcos regulatorios específicos del sector público ecuatoriano (EGSI, LOPDP), así como los tipos de información administrada, presentan desafíos diferentes.

Podrecca et al. (2022) investigan los efectos de la implementación de la norma ISO/IEC 27001 en el desempeño organizacional en organizaciones del sector servicios. Argumentan que la adopción formal de la norma (incluyendo la definición documentada de las políticas de seguridad) conduce a una mejora en la postura de seguridad y en la creación de valor para las partes interesadas. Aunque el estudio se realiza en el sector privado, las conclusiones sobre los beneficios de la formalización de las políticas pueden extenderse al sector público, ya que la confianza de los ciudadanos es equivalente al valor de los clientes en el sector privado. Esta investigación aporta evidencia empírica sobre el impacto positivo de las políticas documentadas, pero no aborda las particularidades de los gobiernos locales ni los requisitos específicos del sector público ecuatoriano.

A nivel nacional, Villarreal et al. (2024) estudian la relación entre los Sistemas de Gestión de Seguridad de la Información y el gobierno de las tecnologías de información en instituciones públicas ecuatorianas, identificando que la ausencia de políticas de seguridad formalizadas es una de las principales causas de las deficiencias en la gobernanza de TI. El estudio concluye que la formalización de un SGSI con políticas documentadas y controles estructurados mejora los indicadores de gobierno y gestión de TI en las instituciones analizadas. Este antecedente es directamente relevante para el presente proyecto, ya que aborda el contexto ecuatoriano y demuestra la pertinencia de formalizar las políticas de seguridad en entidades públicas nacionales. No obstante, el estudio no se enfoca específicamente en el diseño de manuales de políticas ni en el contexto de los gobiernos autónomos descentralizados.

A nivel local, las obras identificadas en el cantón Cañar abordan principalmente la gestión del riesgo tecnológico y la continuidad del negocio en el sector financiero cooperativo. Buscán et al. (2022) proponen un modelo de plan de continuidad del negocio para

cooperativas de ahorro y crédito en el cantón Cañar, que incluye el análisis de procesos críticos, la identificación de riesgos y las estrategias de recuperación. Aunque el alcance de este estudio es el sector financiero cooperativo, que es diferente al contexto del GADICC, la proximidad y la metodología de análisis de riesgos hacen que este estudio sea una referencia local relevante. Considerando la falta de estudios sobre el diseño de políticas de seguridad de la información en gobiernos autónomos descentralizados del cantón Cañar, el presente proyecto es original y relevante.

J. METODOLOGÍA

Este estudio combina métodos cualitativos y cuantitativos. Implica una evaluación de las prácticas existentes de seguridad de la información dentro del departamento de TI de GADICC y describe los riesgos y el cumplimiento con los controles de la Norma ISO/IEC 27001:2022. Este método ilustra el contexto organizacional y la evaluación de riesgos y amenazas de seguridad, que sirve como base para la segmentación basada en evidencia de los borradores de las políticas del manual.

Esta investigación emplea un nivel descriptivo-analítico en el cual se puede describir el entorno de seguridad de la información del departamento de TIC de GADICC, y se pueden identificar las principales vulnerabilidades, junto con el análisis del cumplimiento de los requisitos de la norma ISO/IEC 27001:2022. Asimismo, se evaluará la relación entre los procesos operativos del departamento y la necesidad de definir políticas específicas de seguridad que respondan a los riesgos identificados.

Con base en el diagnóstico y el análisis de riesgos, se procederá al diseño de las políticas de seguridad de la información siguiendo la estructura de los dominios de control de la norma ISO/IEC 27002:2022. Cada política incluirá: propósito, alcance, definiciones, responsabilidades, directrices específicas, controles asociados y mecanismos de revisión. Finalmente, las políticas serán integradas en un manual estructurado que constituirá el producto principal del proyecto, proveyendo al departamento de TI del GADICC un instrumento normativo para la gestión segura de la información institucional, en concordancia con el EGSI y la norma ISO/IEC 27001:2022.

K. CRONOGRAMA DE ACTIVIDADES								
N°	ACTIVIDAD	MES						
		I	II	III	IV	V	VI	MEDIOS DE VERIFICACIÓN
1	Revisión bibliográfica sobre seguridad de la información, políticas de seguridad y norma ISO/IEC 27001:2022	X	X					Matriz de revisión bibliográfica
2	Diagnóstico situacional del departamento de TI del GADICC: entrevistas al personal técnico, análisis documental y revisión de controles existentes		X	X				Documento de diagnóstico situacional
3	Identificación y clasificación de activos de información críticos y análisis de brechas (gap analysis) frente a la norma ISO/IEC 27001:2022			X	X			Inventario de activos y matriz de brechas
4	Análisis de riesgos de seguridad y selección de controles aplicables del Anexo A de la norma ISO/IEC 27002:2022				X			Matriz de riesgos y controles seleccionados
5	Diseño y redacción de las políticas de seguridad de la información por dominio de control				X	X		Políticas de seguridad documentadas
6	Estructuración del manual de políticas de seguridad (procedimientos, roles, responsabilidades y mecanismos de revisión)					X		Manual de políticas de seguridad (borrador)

7	Validación técnica del manual, ajustes finales y consolidación del informe de anteproyecto						X	Documento final de anteproyecto

L. DECLARACIÓN FINAL

Los abajo firmantes declaramos bajo juramento que el proyecto descrito en este documento no ha sido presentado a otra institución nacional o internacional para su financiamiento, no causa perjuicio al ambiente, es de nuestra autoría y no transgrede norma ética alguna.

M. PARTICIPANTES

DIRECTOR:	Ing. Cristhian Humberto Flores Urgiles
ESTUDIANTE 1	Emmanuel David Vega Arcentales

N. FIRMAS DE RESPONSABILIDAD

Lugar:	Cañar
Fecha:	28 de abril del 2026

Firmas:

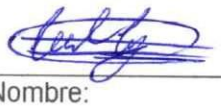


Nombre:

Ing. Cristhian Humberto Flores Urgiles

CC: 0301638375

Director del Proyecto



Nombre:

Emmanuel David Vega Arcentales

C.C.: 0302949011

Estudiante / Egresado

O. APROBACIÓN

Firmas:

Nombre:	Nombre:
CC:	C.C.:
Primer Par Revisor	**Segundo Par Revisor**

P. REFERENCIAS

BIBLIOGRAFÍA

Ali, R. (2026). *Operationalising Information Security Management: A Procedural Framework Analysis of ISO/IEC 27001:2022 Implementation in a Financial-Technology Organisation.* arXiv.

Araujo Castro, G. M. (2019). *Propuesta de un Plan de continuidad del negocio para una entidad pública del Ecuador.* Universidad Técnica de Ambato.

Buscán Pinguil, P. C., Flores Urgilés, C. H., Pinos Castillo, L. F., & Flores Urgilés, C. M. (2022). Modelo de plan de continuidad de negocio de las cooperativas segmento B del cantón Cañar. *Pro Sciences: Revista de Producción, Ciencias e Investigación*.

International Organization for Standardization; International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* Geneva, Switzerland: International Organization for Standardization.

International Organization for Standardization; International Electrotechnical Commission. (2022). *ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls.* Geneva, Switzerland: International Organization for Standardization.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2021). *Esquema Gubernamental de Seguridad de la Información (EGSI), versión 2.0.* Quito, Ecuador: Ministerio de Telecomunicaciones y de la Sociedad de la Información.

NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0.* National Institute of Standards and Technology.

Podrecca, M., Culot, G., Nassimbeni , G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*.

Villarreal Morales, V., Coro Villarreal, K. E., Fernández Sánchez, E. G., & Cueva Martinez, J. P. (2024). Sistema Gestión de Seguridad de la Información y su impacto en el Gobierno y Gestión de las Tecnologías de la Información. *Ciencia Latina Revista Científica Multidisciplinar*.

Anexo 2. Manual de políticas de seguridad de la información del departamento de TI del GADICC

El manual se presenta a continuación como documento independiente, conservando su formato original.

1. Introducción

El Departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado Intercultural (GADICC) del Cantón Cañar administra los sistemas de gestión institucional, las bases de datos ciudadanas, la infraestructura tecnológica y de computación personal, los servicios digitales municipales y los centros de datos municipales. Estos activos incluyen el Sistema Integrado de Desarrollo Municipal (SIM), desarrollado internamente, los gestores de bases de datos institucionales, la red interna municipal, el cortafuegos perimetral y el centro de datos municipal. La información procesada por estos componentes constituye un activo estratégico crucial para la continuidad de los servicios públicos del cantón, el cumplimiento normativo y la confianza de la ciudadanía.

Se determinó un nivel de cumplimiento del 69,8% para 63 controles de la norma ISO/IEC 27002:2022 en el departamento. Este análisis identificó 14 brechas y 5 controles que aún se están implementando. Las brechas se concentran en los dominios de protección física y ambiental (37,5%), organizacional (50%) y de activos (60%). El análisis de la metodología de gestión de riesgos MAGERIT v3 confirmó estas brechas: de los 50 activos evaluados, el valor de 25 se situó generalmente entre 9 y 10. Los riesgos más graves no se centran en los sistemas de información, sino en las condiciones de protección física y organizacional de los mismos.

Este manual aborda dicha situación. Establece la política de seguridad de la información del departamento de TI de GADICC, formalizando las directrices, los procedimientos y las responsabilidades que anteriormente se llevaban a cabo de manera informal y sin documentación. Las políticas se basan en los requisitos de la norma ISO/IEC 27001:2022 y en los controles del Apéndice A de la norma ISO/IEC

27002:2022, y se articulan con la versión 2.0 del Esquema Gubernamental de Seguridad de la Información (EGSI) y la Ley Orgánica de Protección de Datos Personales de Ecuador.

2. Objetivos del manual

2.1. Objetivo general

Establecer las políticas de seguridad de la información del departamento de Tecnologías de la Información del GADICC, basadas en la norma ISO/IEC 27001:2022, orientadas a proteger la confidencialidad, la integridad y la disponibilidad de los activos de información institucionales y a reducir los riesgos determinados en el análisis realizado con la metodología MAGERIT v3.

2.2. Objetivos específicos

- Formalizar los roles, las responsabilidades y los mecanismos de gobernanza de la seguridad de la información dentro de la institución.
- Definir directrices concretas y verificables para el tratamiento de los riesgos calificados como altos y críticos en el análisis de riesgo institucional.
- Establecer los procedimientos de implementación, los responsables y la periodicidad de revisión de cada política, de modo que el manual constituya un instrumento aplicable y auditable.
- Contribuir al cumplimiento de los requisitos legales y regulatorios aplicables al sector público ecuatoriano en materia de seguridad de la información y protección de datos personales.

3. Alcance

El contenido de este manual abarca todos los tipos de activos de información gestionados por los servicios de información y datos del GADICC ICTD, software, equipos de TIC, infraestructura de comunicaciones, soporte de información, equipos auxiliares, contenedores, instalaciones y personal. Este manual se aplica al personal del Departamento de TIC, a los usuarios del sistema institucional en las demás unidades administrativas de la Administración Pública, y a los proveedores de servicios, contratistas y

terceros que acceden a la infraestructura de información o tecnología de la institución. La vinculación de terceros con este manual se regirá por las cláusulas contractuales de la política POL-05.

4. Marco normativo de referencia

Instrumento	Aporte al manual
ISO/IEC 27001:2022	Requisitos del Sistema de Gestión de Seguridad de la Información: contexto, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora.
ISO/IEC 27002:2022	Controles de referencia agrupados en cuatro dominios: organizacional, personas, físico y tecnológico. Constituyen la base de las políticas del capítulo 7.
MAGERIT v3	Metodología aplicada para el inventario, la valoración de activos, la identificación de amenazas y el cálculo del nivel de riesgo que sustenta la priorización de las políticas.
Ley Orgánica de Protección de Datos Personales (LOPDP)	Obligación del sector público de contar con protocolos de seguridad acordes con estándares internacionales para el tratamiento de datos personales de la ciudadanía.
Esquema Gubernamental de Seguridad de la Información (EGSI) v2.0	Estándares mínimos de seguridad de obligatorio cumplimiento para las instituciones públicas ecuatorianas y los gobiernos autónomos descentralizados.
COOTAD y Constitución de la República del Ecuador	Marco de competencias institucionales del GADICC en la prestación de servicios públicos cantonales.

5. Definiciones

Término	Definición
Activo de información	Todo elemento que tiene valor para la institución y que requiere protección: datos, servicios, software, hardware, redes, soportes, instalaciones y personal.
Confidencialidad	Propiedad por la cual la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
Integridad	Propiedad de exactitud y completitud de la información y de los métodos de su procesamiento.
Disponibilidad	Propiedad de la información de ser accesible y utilizable por una entidad autorizada cuando esta lo requiera.
Amenaza	Causa potencial de un incidente no deseado que puede ocasionar daño a un activo de información.
Vulnerabilidad	Debilidad de un activo o de un control que puede ser aprovechada por una amenaza.
Riesgo	Efecto de la incertidumbre sobre los objetivos institucionales; en el presente manual se calcula como el producto del impacto por la probabilidad.
Evento de seguridad	Ocurrencia identificada en un sistema o red que indica una posible brecha de seguridad o una falla de los controles.
Incidente de seguridad	Evento o serie de eventos de seguridad no deseados que tienen una probabilidad significativa de comprometer las operaciones institucionales.
Mínimo privilegio	Principio según el cual a cada usuario se le otorgan únicamente los permisos estrictamente necesarios para cumplir sus funciones.
SGSI	Sistema de Gestión de Seguridad de la Información: conjunto de políticas, procesos y controles orientados a gestionar la seguridad de la información de forma sistemática.

6. Responsabilidad y cumplimiento del manual

La correcta implementación del presente manual constituye una responsabilidad compartida entre distintos niveles de la institución. Para asegurar su eficacia se asignan las siguientes responsabilidades:

Rol	Responsabilidades
Máxima autoridad administrativa	Aprobar formalmente el manual y sus actualizaciones mediante el acto administrativo correspondiente; disponer su difusión obligatoria; asignar los recursos necesarios para la implementación de las políticas; presidir el Comité de Seguridad de la Información.
Comité de Seguridad de la Información	Supervisar la implementación de las políticas; aprobar el cronograma anual de auditorías internas; revisar el manual al menos una vez al año; conocer los incidentes que afecten activos con valor global igual o mayor a 9.
Oficial de Seguridad de la Información	Coordinar la ejecución del manual, dar seguimiento a los planes de acción derivados de auditorías e incidentes y reportar al Comité. Esta designación debe recaer en un profesional distinto de quien administra la plataforma tecnológica, a fin de materializar la segregación de funciones.
Responsable del departamento de TI	Ejecutar y hacer cumplir las políticas; mantener actualizado el inventario y la valoración de los activos; gestionar los incidentes de seguridad; elaborar las propuestas de actualización del manual.
Administradores de sistemas, seguridad, comunicaciones y bases de datos	Aplicar los controles técnicos de las políticas correspondientes a su ámbito; documentar las configuraciones y los cambios ejecutados; reportar de inmediato cualquier evento de seguridad detectado.
Unidad de Talento Humano	Incorporar la inducción de seguridad de la información al proceso de ingreso de personal y apoyar la ejecución del plan anual de capacitación.
Unidad de contratación pública	Incorporar en los contratos las cláusulas de confidencialidad y de seguridad de la información previstas en la política POL-05.
Servidores públicos y usuarios de los sistemas	Cumplir las políticas del manual, utilizar los recursos institucionales conforme a su finalidad y reportar los eventos o sospechas de incidentes de seguridad por el canal establecido.
Auditoría interna	Verificar periódicamente el grado de cumplimiento de las políticas, identificar no conformidades y proponer acciones de mejora.

6.1. Incumplimiento

El incumplimiento de las disposiciones de este manual será reportado a las más altas autoridades administrativas y al Comité de Seguridad de la Información, y dará lugar a la aplicación de sanciones administrativas de conformidad con las normas del Servicio Público del Ecuador y el Reglamento Interno de la Institución, según corresponda, sin perjuicio de la responsabilidad civil o penal que pueda corresponder en este caso.

7. Fundamento: riesgos que atienden las políticas

Las políticas no son prácticas recomendadas genéricas. Cada una está diseñada para abordar un riesgo específico de un activo dentro del departamento de TI. La siguiente tabla resume los riesgos altos y críticos en los que se basa el manual.

Tabla 1. Riesgos prioritarios del departamento de TI del GADICC

Activo	Amenaza (MAGERIT)	Imp.	Prob.	Riesgo	Nivel	Política
ACT-L-02 Cuarto de servidores	[I.7] Condiciones inadecuadas de temperatura o humedad	4	4	16	Crítico	POL-10
ACT-D-01 Base de datos institucional	[A.11] Acceso no autorizado	5	3	15	Alto	POL-03, POL-04
ACT-D-01 Base de datos institucional	[E.19] Fugas de información	5	3	15	Alto	POL-03, POL-13
ACT-D-04 Credenciales de autenticación	[A.5] Suplantación de identidad	5	3	15	Alto	POL-04, POL-12
ACT-D-06 Registros de actividad	[E.3] Errores de monitorización	5	3	15	Alto	POL-06, POL-13
ACT-L-02 Cuarto de servidores	[N.1] Fuego	5	3	15	Alto	POL-09, POL-10
ACT-S-02 Sistema Integrado Municipal	[A.24] Denegación de servicio	4	3	12	Alto	POL-14

ACT-S-07 Certificados digitales (PKI)	[A.6] Abuso de privilegios de acceso	4	3	12	Alto	POL-04, POL-12
ACT-AUX-01 UPS / SAI	[I.6] Corte del suministro eléctrico	4	3	12	Alto	POL-10
ACT-P-01 Administrador de sistemas	[E.28] Indisponibilidad del personal clave	4	3	12	Alto	POL-02
ACT-S-04 Acceso remoto VPN	[A.14] Interceptación de información	4	2	8	Medio	POL-12
ACT-HW-06 Firewall Sophos	[A.24] Denegación de servicio	4	2	8	Medio	POL-14

Nota: Imp. = impacto; Prob. = probabilidad. El riesgo se calcula como impacto × probabilidad, en una escala de 1 a 25 (1-4 bajo; 5-9 medio; 10-15 alto; 16-25 crítico). Fuente: análisis MAGERIT v3 aplicado al departamento de TI del GADICC.

8. Políticas de seguridad de la información

El manual se compone de catorce políticas que abarcan los cuatro aspectos del dominio de la norma ISO/IEC 27002:2022 integrada. Cada política describe el control asignado, el objetivo y el alcance del control, el diseño requerido, cómo debe procesarse y ejecutarse oficialmente, la asignación y el período de revisión requerido.

8.1. Políticas del dominio organizacional

La política de este dominio describe la gobernanza de la seguridad de la información, el marco de trabajo, la asignación de funciones, la clasificación de la información, la gestión del acceso, la relación con terceros, la gestión de incidentes y la mejora continua del manual.

POL-01. Política general de seguridad de la información

Controles ISO/IEC 27002:2022 asociados: 5.1 Políticas de seguridad de la información

Objetivo: Establecer el compromiso formal del GADICC con la seguridad de la información y el marco general que rige su gestión dentro del departamento de Tecnologías de la Información.

Alcance: Todo el personal, los activos de información y los sistemas administrados por el departamento de TI del GADICC, conforme al inventario de cincuenta activos levantado con MAGERIT v3.

Directrices:

- El máximo órgano administrativo de GADICC aprobará formalmente este manual y todas las versiones posteriores.
- El manual se distribuirá al personal del Departamento de Informática y a las áreas de usuarios de los sistemas institucionales.
- El documento se revisará al menos una vez al año o cuando se produzcan cambios significativos en la infraestructura tecnológica, la legislación aplicable o el nivel de riesgo institucional.

Procedimiento de implementación:

1. Elaborar el borrador del manual y presentarlo a la máxima autoridad administrativa o al Comité de Seguridad de la Información, una vez constituido para su revisión.
2. Obtener la aprobación formal mediante resolución o memorando institucional.
3. Publicar y distribuir el manual aprobado a todo el personal del departamento de TI y a las áreas usuarias, mediante correo institucional y una sesión informativa inicial.
4. Registrar la fecha de aprobación y programar la siguiente revisión en el calendario institucional.

Responsable: Máxima autoridad administrativa (aprobación); responsable de TI (elaboración y difusión).

Periodicidad de revisión: Anual.

POL-02. Roles, responsabilidades y Comité de Seguridad de la Información

Controles ISO/IEC 27002:2022 asociados: 5.2 Roles y responsabilidades de seguridad de la información · 5.35 Revisión independiente de la seguridad de la información

Objetivo: Formalizar las responsabilidades de seguridad y establecer un mecanismo de supervisión independiente, dado que las funciones de administración de sistemas, seguridad y comunicaciones se concentran actualmente en un número reducido de personal (activo ACT-P-01).

Alcance: La estructura organizativa del GADICC vinculada a la gestión de la seguridad de la información.

Directrices:

- Se creará un comité de seguridad de la información. Lo integrarán el ejecutivo de mayor rango, el responsable de TI y un representante administrativo. El comité se reunirá al menos una vez cada seis meses.
- Las funciones de administrador de sistemas, administrador de seguridad, administrador de comunicaciones y administrador de bases de datos se documentarán y asignarán formalmente.
- Personal independiente realizará auditorías internas al menos una vez al año, las cuales no operarán los sistemas que se estén evaluando.

Procedimiento de implementación:

1. Designar formalmente, mediante memorando de la máxima autoridad, a los integrantes del Comité de Seguridad de la Información.
2. Notificar por escrito a cada funcionario del departamento de TI el rol de seguridad que le corresponde.

3. Convocar y realizar la primera sesión del comité para aprobar el cronograma anual de auditorías internas.
4. Designar al personal, interno o externo al área de TI, que ejecutará la primera auditoría independiente.

Responsable: Comité de Seguridad de la Información.

Periodicidad de revisión: Semestral.

POL-03. Clasificación y etiquetado de la información

Controles ISO/IEC 27002:2022 asociados: 5.12 Clasificación de la información · 5.13 Etiquetado de la información

Objetivo: Establecer niveles de clasificación de la información institucional para proteger los activos de mayor criticidad (ACT-D-01, ACT-D-04 y ACT-D-06, entre los activos con valor global de 9 a 10).

Alcance: Toda la información gestionada por el departamento de TI, en formato físico y digital.

Directrices:

- La información se clasificará en los niveles Público, Interno, Confidencial y Crítico, según el impacto que pueda tener una divulgación no autorizada.
- Cualquier activo de información con un valor global (VG) de 9 o superior se clasificará como mínimo como confidencial.
- Los documentos y las bases de datos se marcarán, ya sea física o digitalmente, indicando su nivel de clasificación y el propietario de dicha clasificación.

Procedimiento de implementación:

1. Elaborar una guía de clasificación con los cuatro niveles definidos y ejemplos basados en los activos del inventario.

2. Revisar la valoración de cada activo y asignarle el nivel de clasificación correspondiente.
3. Etiquetar los activos digitales y físicos conforme a la clasificación asignada.
4. Notificar al responsable de cada activo su nivel de clasificación y las restricciones de manejo aplicables.

Responsable: Responsable de TI, en coordinación con el propietario de cada activo.

Periodicidad de revisión: Anual, o al incorporarse nuevos activos al inventario.

POL-04. Gestión de accesos y derechos de acceso

Controles ISO/IEC 27002:2022 asociados: 5.18 Derechos de acceso · 8.5 Autenticación segura

Objetivo: Garantizar que el acceso a los sistemas y a la información institucional se otorgue únicamente al personal autorizado y de acuerdo con las funciones que desempeña.

Alcance: El Sistema Integrado Municipal (SIM), los gestores de base de datos, la infraestructura de certificados digitales y los demás activos de tipo software y servicios del inventario.

Directrices:

- Derechos de acceso se otorgarán a continuación conforme a principio de mínimo privilegio y se revisarán una vez por semestre mínimo.
- Certificados electrónicos (ACT-S-07) y credenciales de autenticación (ACT-D-04) se administrarán según un procedimiento formulado de emisión, renovación y rescisión.
- El acceso remoto se permitirá únicamente a través de la VPN institucional (ACT-S-04), con autenticación multifactor para los cargos administrativos.

Procedimiento de implementación:

1. Levantar un inventario de usuarios y perfiles de acceso vigentes en el SIM, los gestores de base de datos y la VPN.

2. Ajustar los permisos existentes al principio de mínimo privilegio, retirando los accesos innecesarios.
3. Habilitar la autenticación multifactor para los roles administrativos y el acceso remoto.
4. Programar y ejecutar la revisión semestral de los derechos de acceso otorgados.

Responsable: Administrador de seguridad.

Periodicidad de revisión: Semestral.

POL-05. Relaciones con proveedores y terceros

Controles ISO/IEC 27002:2022 asociados: 5.19 Seguridad de la información en las relaciones con proveedores · 5.20 Requisitos de seguridad en los acuerdos · 5.21 Gestión de la seguridad en la cadena de suministro de TIC · 5.22 Seguimiento y gestión de cambios de los servicios de proveedores

Objetivo: Formalizar los requisitos de seguridad de la información en los contratos con proveedores de tecnología y servicios externos, incluidos los servicios de pago e intercambio de información (ACT-S-06).

Alcance: Todo proveedor o tercero con acceso a los sistemas o a la información del GADICC.

Directrices:

- Todo contrato con proveedores de TI incluirá cláusulas de confidencialidad y de cumplimiento de controles mínimos de seguridad.
- Se mantendrá un registro de proveedores con acceso a los sistemas institucionales y el alcance de dicho acceso.
- Se evaluará periódicamente el cumplimiento de los proveedores críticos, en particular los de alojamiento y los de pagos e intercambio de información.

Procedimiento de implementación:

1. Identificar a todos los proveedores actuales con acceso a sistemas o información del GADICC (alojamiento, pagos, soporte técnico).
2. Incorporar cláusulas de confidencialidad y de seguridad de la información en los contratos vigentes y en los futuros.
3. Elaborar y mantener actualizado el registro de proveedores con el alcance de su acceso.
4. Programar la evaluación anual del cumplimiento de seguridad de los proveedores críticos.

Responsable: Responsable de TI, en coordinación con la unidad de contratación pública.

Periodicidad de revisión: Anual, o al renovar contratos.

POL-06. Gestión de incidentes y evaluación de eventos de seguridad

Controles ISO/IEC 27002:2022 asociados: 5.25 Evaluación y decisión sobre eventos de seguridad de la información · 8.16 Actividades de monitoreo

Objetivo: Establecer un procedimiento formal para la identificación, evaluación y reporte de eventos e incidentes de seguridad, subsanando la brecha detectada en el diagnóstico institucional respecto de la valoración de eventos de seguridad.

Alcance: Todos los sistemas y registros de actividad del departamento de TI (ACT-D-06).

Directrices:

- Todos los eventos de seguridad detectados en los registros serán evaluados en un plazo de 24 horas para determinar si constituyen un incidente.
- Los incidentes de diversa gravedad se comunicarán a la máxima autoridad administrativa cuando afecten a activos con un valor global de 9 dólares o más.
- Se conservará un registro de los incidentes y de las medidas correctivas adoptada

Procedimiento de implementación:

1. Documentar el procedimiento de reporte, clasificación y escalamiento de incidentes.

2. Habilitar un canal de reporte accesible para todo el personal (correo institucional o formulario interno).
3. Capacitar al personal de TI en la evaluación de eventos dentro del plazo de veinticuatro horas establecido.
4. Implementar la bitácora de incidentes y de las acciones correctivas aplicadas.

Responsable: Responsable de TI.

Periodicidad de revisión: Continua; el procedimiento se revisará anualmente.

POL-07. Revisión y mejora continua del manual

Controles ISO/IEC 27002:2022 asociados: 5.35 Revisión independiente de la seguridad de la información · Cláusula 10 de la norma ISO/IEC 27001:2022 (mejora)

Objetivo: Asegurar que el manual y sus políticas se mantengan vigentes y efectivos frente a cambios tecnológicos, regulatorios u organizacionales.

Alcance: El conjunto de políticas que integran el presente manual.

Directrices:

- El manual se revisará formalmente al menos una vez al año por el Comité de Seguridad de la Información.
- Toda auditoría interna o externa que identifique no conformidades generará un plan de acción con responsables y plazos definidos.
- Las actualizaciones del manual se documentarán con control de versiones y se comunicarán al personal afectado.

Procedimiento de implementación:

1. Incluir en el cronograma anual del Comité de Seguridad una sesión dedicada a la revisión del manual.

2. Recopilar los hallazgos de auditorías internas o externas y los incidentes registrados durante el periodo.
3. Actualizar las políticas afectadas y documentar los cambios con número de versión y fecha.
4. Comunicar las actualizaciones al personal correspondiente.

Responsable: Comité de Seguridad de la Información.

Periodicidad de revisión: Anual.

8.2. Políticas del dominio de personas

Este dominio aborda el factor humano de la seguridad de la información: la concienciación del personal, su formación y los mecanismos de reporte de eventos.

POL-08. Concienciación, formación y reporte de eventos de seguridad

Controles ISO/IEC 27002:2022 asociados: 6.8 Reporte de eventos de seguridad de la información (relacionado con 6.3 Concienciación, educación y capacitación)

Objetivo: Fortalecer el conocimiento del personal técnico y administrativo sobre sus responsabilidades de seguridad y sobre los procedimientos de reporte de incidentes, atendiendo la brecha detectada en el diagnóstico institucional.

Alcance: Todo el personal del departamento de TI y los usuarios internos (ACT-P-05) de los sistemas institucionales.

Directrices:

- Todo el personal del departamento de informática deberá completar una formación anual en seguridad de la información.
- Se pondrán a disposición de todo el personal procedimientos de notificación sencillos y conocidos para incidentes y/o incidentes sospechosos.
- El personal de nuevo ingreso recibirá una formación inicial sobre seguridad de la información antes de acceder a los sistemas de la institución.

Procedimiento de implementación:

1. Diseñar el contenido de la capacitación anual: políticas del manual, clasificación de la información y reporte de incidentes.
2. Programar la capacitación obligatoria para todo el personal de TI y los usuarios clave de los sistemas institucionales.

3. Incorporar la inducción de seguridad de la información al proceso de ingreso de personal nuevo.
4. Evaluar la comprensión del personal mediante una prueba corta o encuesta posterior a la capacitación.

Responsable: Responsable de TI, en coordinación con la Unidad de Talento Humano.

Periodicidad de revisión: Anual.

8.3. Políticas del dominio físico

Este dominio concentra las medidas de protección del centro de datos y de la infraestructura física que soporta al resto del inventario de activos. Corresponde al dominio con el nivel de cumplimiento más bajo del diagnóstico institucional, por lo que sus políticas se consideran de implementación prioritaria.

POL-09. Seguridad física del centro de datos

Controles ISO/IEC 27002:2022 asociados: 7.2 Entrada física · 7.3 Seguridad de oficinas, salas e instalaciones · 7.8 Emplazamiento y protección de equipos

Objetivo: Proteger el cuarto de servidores (ACT-L-02) y los equipos críticos (ACT-HW-01 y ACT-HW-02) frente a accesos no autorizados, subsanando la brecha identificada como la más crítica del diagnóstico institucional: 37,5 % de cumplimiento en el dominio de seguridad física y ambiental.

Alcance: Las instalaciones físicas del centro de datos municipal.

Directrices:

- El acceso al cuarto de servidores se restringirá mediante un mecanismo de control llave, tarjeta o registro de acceso y se limitará al personal autorizado de TI.
- Se mantendrá un registro de ingresos de personal propio y de terceros al centro de datos.

- Los equipos de red y los servidores se ubicarán en racks cerrados (ACT-L-03), fuera del alcance de personal no autorizado.

Procedimiento de implementación:

1. Instalar un mecanismo de control de acceso en la puerta del cuarto de servidores.
2. Implementar y mantener el registro de ingresos de personal propio y visitantes.
3. Asegurar en racks cerrados los equipos que actualmente no cuenten con esta protección.
4. Realizar una inspección trimestral del cumplimiento de estos controles.

Responsable: Responsable de TI.

Periodicidad de revisión: Anual.

POL-10. Protección ambiental y continuidad eléctrica

Controles ISO/IEC 27002:2022 asociados: 7.5 Protección contra amenazas físicas y ambientales · 7.11 Instalaciones de suministro

Objetivo: Reducir el riesgo crítico identificado en la matriz de riesgo condiciones inadecuadas de temperatura o humedad, con nivel de riesgo 16 y garantizar la continuidad eléctrica del centro de datos (ACT-AUX-01 y ACT-AUX-02).

Alcance: El cuarto de servidores y los sistemas de respaldo eléctrico del GADICC.

Directrices:

- Se instalará y mantendrá un sistema de climatización adecuado en el cuarto de servidores, con monitoreo de temperatura y humedad.
- El UPS y el generador eléctrico se someterán a mantenimiento preventivo periódico y a pruebas de autonomía.
- Se instalarán detectores de humo o sistemas de mitigación de incendios acordes con el riesgo identificado por la amenaza [N.1] Fuego.

Procedimiento de implementación:

1. Evaluar el estado actual del sistema de climatización e instalar o ajustar el equipo necesario.
2. Programar el mantenimiento preventivo periódico del UPS y del generador, incluyendo pruebas de autonomía.
3. Instalar detectores de humo u otro sistema de mitigación de incendios apropiado para equipamiento eléctrico en el cuarto de servidores.
4. Documentar los resultados de cada mantenimiento y prueba realizada.

Responsable: Responsable de TI, en coordinación con el área administrativa.

Periodicidad de revisión: Semestral.

POL-11. Seguridad del cableado estructurado

Controles ISO/IEC 27002:2022 asociados: 7.12 Seguridad del cableado

Objetivo: Proteger el cableado estructurado (ACT-AUX-04) y el backbone de fibra óptica (ACT-AUX-03) frente a daños físicos o interceptación.

Alcance: La infraestructura de cableado de la red institucional.

Directrices:

- El cableado se instalará en conductos protegidos y se mantendrá alejado de fuentes de interferencia electromagnética.
- Se documentará el trazado del teleférico y se etiquetarán los puntos de la red.
- Todas las intervenciones en el teleférico serán registradas y comunicadas por el responsable de comunicaciones.

Procedimiento de implementación:

1. Elaborar el mapa actualizado del cableado estructurado y del backbone de fibra óptica.
2. Verificar y corregir los tramos expuestos a interferencia electromagnética o daño físico.

3. Etiquetar los puntos de red conforme al mapa elaborado.
4. Establecer que toda intervención futura sobre el cableado quede registrada y autorizada por el administrador de comunicaciones.

Responsable: Administrador de comunicaciones.

Periodicidad de revisión: Anual.

8.4. Políticas del dominio tecnológico

Este dominio agrupa los controles técnicos aplicables a la autenticación, la criptografía, el monitoreo de la actividad y la protección de la red institucional.

POL-12. Uso de criptografía y autenticación segura

Controles ISO/IEC 27002:2022 asociados: 8.5 Autenticación segura · 8.24 Uso de criptografía

Objetivo: Proteger la confidencialidad de las credenciales (ACT-D-04), el acceso remoto (ACT-S-04) y los certificados digitales (ACT-S-07), subsanando la brecha de uso de controles criptográficos detectada en el diagnóstico institucional.

Alcance: Los sistemas de autenticación, acceso remoto y firma electrónica del GADICC.

Directrices:

- Las contraseñas y credenciales se almacenarán cifradas, y se aplicará autenticación multifactor para los accesos administrativos y remotos.
- La VPN institucional utilizará protocolos de cifrado vigentes y se auditará periódicamente su configuración.
- Los certificados digitales se renovarán antes de su vencimiento y se revocarán de inmediato ante cualquier sospecha de compromiso.

Procedimiento de implementación:

1. Configurar el cifrado de las credenciales almacenadas y de las conexiones VPN conforme a protocolos vigentes.
2. Habilitar la autenticación multifactor para los accesos administrativos y remotos.
3. Establecer el procedimiento de emisión, renovación y revocación de los certificados digitales.
4. Auditar semestralmente la configuración criptográfica de los sistemas críticos.

Responsable: Administrador de seguridad.

Periodicidad de revisión: Semestral.

POL-13. Monitoreo de actividad y gestión de registros

Controles ISO/IEC 27002:2022 asociados: 8.16 Actividades de monitoreo (relacionado con 8.15 Registro de eventos)

Objetivo: Garantizar la trazabilidad de las acciones ejecutadas sobre los sistemas institucionales mediante el monitoreo de los registros de actividad (ACT-D-06), atendiendo el riesgo de errores de monitorización identificado en la matriz de riesgo.

Alcance: Los servidores, aplicaciones y equipos de red del departamento de TI.

Directrices:

- Se realizarán revisiones periódicas de los registros de los sistemas críticos. Estos registros se conservarán durante el tiempo que determine la institución.
- Se registrarán los eventos inusuales en los sistemas con un mayor nivel de criticidad: SIM, base de datos institucional y cortafuegos perimetral.
- Es necesario restringir el acceso para preservar los registros como prueba.

Procedimiento de implementación:

1. Configurar la generación y el almacenamiento centralizado de los registros de los sistemas críticos.
2. Definir el periodo mínimo de conservación de los registros conforme a las necesidades institucionales.
3. Configurar alertas automáticas para eventos anómalos en el SIM, la base de datos institucional y el firewall.
4. Restringir el acceso a los registros de actividad al personal autorizado.

Responsable: Responsable de TI.

Periodicidad de revisión: Semestral.

POL-14. Seguridad de las redes y protección perimetral

Controles ISO/IEC 27002:2022 asociados: 8.7 Protección contra código malicioso · 8.20 Seguridad de las redes

Objetivo: Proteger la red institucional (ACT-COM-01) y el firewall perimetral (ACT-HW-06) frente a accesos no autorizados y software malicioso.

Alcance: La red interna, la conexión a Internet y los sistemas de protección perimetral del GADICC.

Directrices:

- La segmentación de la red institucional se mantendrá en VLANs en función de la criticidad de cada área o sistema.
- Las reglas del perímetro del cortafuegos se revisarán y actualizarán periódicamente, y los cambios realizados quedarán documentados.
- El software antivirus (ACT-SW-08) se actualizará en todos los dispositivos y servidores, y se realizarán comprobaciones periódicas de la cobertura de actualizaciones.

Procedimiento de implementación:

1. Revisar y documentar la segmentación actual de las VLAN institucionales.
2. Actualizar las reglas del firewall perimetral conforme a los riesgos identificados en la matriz de riesgo.
3. Verificar que el antivirus institucional esté actualizado en todos los servidores y equipos.
4. Programar revisiones semestrales de la configuración de red y del firewall.

Responsable: Administrador de comunicaciones y administrador de seguridad.

Periodicidad de revisión: Semestral.

9. Vigencia, difusión y revisión

Este manual entrará en vigor una vez aprobado por el responsable administrativo del GADICC. Hasta entonces, no será necesario que los empleados ni terceros, según se definen en el Capítulo 3, cumplan con el manual.

El departamento de tecnología de la información notificará a todos los empleados sobre el nuevo manual por correo electrónico y realizará una reunión informativa inicial. Se conservará un registro de la notificación para todos los empleados. El Comité de Seguridad de la Información revisará la política anualmente o cuando cambien los requisitos relacionados con la infraestructura, las leyes aplicables o el nivel de riesgo institucional, según se define en la política POL-07.

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Emmanuel David Vega Arcentales portador de la cédula de ciudadanía N.° **0302949011**. En calidad de autor y titular de los derechos patrimoniales del proyecto de investigación "**Diseño de un manual de políticas de seguridad de la información para el departamento de TI del GADICC, basado en la norma ISO/IEC 27001:2022**" de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de este trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cañar, 29 de septiembre 2026

Emmanuel David Vega Arcentales

C.I. 0302949011