

UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA LA EMPRESA EMMAIPC-EP

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

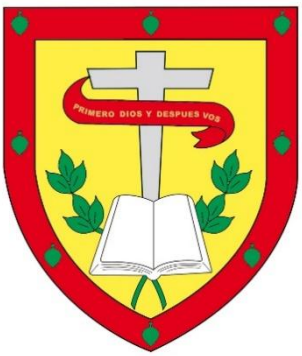
AUTOR: KEVIN ALEXANDER CANTOS ESPINOZA

DIRECTOR: ING. DANNY PATRICIO ANDRADE CÁRDENAS

CAÑAR-ECUADOR

2026

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDADCATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA LA EMPRESA EMMAIPC-EP

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

AUTOR: KEVIN ALEXANDER CANTOS ESPINOZA

DIRECTOR: ING. DANNY PATRICIO ANDRADE CARDENAS

CAÑAR- ECUADOR

2026

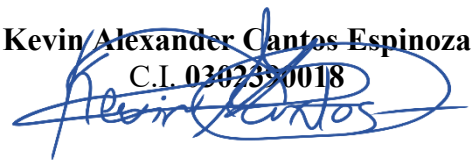
DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Kevin Alexander Cantos Espinoza portador de la cédula de ciudadanía Nº **0302390018** Declaro ser el autor de la obra: **"Diseño de un Sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la empresa EMMAIPC-EP",** sobre la cual me hago responsable sobre 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, 30 **de septiembre de 2026**

Kevin Alexander Cantos Espinoza
C.I. **0302390018**



Universidad Católica de Cuenca	CERTIFICADO DEL TUTOR

CERTIFICADO DEL TUTOR

Certifico que el presente trabajo denominado **Diseño de un Sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la empresa EMMAIPC-EP "** realizado por **Kevin Alexander Cantos Espinoza,** con documento de identidad No. **0302390018**, 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, 30 **de septiembre de 2026**

Ing. Danny Patricio Andrade Cárdenas
DIRECTOR DEL TRABAJO INVESTIGATIVO
UNIVERSIDAD CATÓLICA DE CUENCA EXTENSIÓN CAÑAR

DEDICATORIA

A mi abuelita, **Zoila Rodríguez Clavijo**, por ser el pilar de nuestra familia y la raíz de todo lo que soy; por sus oraciones, sus consejos y el amor con el que me ha acompañado desde mis primeros pasos.

A mi madre, **Julia Dolores Espinoza Rodríguez**, por su esfuerzo incansable, su fortaleza y su confianza en mí; porque cada uno de mis logros lleva su nombre y es el fruto de sus sacrificios y de su ejemplo de perseverancia.

A toda mi familia, por su apoyo constante, su paciencia y su aliento en los momentos difíciles; porque este trabajo, más que mío, es de todos ustedes.

Kevin Alexander Cantos Espinosa

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. Danny Patricio Andrade Cárdenas, 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

La Empresa Pública Municipal Mancomunada de Aseo Integral de los cantones Cañar, Biblián, El Tambo y Suscal (EMMAIPC-EP) gestiona información administrativa, operativa y financiera sin un marco formal de seguridad que proteja la confidencialidad, la integridad y la disponibilidad de sus activos. El objetivo de esta investigación fue diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 para la institución. Se aplicó un enfoque mixto, de nivel descriptivo con alcance propositivo, y la metodología de gestión de riesgos ISO/IEC 27005:2022. El diagnóstico identificó 91 activos tecnológicos, de los cuales el 59,3 % superó su vida útil, un nivel de madurez de 1,5 sobre 5 y 16 riesgos, cinco de nivel muy alto y ocho de nivel alto; el hallazgo más severo corresponde al sistema de facturación y recaudación alojado en la nube bajo una cuenta administrativa del proveedor. La propuesta comprende un inventario valorado de 21 activos de información, un plan de tratamiento de riesgos, una Declaración de Aplicabilidad con 86 controles aplicables del Anexo A, una política general, ocho políticas específicas, siete roles, diez indicadores y un modelo de implementación de doce meses bajo el ciclo PHVA. La validación evidenció una cobertura riesgo-control del 100 % y que 14 de los 16 riesgos alcanzan un nivel residual aceptable. Se concluye que las principales brechas son organizativas antes que tecnológicas y que la norma es aplicable a una empresa pública pequeña cuando el diseño se adapta a su estructura real.

Palabras clave: seguridad de la información, SGSI, ISO/IEC 27001:2022, gestión de riesgos, sector público

ABSTRACT

The Cañar Canton Municipal Public Enterprise for Comprehensive Sanitation (EMMAIPC-EP) manages administrative, operational, and financial information without a formal security framework to protect the confidentiality, integrity, and availability of its assets. This research aimed to design an Information Security Management System (ISMS) for the institution based on the ISO/IEC 27001:2022 standard. A mixed approach was applied, with a descriptive level and a proposal-oriented scope, along with the ISO/IEC 27005:2022 risk management methodology. The assessment identified 91 technological assets, of which 59.3% had exceeded their useful life, with a maturity level of 1.5 out of 5, and 16 risks, five of them at a very high level and eight at a high level; the most serious finding relates to the cloud-based billing and collection system hosted under the provider's administrative account. The proposal includes a valued inventory of 21 information assets, a risk treatment plan, a Statement of Applicability with 86 applicable controls from Annex A, a general policy, eight specific policies, seven roles, ten indicators, and twelve-month implementation model based on the PDCA cycle. The validation revealed 100% risk-control coverage and showed that 14 of the 16 risks reached an acceptable residual risk level. It was concluded that the main gaps are organizational rather than technological and that the standard is applicable to a small public enterprise when the design is adapted to its actual structure.

Keywords: information security, ISMS, ISO/IEC 27001:2022, risk management, public sector.

ÍNDICE

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD 3

CERTIFICADO DEL TUTOR 4

CERTIFICADO DEL TUTOR 4

DEDICATORIA 5

AGRADECIMIENTO 6

Resumen 7

ÍNDICE 9

ÍNDICE DE TABLAS 15

ÍNDICE DE FIGURAS 16

Introducción 17

CAPÍTULO I 18

1.1 Planteamiento del problema 18

1.1.1 Formulación del problema 19

1.2 Antecedentes de la Investigación 19

1.3 Justificación de la investigación 21

1.4 Objetivos 22

1.4.1 Objetivo General 22

1.4.2 Objetivo Específico 22

1.5 Limitaciones 23

1.6 Delimitaciones 24

CAPÍTULO II 25

2 MARCO TEÓRICO 25

2.1 Seguridad de la información 25

2.1.1 Concepto de seguridad de la información 25

2.1.2 Importancia de la seguridad de la información en las organizaciones 25

2.1.3 Principios fundamentales de seguridad de la información 25

2.2 Activos de información 26

2.2.1 Concepto de activo de información 26

2.2.2 Clasificación de activos de información 27

2.2.3 Identificación y valoración de activos de información 28

2.3 Gestión de riesgos de seguridad de la información 28

2.3.1 Concepto de riesgo de seguridad de la información 28

2.3.2 Amenazas y vulnerabilidades 28

2.3.3 Análisis y evaluación de riesgos 29

2.3.4 Tratamiento de riesgos 30

2.4 Sistema de Gestión de Seguridad de la Información (SGSI) 31

2.4.1 Concepto de SGSI 31

2.4.2 Objetivos y beneficios del SGSI 31

2.4.3 Componentes de un SGSI 32

2.4.4 Ciclo PHVA aplicado a la seguridad de la información 32

2.5 Norma ISO/IEC 27001:2022 33

2.6 Metodologías 33

2.6.1 Metodología ISO/IEC 27005:2022 34

2.6.2 Metodología MAGERIT 34

2.6.3 Metodología OCTAVE 34

2.7 Marco normativo ecuatoriano para la seguridad de la información 36

2.7.1 Ley Orgánica de Protección de Datos Personales 36

2.7.2 Esquema Gubernamental de Seguridad de la Información 37

2.7.3 Implicaciones para el diseño del SGSI de la EMMAIPC-EP..... 38

CAPÍTULO III 38

3 MARCO METODOLÓGICO 38

3.1 Enfoque de la investigación 39

3.2 Nivel de la investigación..... 39

3.3 Población y muestra..... 39

3.4 Técnicas e instrumentos de recolección de información 40

3.5 Tratamiento de la información..... 42

3.6 Selección de la metodología para la gestión de riesgos..... 43

3.7 Fases para el diseño del SGSI basado en la norma ISO/IEC 27001:2022..... 44

3.8 Contexto organizacional de la EMMAIPC-EP 45

3.8.1 Caracterización institucional 45

3.8.2 Estructura y capacidad de la Unidad de Tecnologías de la Información y Comunicación..... 46

3.9 Diagnóstico de la situación actual de la seguridad de la información 46

3.9.1 Inventario y estado de los activos tecnológicos 47

3.9.2 Infraestructura de servidor, red y almacenamiento 48

3.9.3 Portafolio de aplicaciones y servicios en la nube 50

3.9.4 Arquitectura de datos y asignación de responsabilidades 51

3.9.5 Respaldos y continuidad 52

3.9.6 Nivel de madurez de la seguridad de la información 53

3.10 Indicadores de línea base 55

3.11 Análisis e interpretación de los resultados 55

3.12 Implicaciones para el diseño del Sistema de Gestión de Seguridad de la Información 57

CAPÍTULO IV 59

4 PROPUESTA 59

4.1 Título de la propuesta 59

4.2 Presentación 59

4.3 Objetivo de la propuesta 59

4.4 Justificación de la propuesta 60

4.5 Fase 1: Contexto, partes interesadas y alcance del SGSI 61

4.5.1 Contexto interno y externo 61

4.5.2 Partes interesadas y requisitos 61

4.5.3 Declaración de alcance del SGSI 62

4.6 Fase 2: Inventario valorado de activos de información 63

4.6.1 Escala de valoración 63

4.6.2 Inventario valorado 63

4.7 Fase 3: Análisis y evaluación de riesgos 65

4.7.1 Criterios de probabilidad, impacto y aceptación 65

4.7.2 Matriz de identificación y evaluación de riesgos 66

4.7.3 Resultados de la evaluación 67

4.8 Fase 4: Tratamiento de riesgos y selección de controles 68

4.8.1 Opciones de tratamiento aplicadas 68

4.8.2 Plan de tratamiento de riesgos 68

4.8.3 Declaración de Aplicabilidad 70

4.9 Fase 5: Políticas y modelo de implementación 71

4.9.1 Política general de seguridad de la información 71

4.9.2 Políticas específicas del SGSI 72

4.9.3 Roles y responsabilidades 73

4.9.4 Modelo de implementación bajo el ciclo PHVA 74

4.9.5 Cronograma de implementación 74

4.9.6 Recursos requeridos 75

4.9.7 Indicadores de desempeño 76

4.10 Validación de la propuesta 77

4.10.1 Verificación de la cobertura riesgo–control 77

4.10.2 Verificación del cumplimiento de los requisitos de la norma 77

4.11 Resultados de la propuesta 78

CONCLUSIONES 81

RECOMENDACIONES 83

Bibliografía 83

Registro de firmas 114

Historial de modificaciones 114

Identificación del documento 114

Índice 116

1. OBJETO 117

2. ALCANCE 117

3. MARCO LEGAL Y NORMATIVO 117

4. DEFINICIONES 118

5. ROLES Y RESPONSABILIDADES 119

6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN 120

7. POLÍTICAS ESPECÍFICAS 121

POL-01. Gestión de activos de información 121

POL-02. Control de acceso 122

POL-03. Respaldo y recuperación de la información 123

POL-04. Seguridad de redes y comunicaciones 123

POL-05. Relación con proveedores y servicios en la nube 124

POL-06. Gestión de incidentes de seguridad de la información 125

POL-07. Seguridad del personal 126

POL-08. Protección de datos personales 127

8. CUMPLIMIENTO, EXCEPCIONES Y RÉGIMEN DISCIPLINARIO 129

9. SEGUIMIENTO Y MEDICIÓN 129

10. VIGENCIA, REVISIÓN Y ACTUALIZACIÓN 130

ANEXO. MATRIZ DE TRAZABILIDAD POLÍTICA – RIESGO – CONTROL 131

ÍNDICE DE TABLAS

Tabla 1. Clasificación de activos de información 26
Tabla 2. Ejemplos de amenazas y vulnerabilidades frecuentes 28
Tabla 3. Objetivos y Beneficios del SGSI 31
Tabla 4. Fases PHVA aplicado al SGSI 32
Tabla 5. Fases del diseño de un SGSI basado en ISO/IEC 27001:2022 33
Tabla 6. Fuentes documentales institucionales utilizadas 38
Tabla 7. Técnicas e instrumentos de recolección de información 39
Tabla 8. Criterios de confiabilidad aplicados a la información 40
Tabla 9. Matriz de selección de la metodología de gestión de riesgos 41
Tabla 10. Fases metodológicas para el diseño del SGSI 43
Tabla 11. Composición del inventario tecnológico por categoría 45
Tabla 12. Estado de conservación y vida útil de los activos tecnológicos 46
Tabla 13. Estado de los equipos de usuario final 46
Tabla 14. Características del servidor institucional 47
Tabla 15. Infraestructura de red y comunicaciones identificada 48
Tabla 16. Portafolio de aplicaciones y sistemas de información 49
Tabla 17. Servicios en la nube y riesgo asociado 50
Tabla 18. Fuentes de información institucional y criticidad 51
Tabla 19. Estado de los mecanismos de respaldo y recuperación 52
Tabla 20. Escala de valoración de madurez aplicada 52
Tabla 21. Valoración preliminar de madurez por dominio 53
Tabla 22. Indicadores de línea base de la seguridad de la información 54
Tabla 23. Brechas identificadas frente a los temas de controles de la ISO/IEC 27002:2022 56
Tabla 24. Partes interesadas y requisitos de seguridad de la información 62
Tabla 25. Alcance del Sistema de Gestión de Seguridad de la Información 63
Tabla 26. Escala de valoración de activos de información 63
Tabla 27. Inventario valorado de activos de información 64
Tabla 28. Escalas de probabilidad e impacto 66
Tabla 29. Matriz de nivel de riesgo 66

Tabla 30. Matriz de identificación y evaluación de riesgos 67
Tabla 31. Distribución de los riesgos identificados por nivel 68
Tabla 32. Plan de tratamiento de riesgos y controles seleccionados 69
Tabla 33. Resumen de la Declaración de Aplicabilidad por tema de controles 71
Tabla 34. Controles excluidos de la Declaración de Aplicabilidad..... 71
Tabla 35. Políticas específicas del Sistema de Gestión de Seguridad de la Información73
Tabla 36. Estructura de roles y responsabilidades del SGSI 74
Tabla 37. Modelo de implementación del SGSI bajo el ciclo PHVA 75
Tabla 38. Cronograma propuesto de implementación..... 75
Tabla 39. Recursos requeridos para la implementación 76
Tabla 40. Indicadores de desempeño del SGSI 77
Tabla 41. Verificación del cumplimiento de los requisitos de la norma 78
Tabla 42. Comparación entre la línea base y la situación esperada 80

ÍNDICE DE FIGURAS

Figura 1. Principios fundamentales de la seguridad de la información. 25
Figura 2. Matriz de análisis de riesgo e impacto para la evaluación de riesgos. 29
Figura 3. Estrategias principales para el tratamiento del riesgo. 30
Figura 4. Ciclo PHVA aplicado al Sistema de Gestión de Seguridad de la Información. 35
Figura 5. Perfil preliminar de madurez de la seguridad de la información en la EMMAIPC-EP. 58
Figura 6. Trazabilidad de los productos del diseño del Sistema de Gestión de Seguridad de la Información. 81

Introducción

La información constituye hoy uno de los activos más valiosos de cualquier organización y, en el caso de las entidades públicas, su protección no es únicamente una necesidad operativa sino también una obligación legal. El crecimiento sostenido de los incidentes de seguridad, la digitalización de los procesos administrativos y la entrada en vigor de la Ley Orgánica de Protección de Datos Personales han situado la seguridad de la información en el centro de la gestión institucional. Frente a este escenario, la norma ISO/IEC 27001:2022 ofrece un marco reconocido internacionalmente para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.

La Empresa Pública Municipal Mancomunada de Aseo Integral de los cantones Cañar, Biblián, El Tambo y Suscal (EMMAIPC-EP) presta un servicio público esencial cuya operación depende de sistemas de información que administran datos de contribuyentes, contratos, emisiones tributarias, recaudación y expedientes documentales. Sin embargo, la institución no cuenta con políticas de seguridad aprobadas, con un inventario valorado de sus activos de información ni con un proceso formal de gestión de riesgos, situación que la expone a la pérdida de disponibilidad, integridad y confidencialidad de información crítica para la prestación del servicio.

El presente trabajo tiene como propósito diseñar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2022 para la EMMAIPC-EP, aplicando la metodología ISO/IEC 27005:2022 para la gestión de riesgos y tomando como referencia normativa nacional la Ley Orgánica de Protección de Datos Personales y el Esquema Gubernamental de Seguridad de la Información. El alcance comprende el diseño documental del sistema y no su ejecución operativa ni su certificación.

El documento se organiza en cuatro capítulos. El Capítulo I presenta el marco referencial, con el planteamiento y la formulación del problema, los antecedentes, la justificación, los objetivos, las limitaciones y las delimitaciones de la investigación. El Capítulo II desarrolla el marco teórico sobre seguridad de la información, activos de información, gestión de riesgos, sistemas de gestión y la norma ISO/IEC 27001:2022, e incluye el análisis de las metodologías de gestión de riesgos consideradas. El Capítulo III expone el marco metodológico, la selección de la metodología aplicada, las fases del diseño y los resultados del diagnóstico institucional. El Capítulo IV desarrolla la propuesta, con el alcance del sistema, el inventario valorado de activos, la matriz de

riesgos, el plan de tratamiento, la Declaración de Aplicabilidad, las políticas y el modelo de implementación. Finalmente se presentan las conclusiones y las recomendaciones derivadas del trabajo.

CAPÍTULO I

1.1 Planteamiento del problema

En la actualidad, la información representa uno de los activos estratégicos más importantes para las organizaciones, debido a que su disponibilidad, integridad y confidencialidad permiten garantizar la continuidad de los procesos administrativos, operativos y financieros. Sin embargo, el crecimiento de la transformación digital ha incrementado la cantidad de datos gestionados y, con ello, los riesgos asociados a amenazas como accesos no autorizados, pérdida o alteración de información, errores humanos y ataques informáticos. En este contexto, la implementación de estándares internacionales de seguridad de la información constituye un elemento fundamental para fortalecer la gestión de riesgos y garantizar la protección adecuada de los activos informacionales (Podrecca et al., 2022).

Las instituciones del sector público presentan una mayor exposición debido al volumen y sensibilidad de la información que administran, además de las limitaciones frecuentes relacionadas con la ausencia de políticas, procedimientos y controles formales de seguridad. En el caso ecuatoriano, normativas como la Ley Orgánica de Protección de Datos Personales (LOPDP) y el Esquema Gubernamental de Seguridad de la Información (EGSI) establecen la necesidad de implementar mecanismos orientados a proteger la información institucional. No obstante, muchas entidades aún presentan dificultades para gestionar adecuadamente sus riesgos tecnológicos, lo que puede comprometer la confidencialidad, integridad y disponibilidad de sus activos de información (Villarreal Morales et al., 2024).

La EMMAIPC-EP administra información administrativa, operativa y financiera mediante servidores, sistemas de gestión, bases de datos, redes internas y equipos tecnológicos; sin embargo, no cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI) formal basado en estándares internacionales como la norma ISO/IEC 27001:2022. El diagnóstico institucional realizado en 2026 lo evidencia con datos concretos: de los 91 activos tecnológicos inventariados, el 59,3 % superó su vida útil y el

41,8 % se encuentra en estado regular, malo o en reposición; el nivel de madurez de la seguridad de la información es de 1,5 sobre 5; no existen políticas de seguridad aprobadas ni procedimientos de respaldo documentados y probados; no se ha designado un responsable de seguridad de la información; y el sistema de facturación y recaudación, alojado en la nube, opera bajo una cuenta administrativa de titularidad del proveedor (EMMAIPC-EP, 2026a). Esta ausencia de políticas, controles, procedimientos de gestión de incidentes y mecanismos estructurados de evaluación de riesgos limita la capacidad institucional para prevenir y responder ante amenazas de seguridad, y puede afectar la continuidad operativa y la confianza institucional. Por ello, surge la necesidad de diseñar un SGSI basado en ISO/IEC 27001:2022 que permita fortalecer la protección de los activos de información de la EMMAIPC-EP, garantizando niveles adecuados de confidencialidad, integridad y disponibilidad.

1.1.1 Formulación del problema

Actualmente, la EMMAIPC-EP no cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI) formal que permita administrar de manera estructurada los riesgos asociados a sus activos de información. La ausencia de políticas, procedimientos, controles de seguridad y mecanismos definidos para la gestión de incidentes limita la capacidad institucional para proteger la confidencialidad, integridad y disponibilidad de la información administrativa, operativa y financiera que gestiona la entidad. Esta situación representa una vulnerabilidad dentro de la gestión tecnológica institucional, debido a que los recursos informáticos, bases de datos, sistemas de información y redes internas pueden estar expuestos a amenazas como accesos no autorizados, pérdida de información, alteración de datos o interrupciones en los servicios tecnológicos.

¿Cómo diseñar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2022 que permita fortalecer la confidencialidad, integridad y disponibilidad de los activos de información de la EMMAIPC-EP?

1.2 Antecedentes de la Investigación

Kitsios et al. (2023) desarrollaron una investigación titulada *"The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector"*, cuyo objetivo fue analizar cómo las organizaciones del sector de

tecnologías de la información adoptan la norma ISO/IEC 27001 y qué valor y beneficios obtienen de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). La investigación aplicó un estudio basado en el análisis de una organización del sector tecnológico que implementó un plan de adecuación para cumplir con los requisitos establecidos por la norma internacional. Los resultados evidenciaron que la implementación de ISO/IEC 27001 permite mejorar la gestión de riesgos, establecer controles sistemáticos, fortalecer la gobernanza de la información y aumentar la capacidad organizacional para proteger sus activos críticos. Este estudio aporta a la presente investigación debido a que demuestra que un SGSI basado en estándares internacionales constituye una herramienta estratégica para estructurar políticas, procedimientos y controles orientados a garantizar la confidencialidad, integridad y disponibilidad de la información dentro de una organización.

En el contexto internacional, Domínguez-Domínguez et al. (2023) desarrollaron una investigación titulada “Evaluation of an information security management system at a Mexican higher education institution”, cuyo objetivo fue evaluar el nivel de gestión de seguridad de la información mediante criterios relacionados con la norma ISO/IEC 27001. El estudio aplicó una metodología basada en la recopilación de información mediante encuestas, entrevistas y análisis de la gestión institucional, identificando deficiencias relacionadas con la capacitación del personal, conocimiento administrativo y aplicación de controles de seguridad. Los resultados demostraron que la ausencia de una gestión formal de riesgos limita la capacidad organizacional para prevenir incidentes de seguridad, evidenciando la importancia de implementar Sistemas de Gestión de Seguridad de la Información en instituciones que manejan grandes volúmenes de datos.

También en el ámbito internacional, Kurniawan et al. (2022) realizaron en Indonesia un estudio sobre la medición del desempeño de sistemas de información utilizando niveles de madurez asociados a controles de seguridad. La investigación permitió identificar brechas existentes entre el estado actual de seguridad y el nivel esperado por la organización, concluyendo que la evaluación periódica de controles permite establecer estrategias de mejora y fortalecer la protección de los activos de

información. Este antecedente demuestra la importancia de realizar diagnósticos iniciales antes del diseño de un SGSI, debido a que permiten determinar vulnerabilidades, riesgos y oportunidades de mejora dentro de una institución.

A nivel nacional, Donoso Vargas et al. (2023) aplicaron un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 en el sistema de rehabilitación social del Ecuador, específicamente sobre los mecanismos electrónicos de monitoreo de personas con medidas sustitutivas. El estudio definió los controles necesarios para proteger la información georreferenciada de los ciudadanos monitoreados y demostró la viabilidad de aplicar la norma en el sector público ecuatoriano bajo el marco legal vigente. Su aporte a esta investigación es la validación de la norma en instituciones públicas nacionales sujetas a la protección de datos personales; sin embargo, se centra en un sistema de monitoreo especializado y no en los procesos administrativos y financieros de una empresa municipal.

A nivel local, Aguilar-Coronel y Cuenca-Tapia (2025), de la Universidad Católica de Cuenca, diseñaron un Sistema de Gestión de Seguridad de la Información basado en el estándar ISO/IEC 27001 para la empresa EJEPROY Cía. Ltda. El diseño se estructuró en cinco fases que comprenden la definición del alcance, la obtención del aval de la alta gerencia, la elaboración del inventario de activos de información, el análisis de riesgos y la selección de controles. Este trabajo constituye el antecedente más cercano al presente proyecto por su alcance metodológico y su origen institucional; la diferencia radica en que se desarrolla sobre una empresa privada de construcción, mientras que la presente investigación aborda una empresa pública municipal mancomunada sujeta al Esquema Gubernamental de Seguridad de la Información y a la Ley Orgánica de Protección de Datos Personales.

1.3 Justificación de la investigación

El presente proyecto se justifica debido a la creciente necesidad de las organizaciones de fortalecer la protección de sus activos de información frente al aumento de amenazas cibernéticas, vulnerabilidades tecnológicas y riesgos asociados al tratamiento de datos digitales. La información constituye un recurso estratégico para la continuidad operativa, la toma de decisiones y el cumplimiento de los objetivos institucionales, por lo que su adecuada gestión requiere la aplicación de metodologías

estructuradas que permitan garantizar principios fundamentales como la confidencialidad, integridad y disponibilidad.

En el caso de la EMMAIPC-EP, la ausencia de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 representa una limitación para la identificación, evaluación y tratamiento adecuado de los riesgos relacionados con sus activos de información. Por ello, el diseño de un SGSI permitirá establecer lineamientos, políticas, controles y procedimientos orientados a una gestión preventiva y sistemática de la seguridad de la información, fortaleciendo la capacidad institucional para responder ante posibles incidentes y mejorar la continuidad de sus procesos críticos.

Desde una perspectiva académica y práctica, la investigación aportará una propuesta metodológica fundamentada en estándares internacionales que podrá servir como referencia para futuras implementaciones de sistemas de gestión de seguridad en instituciones del sector público. Los principales beneficiarios serán la EMMAIPC-EP, su personal y los usuarios de los servicios institucionales, debido a que una adecuada gestión de la seguridad de la información contribuye a proteger los datos administrados por la entidad y fortalecer la confianza ciudadana en la gestión pública.

1.4 Objetivos

1.4.1 Objetivo General

Diseñar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2022 para la EMMAIPC-EP, mediante el diagnóstico de la situación actual, la gestión de riesgos sobre los activos de información y la definición de controles de seguridad, con el fin de fortalecer la confidencialidad, integridad y disponibilidad de la información institucional.

1.4.2 Objetivo Específico

- Construir el marco teórico relacionado con la seguridad de la información, la gestión de riesgos y la norma ISO/IEC 27001:2022, mediante la revisión de literatura científica y normativa vigente, para fundamentar conceptualmente el diseño del Sistema de Gestión de Seguridad de la Información en EMMAIPC-EP.

- Identificar los activos de información y riesgos de seguridad en la empresa EMMAIPC-EP, mediante un diagnóstico documental y análisis del entorno tecnológico, previa selección justificada de la metodología de gestión de riesgos, para determinar las principales vulnerabilidades que afectan la información institucional.
- Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022, a través de la definición de controles, políticas y procedimientos alineados a la norma ISO/IEC 27002:2022, para mejorar la protección de los activos de información.
- Proponer un modelo de implementación del SGSI basado en el ciclo PHVA, mediante la integración de la gestión de riesgos y el seguimiento de controles, para fortalecer la seguridad de la información y la continuidad operativa en EMMAIPC-EP.
- Validar el diseño del Sistema de Gestión de Seguridad de la Información, mediante la verificación de la cobertura entre riesgos y controles, la comprobación del cumplimiento de los requisitos de la norma ISO/IEC 27001:2022, para confirmar su pertinencia y aplicabilidad en el contexto de la EMMAIPC-EP.

1.5 Limitaciones

- No se dispuso de registros históricos de incidentes de seguridad, pues la institución no contaba con documentación formal de eventos como pérdida de información, accesos no autorizados, vulnerabilidades detectadas o fallas tecnológicas. Por ello, la probabilidad de los riesgos se estimó de forma cualitativa a partir del criterio del personal técnico y de las condiciones observadas, lo que introduce subjetividad en la valoración y limita la validez de las frecuencias asignadas; la medición de los indicadores durante la implementación permitirá contrastarlas.
- La investigación dependió de la colaboración del personal y del acceso a la información institucional. El diagnóstico se apoyó en la revisión documental y en la información

proporcionada por la Unidad de Tecnologías de la Información y Comunicación, conformada por un solo servidor público, sin pruebas técnicas de vulnerabilidades ni verificación directa de configuraciones; en consecuencia, el estado de algunos controles técnicos se determinó por declaración y no por comprobación, lo que afecta la validez interna de la línea base de cumplimiento.

- El trabajo se desarrolló dentro de un periodo académico, lo que impidió ejecutar la implementación del SGSI, la auditoría interna, la medición de los indicadores tras su aplicación ni una validación externa del diseño. En consecuencia, los resultados se limitan al diseño y a su validación interna, y la eficacia real de los controles propuestos no fue comprobada.

1.6 Delimitaciones

- El estudio se centrará en un diseño de Sistema de Gestión de seguridad de la información para la EMMAIPC-EP tomando como referencia los requisitos establecidos en la norma ISO/IEC 27001:2022.
- La investigación se limitará al diagnóstico de la situación actual, identificación de activos de información, análisis de riesgos y definición de controles de seguridad alineados con la norma ISO/IEC 27001:2022, sin considerar la ejecución operativa de dichos controles dentro de la institución.
- El proyecto estará enfocado en los activos tecnológicos y procesos institucionales relacionados con la gestión de información de EMMAIPC-EP, sin abarcar otras entidades públicas o privadas externas a la organización.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 Seguridad de la información

2.1.1 Concepto de seguridad de la información

La seguridad de la información puede definirse como el conjunto de medidas técnicas, organizativas y humanas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, independientemente del formato o medio en que se encuentre. Coronel y Quirumbay (2022) precisan que este concepto trasciende la seguridad de los equipos informáticos y se extiende al gobierno y la gestión de la información como recurso organizacional, considerando tanto los datos digitales como los soportes físicos y los procesos que los utilizan.

2.1.2 Importancia de la seguridad de la información en las organizaciones

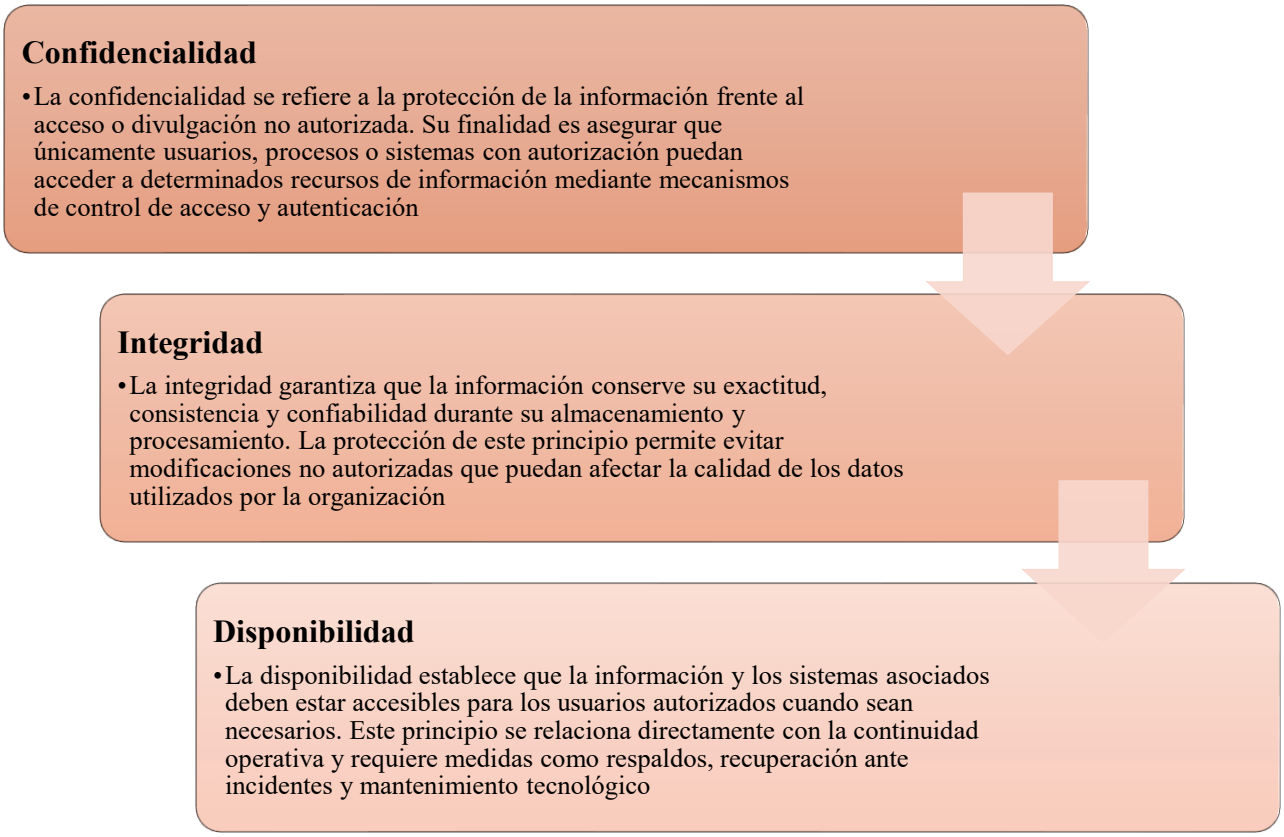
La relevancia de la seguridad de la información radica en su capacidad para proteger los activos críticos de la organización, reducir la exposición a riesgos y sostener la continuidad de las operaciones. Nurbojatmiko et al. (2025) destacan que la adopción de un enfoque estructurado de seguridad, alineado con la norma ISO/IEC 27001, permite a las organizaciones responder de manera sistemática a los desafíos de la era de la Sociedad 5.0, en la que la información se convierte en el eje de la toma de decisiones. La ausencia de mecanismos adecuados de protección puede derivar en pérdida de datos, interrupción de servicios, sanciones legales y deterioro de la reputación institucional.

2.1.3 Principios fundamentales de seguridad de la información

Los principios fundamentales de la seguridad de la información se sintetizan en la denominada tríada CIA, que agrupa la confidencialidad, la integridad y la disponibilidad. Ortega Ovalle (2026) explica que estos tres pilares constituyen el fundamento sobre el cual la norma ISO/IEC 27001:2022 estructura los requisitos de un SGSI, orientando la aplicación de controles y la gestión de riesgos. A continuación, se describe en la Figura 1 los principales principios fundamentales:

Figura 1

Principios fundamentales de la seguridad de la información.



Nota. (Universitat Carlemany, 2025)

2.2 Activos de información

Los activos de información constituyen el objeto principal de protección de un SGSI, por lo que su identificación resulta un requisito previo para cualquier proceso de gestión de la seguridad. La norma ISO/IEC 27005:2022 adopta un enfoque basado en activos, en el que cada activo se vincula con amenazas y vulnerabilidades específicas que pueden comprometer los objetivos de seguridad de la organización.

2.2.1 Concepto de activo de información

Los activos de información son cualquier tipo de recurso que contenga información valiosa para una organización. Estos incluyen datos, documentos, correos electrónicos, software, sistemas, redes, dispositivos y bases de datos. La protección de estos activos es crucial para garantizar la privacidad, integridad y disponibilidad de la

información, y prevenir ciberataques como el robo de identidad y el fraude (Coronel Suárez & Quirumbay Yagual, 2022).

2.2.2 Clasificación de activos de información

La clasificación de los activos permite asignar niveles de protección proporcionales a su valor y sensibilidad, lo que facilita la toma de decisiones sobre los controles a implementar. En la Tabla 1 se presenta una clasificación de los principales tipos de activos de información.

Tabla 1

Clasificación de activos de información

Tipo de activos	Concepto
Datos e información	Constituyen uno de los activos más valiosos de una organización, ya que incluyen bases de datos, registros financieros, expedientes y documentos críticos. Su protección requiere controles de acceso basados en roles, cifrado cuando sea necesario y la realización periódica de copias de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información ante incidentes o pérdidas de datos.
Software	Comprende sistemas operativos, aplicaciones y plataformas de gestión que soportan las operaciones de la organización. Es fundamental mantenerlos actualizados mediante parches de seguridad, gestionar las vulnerabilidades de forma continua y verificar la integridad de las aplicaciones para reducir el riesgo de explotación por parte de atacantes.
Hardware	Incluye servidores, computadoras, dispositivos de almacenamiento y equipos de red. Estos activos requieren medidas de protección física contra robos, daños o accesos no autorizados, además de mantenimiento preventivo y monitoreo continuo para asegurar su correcto funcionamiento y disponibilidad.
Servicios	Engloba servicios de red, correo electrónico, conectividad y plataformas en la nube. Su seguridad depende de la disponibilidad, la continuidad operativa y el cumplimiento de acuerdos de nivel de servicio (SLA), además de mecanismos de monitoreo y recuperación ante incidentes que minimicen interrupciones.
Personas	El personal técnico, administrativo y directivo representa un activo esencial en la seguridad de la información. Es necesario proporcionar capacitación continua en ciberseguridad, definir claramente responsabilidades y promover una cultura organizacional que reduzca errores humanos y fortalezca el cumplimiento de las políticas de seguridad.

Nota. Elaboración propia con base en la norma ISO/IEC 27005:2022 (International Organization for Standardization & International Electrotechnical Commission, 2022a).

2.2.3 Identificación y valoración de activos de información

La identificación consiste en elaborar un inventario detallado de los activos, mientras que la valoración establece su importancia en función del impacto que tendría su pérdida, alteración o divulgación. Olvera Peña et al. (2026) evidencian, mediante la aplicación de la norma ISO/IEC 27001:2022, que la identificación y valoración de los activos tecnológicos permite determinar su nivel de riesgo y priorizar las acciones de protección, empleando escalas de valoración consistentes que respaldan la toma de decisiones.

2.3 Gestión de riesgos de seguridad de la información

2.3.1 Concepto de riesgo de seguridad de la información

El riesgo de seguridad de la información se entiende como la posibilidad de que una amenaza explote una vulnerabilidad de un activo, generando un impacto negativo para la organización. La norma ISO/IEC 27005:2022 define el riesgo en términos de la combinación entre la probabilidad de ocurrencia de un evento y la magnitud de sus consecuencias, lo que permite priorizar los riesgos según su nivel de gravedad (International Organization for Standardization & International Electrotechnical Commission, 2022a).

2.3.2 Amenazas y vulnerabilidades

Las amenazas son eventos o acciones potenciales que pueden causar daño a los activos, mientras que las vulnerabilidades son debilidades que pueden ser aprovechadas por dichas amenazas. Boné-Andrade et al. (2023) advierten que el panorama de amenazas se ha intensificado con la adopción de modelos de trabajo híbridos y remotos, lo que exige estrategias de ciberseguridad que combinen medidas técnicas, organizativas y de concienciación del personal. En la Tabla 2 se sintetizan amenazas y vulnerabilidades frecuentes en los entornos organizacionales.

Tabla 2

Ejemplos de amenazas y vulnerabilidades frecuentes

Amenaza	Vulnerabilidad asociada	Posible impacto
Software malicioso (malware, ransomware)	Falta de actualización y de antivirus.	Pérdida o secuestro de información.
Accesos no autorizados	Contraseñas débiles y ausencia de control de acceso.	Fuga o alteración de datos sensibles.

Amenaza	Vulnerabilidad asociada	Posible impacto
Error humano	Falta de capacitación del personal.	Divulgación o pérdida accidental de información.
Fallos técnicos	Ausencia de respaldos y mantenimiento.	Interrupción de servicios y pérdida de datos.
Ingeniería social (phishing)	Escasa concienciación en seguridad.	Acceso indebido a credenciales y sistemas.

Nota. Elaboración propia.

2.3.3 Análisis y evaluación de riesgos

El análisis de riesgos consiste en determinar el nivel de cada riesgo a partir de la probabilidad y el impacto, mientras que la evaluación compara dichos niveles con los criterios de aceptación definidos por la organización. La matriz de probabilidad e impacto (Figura 2) representa gráficamente este proceso, permitiendo clasificar los riesgos en niveles alto, medio y bajo mediante la combinación de la probabilidad de ocurrencia y la severidad de las consecuencias. Esta clasificación facilita la priorización de los riesgos que requieren tratamiento y la toma de decisiones sobre la implementación de controles. Olvera Peña et al. (2026) demuestran que la valoración sistemática de los activos, las amenazas y las vulnerabilidades permite obtener puntajes de riesgo que orientan la selección de controles del Anexo A de la norma ISO/IEC 27001:2022 y sustentan el tratamiento posterior.

Figura 2

Matriz de análisis de riesgo e impacto para la evaluación de riesgos.



Nota. (SafetyCulture, 2026)

2.3.4 Tratamiento de riesgos

El tratamiento de riesgos comprende la selección e implementación de las opciones más adecuadas para gestionar los riesgos identificados y evaluados, con el propósito de reducir su impacto sobre los activos de información y mantenerlos dentro de los niveles de aceptación definidos por la organización. De acuerdo con la norma ISO/IEC 27005:2022, existen cuatro estrategias principales para el tratamiento del riesgo se presenta a continuación en la Figura 3:

Figura 3

Estrategias principales para el tratamiento del riesgo.



Nota. Autoría Propia.

Asimismo, cada decisión de tratamiento debe documentarse y justificarse adecuadamente, estableciendo los controles que serán implementados, los responsables de su ejecución y los plazos definidos para su aplicación. Finalmente, estas decisiones se reflejan en la Declaración de Aplicabilidad (Statement of Applicability, SoA), documento que justifica la inclusión o exclusión de los controles del Anexo A de la norma ISO/IEC 27001:2022 y constituye una evidencia fundamental para la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información (International Organization for Standardization & International Electrotechnical Commission, 2022a).

2.4 Sistema de Gestión de Seguridad de la Información (SGSI)

2.4.1 Concepto de SGSI

Un Sistema de Gestión de Seguridad de la Información es el conjunto coordinado de políticas, procedimientos, roles, controles y actividades que una organización despliega para gestionar de manera sistemática la seguridad de su información. Nurbojatmiko et al. (2025) concluyen, tras una revisión sistemática de literatura, que la norma ISO/IEC 27001 constituye una solución integral para la seguridad de la información, al combinar la gestión de riesgos con la mejora continua.

2.4.2 Objetivos y beneficios del SGSI

Los objetivos de un SGSI se orientan a proteger la confidencialidad, integridad y disponibilidad de la información y a reducir los riesgos a niveles aceptables. Entre sus beneficios se encuentran la protección de los activos, el cumplimiento normativo y el fortalecimiento de la confianza institucional. Donoso Vargas et al. (2023) evidencian que la aplicación de un SGSI basado en la norma ISO/IEC 27001 en el ámbito público permite establecer diagnósticos, gestionar riesgos y definir mecanismos de aplicabilidad y seguimiento, lo que mejora la gestión de la seguridad de la información. La siguiente tabla presenta de manera resumida los principales objetivos y beneficios de un Sistema de Gestión de Seguridad de la Información:

Tabla 3

Objetivos y Beneficios del SGSI

Objetivo del SGSI	Beneficio para la organización
Proteger la confidencialidad, integridad y disponibilidad de la información.	Reduce accesos no autorizados, alteraciones, pérdidas y fallos en el acceso a la información.
Identificar, evaluar y tratar los riesgos de seguridad.	Permite priorizar controles y utilizar los recursos según el nivel de riesgo existente.
Definir políticas, responsabilidades y procedimientos.	Mejora la coordinación, la toma de decisiones y la rendición de cuentas.
Cumplir requisitos legales, regulatorios y contractuales.	Disminuye la posibilidad de sanciones, incumplimientos y conflictos con clientes o proveedores.
Fortalecer la cultura de seguridad.	Aumenta la conciencia y participación del personal en la protección de la información.
Mejorar continuamente la seguridad.	Facilita la detección de fallas, la corrección de incidentes y la adaptación frente a nuevas amenazas.

Objetivo del SGSI	Beneficio para la organización
Aumentar la resiliencia y continuidad del negocio.	Mejora la capacidad para responder y recuperarse ante incidentes de seguridad.
Generar confianza en las partes interesadas.	Fortalece la reputación institucional y puede facilitar contratos, licitaciones y relaciones comerciales.

Nota. (Donoso Vargas et al., 2023)

2.4.3 Componentes de un SGSI

Un Sistema de Gestión de Seguridad de la Información (SGSI) está compuesto por elementos que permiten organizar, proteger y mejorar la seguridad de la información dentro de una organización. Entre sus principales componentes se encuentran la definición del contexto y alcance, el liderazgo de la alta dirección, la gestión de riesgos, la planificación de objetivos, la asignación de recursos y responsabilidades, la documentación de políticas y procedimientos, la aplicación de controles de seguridad, la gestión de incidentes, la evaluación del desempeño y la mejora continua. Todos estos elementos se integran mediante la participación coordinada de las personas, los procesos y la tecnología (Kamil et al., 2023).

2.4.4 Ciclo PHVA aplicado a la seguridad de la información

El ciclo PHVA (Planificar, Hacer, Verificar y Actuar), también conocido como ciclo de Deming, constituye el modelo de mejora continua sobre el cual se estructura la norma ISO/IEC 27001:2022. Este ciclo permite gestionar el SGSI de manera iterativa, asegurando su adaptación permanente a los cambios del entorno. En la Tabla 4 se describe su aplicación al diseño de un SGSI.

Tabla 4

Fases PHVA aplicado al SGSI

Fase	Descripción	Aplicación al diseño del SGSI
Planificar	Establecer el contexto, la política, los objetivos y la evaluación de riesgos.	Definición del alcance, inventario de activos y análisis de riesgos.
Hacer	Implementar y operar los controles y procedimientos definidos.	Aplicación de políticas y controles de seguridad seleccionados.
Verificar	Monitorear y evaluar el desempeño del SGSI.	Revisión de indicadores, auditorías internas y seguimiento.
Actuar	Adoptar acciones correctivas y de mejora continua.	Ajuste de controles y actualización del SGSI.

Nota. Elaboración propia.

2.5 Norma ISO/IEC 27001:2022

El diseño de un SGSI constituye la fase que traduce los fundamentos teóricos y normativos en una propuesta concreta para la organización. Este proceso se estructura conforme a los requisitos de la norma ISO/IEC 27001:2022 y comprende el diagnóstico inicial, la identificación de brechas, la definición de políticas y el modelo de implementación. En la Tabla 5 se resumen estas fases (International Organization for Standardization & International Electrotechnical Commission, 2022a).

Tabla 5

Fases del diseño de un SGSI basado en ISO/IEC 27001:2022

Fase	Descripción	Resultado esperado
Diagnóstico inicial	Evaluación del estado actual de la seguridad de la información.	Línea base de seguridad de la organización.
Identificación de brechas	Comparación entre el estado actual y los requisitos de la norma.	Informe de brechas frente a ISO/IEC 27001:2022.
Definición de políticas	Elaboración de políticas y procedimientos de seguridad.	Documentación del SGSI.
Modelo de implementación	Estructuración del sistema bajo el ciclo PHVA.	Plan de diseño e implementación del SGSI.

Nota. Elaboración *propia*

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) comienza con un diagnóstico inicial para conocer el estado actual de la seguridad en la organización y establecer una línea base. Posteriormente, se identifican las brechas mediante la comparación de la situación existente con los requisitos de la norma ISO/IEC 27001:2022. Con base en estos resultados, se definen las políticas y procedimientos necesarios para fortalecer la gestión de la seguridad de la información. Finalmente, se diseña el modelo de implementación siguiendo el ciclo PHVA (Planificar, Hacer, Verificar y Actuar), lo que permite una implementación estructurada y la mejora continua del SGSI.

2.6 Metodologías

A continuación, se describen tres metodologías reconocidas para la gestión de riesgos de seguridad de la información, con el propósito de seleccionar la más adecuada para el diseño del SGSI

2.6.1 Metodología ISO/IEC 27005:2022

La norma ISO/IEC 27005:2022 proporciona directrices para la gestión de riesgos de seguridad de la información dentro del ciclo de vida del SGSI, alineadas directamente con los requisitos de la ISO/IEC 27001. Su proceso comprende la identificación, el análisis, la evaluación y el tratamiento del riesgo, permitiendo un enfoque tanto cualitativo como cuantitativo según el contexto de la organización. Su principal ventaja es la compatibilidad nativa con la estructura de cláusulas y el Anexo A de la ISO/IEC 27001:2022, lo que facilita la trazabilidad entre el análisis de riesgos y la Declaración de Aplicabilidad (International Organization for Standardization & International Electrotechnical Commission, 2022a).

2.6.2 Metodología MAGERIT

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) fue desarrollada por el Consejo Superior de Administración Electrónica de España y es actualmente mantenida por la Secretaría General de Administración Digital, con la colaboración del Centro Criptológico Nacional. Su versión vigente, MAGERIT v3, se estructura en tres libros método, catálogo de elementos y guía técnica y toma como referencia la norma ISO 31000 para el proceso de gestión de riesgos, el método comprende el inventario y la valoración de activos en cinco dimensiones, la identificación de amenazas y vulnerabilidades, la selección de salvaguardas y la estimación del riesgo residual, apoyándose en herramientas especializadas como PILAR para el análisis cualitativo y cuantitativo, conforme al Libro I (Método) de la metodología (Ministerio de Hacienda y Administraciones Públicas, 2012).

2.6.3 Metodología OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) es una metodología desarrollada por el Software Engineering Institute de la Universidad Carnegie Mellon, orientada a priorizar los riesgos operativos por encima del detalle técnico. Su versión más reciente, OCTAVE Allegro, simplifica el proceso original para adaptarlo a organizaciones con recursos limitados en seguridad de la información, mediante un método autodirigido que involucra al personal de distintos niveles de la organización (Miranda Jiménez, 2021). El proceso se desarrolla en tres fases evaluación organizacional, identificación de vulnerabilidades tecnológicas y desarrollo de un plan de

mitigación y privilegia un enfoque cualitativo basado en talleres y en la percepción de los propios colaboradores sobre los activos críticos.

Figura 4

Ciclo PHVA aplicado al Sistema de Gestión de Seguridad de la Información.



Nota. Elaboración propia con base en International Organization for Standardization e International Electrotechnical Commission (2022b).

2.7 Marco normativo ecuatoriano para la seguridad de la información

Además de la norma internacional ISO/IEC 27001:2022, el diseño de un SGSI en una empresa pública ecuatoriana debe considerar las obligaciones que impone el ordenamiento jurídico nacional. Tres instrumentos resultan determinantes para la EMMAIPC-EP: la Ley Orgánica de Protección de Datos Personales (LOPDP), la Ley Orgánica para la Transformación Digital y Audiovisual (LOTDA) y el Esquema Gubernamental de Seguridad de la Información (EGSI). A continuación se describe cada uno y su relación con la norma ISO/IEC 27001:2022.

2.7.1 Ley Orgánica de Protección de Datos Personales

La LOPDP, publicada en el Quinto Suplemento del Registro Oficial N.º 459 de 26 de mayo de 2021, regula el tratamiento de datos personales por parte de personas naturales y jurídicas, públicas y privadas, y es de aplicación obligatoria para las instituciones del sector público (Asamblea Nacional del Ecuador, 2021). La ley establece principios de tratamiento como juridicidad, lealtad, transparencia, finalidad, pertinencia y minimización, proporcionalidad, confidencialidad, calidad y exactitud, conservación, seguridad y responsabilidad proactiva; reconoce al titular los derechos de información, acceso, rectificación y actualización, eliminación, oposición, portabilidad y suspensión del tratamiento; y define las figuras del responsable y del encargado del tratamiento, así como del delegado de protección de datos personales, cuya designación es obligatoria para las entidades del sector público.

En materia de seguridad, la LOPDP exige al responsable del tratamiento implementar medidas técnicas, organizativas y administrativas adecuadas para proteger la confidencialidad, la integridad y la disponibilidad de los datos personales, aplicar los principios de privacidad desde el diseño y por defecto, realizar evaluaciones de impacto cuando el tratamiento conlleve alto riesgo y notificar las vulneraciones de seguridad a la Autoridad de Protección de Datos Personales y, cuando corresponda, a los titulares (Asamblea Nacional del Ecuador, 2021). El artículo 38 de la ley dispone, además, que el mecanismo gubernamental de seguridad de la información incluya las medidas aplicables al tratamiento de datos personales en todas las instituciones comprendidas en el artículo 225 de la Constitución, lo que vincula directamente la protección de datos con el EGSI. Para la EMMAIPC-EP, que trata datos personales de usuarios del servicio de aseo,

contribuyentes y servidores públicos en sus sistemas de facturación, recaudación y talento humano, estas obligaciones se cubren mediante los controles del Anexo A de la norma ISO/IEC 27001:2022 relativos a la privacidad y protección de la información de identificación personal (A.5.34), la clasificación de la información (A.5.12), el control de acceso (A.5.15) y la gestión de incidentes (A.5.24 a A.5.28), que fueron considerados en la Declaración de Aplicabilidad y en la política específica de protección de datos personales de este trabajo.

2.7.2 Esquema Gubernamental de Seguridad de la Información

El EGSI es el mecanismo definido por el Estado ecuatoriano para implementar un sistema de gestión de seguridad de la información en el sector público. Su primera versión se expidió en 2013 y la versión 2.0 mediante el Acuerdo Ministerial N.º 025-2019, de aplicación obligatoria únicamente para las instituciones de la Administración Pública Central, Institucional y dependiente de la Función Ejecutiva. La Ley Orgánica para la Transformación Digital y Audiovisual, publicada en el Suplemento del Registro Oficial N.º 245 de 7 de febrero de 2023, creó el Marco de Seguridad Digital del Estado y dispuso que las entidades de la Administración Pública establezcan, mantengan y documenten un sistema de gestión de la seguridad de la información (Asamblea Nacional del Ecuador, 2023).

En aplicación de ese mandato, el Ministerio de Telecomunicaciones y de la Sociedad de la Información expidió, mediante el Acuerdo Ministerial N.º MINTEL-MINTEL-2024-0003 de 8 de febrero de 2024, la versión vigente del EGSI y derogó el Acuerdo 025-2019. La nueva versión amplía la obligatoriedad a todas las entidades, organismos e instituciones del sector público comprendidas en el artículo 225 de la Constitución, incluidas las personas jurídicas creadas por los gobiernos autónomos descentralizados para la prestación de servicios públicos, como las empresas públicas municipales y mancomunadas; dispone realizar la evaluación de riesgos sobre los activos de información de los procesos esenciales y elaborar el plan de tratamiento conforme a la guía de gestión de riesgos anexa al acuerdo; obliga a conformar un Comité de Seguridad de la Información con al menos tres integrantes y a designar un Oficial de Seguridad de la Información con formación y experiencia en la materia; fija un plazo de doce meses para su implementación y exige un informe anual de cumplimiento de la gestión de riesgos suscrito por el presidente del comité (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2024). El EGSI se estructura sobre los dominios y controles

de la familia ISO/IEC 27000, de modo que un SGSI diseñado conforme a la norma ISO/IEC 27001:2022 satisface los requisitos del esquema y, a la vez, prepara a la institución para una eventual certificación.

2.7.3 Implicaciones para el diseño del SGSI de la EMMAIPC-EP

La convergencia de estos tres instrumentos determina que, para la EMMAIPC-EP, la seguridad de la información no es una buena práctica opcional sino una obligación legal exigible, cuya inobservancia puede acarrear responsabilidades administrativas para la máxima autoridad y sanciones en materia de protección de datos. Por ello, el diseño propuesto en este trabajo adopta la norma ISO/IEC 27001:2022 como marco técnico y alinea sus productos con las exigencias nacionales: el inventario y la valoración de activos y la matriz de riesgos responden a la evaluación de riesgos que exige el EGSI; la estructura de roles incorpora el Comité de Seguridad de la Información y el Responsable de Seguridad de la Información, equivalente al Oficial de Seguridad de la Información del esquema; la política general y las políticas específicas incluyen la protección de datos personales conforme a la LOPDP; y los indicadores y el cronograma de doce meses del modelo de implementación coinciden con el plazo y el informe anual de cumplimiento establecidos por el acuerdo ministerial. De esta manera, el SGSI diseñado permite a la institución cumplir simultáneamente con el estándar internacional y con la normativa ecuatoriana vigente.

CAPÍTULO III

3 MARCO METODOLÓGICO

El presente capítulo describe el diseño metodológico aplicado para el desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI) de la EMMAIPC-EP. Se define el enfoque y el nivel de la investigación, la población y la muestra de activos de información considerada, las técnicas e instrumentos empleados para la recolección de datos y el tratamiento otorgado a la información obtenida. Posteriormente, se justifica la selección de la metodología de gestión de riesgos, se establecen las fases que estructuran el diseño del SGSI conforme a la norma ISO/IEC 27001:2022 y se presentan los resultados del diagnóstico de la situación actual de la seguridad de la información institucional, los cuales constituyen la línea base sobre la que se construye la propuesta desarrollada en el Capítulo IV.

3.1 Enfoque de la investigación

La investigación adopta un enfoque mixto, con predominancia cualitativa y componente cuantitativo complementario. El componente cualitativo permite interpretar los requisitos establecidos en la norma ISO/IEC 27001:2022, analizar el marco normativo ecuatoriano aplicable al sector público y comprender la organización, los procesos y las responsabilidades vinculadas al tratamiento de la información institucional, elementos que no pueden reducirse a mediciones numéricas.

El componente cuantitativo se expresa en la clasificación y el cálculo de indicadores sobre el inventario de activos tecnológicos, la valoración de activos de información mediante escalas ordinales, la determinación del nivel de riesgo a partir de la combinación entre probabilidad e impacto, y la valoración del nivel de madurez de los dominios de seguridad mediante una escala de capacidad de cero a cinco. La combinación de ambos enfoques resulta pertinente porque el diseño de un SGSI exige simultáneamente comprender el contexto organizacional y sustentar decisiones de tratamiento del riesgo en evidencias medibles y verificables.

3.2 Nivel de la investigación

La investigación es de nivel descriptivo con alcance propositivo. Es descriptiva porque caracteriza el estado actual de los activos de información, la infraestructura tecnológica, las aplicaciones institucionales, la gestión de datos, los mecanismos de respaldo y el nivel de madurez de la seguridad de la información en la EMMAIPC-EP, sin manipular variables ni establecer relaciones causales entre ellas.

Es propositiva porque, a partir de la caracterización obtenida y de la identificación de brechas frente a los requisitos normativos, se elabora una propuesta concreta: el diseño de un Sistema de Gestión de Seguridad de la Información con políticas, controles y un modelo de implementación estructurado bajo el ciclo PHVA. El estudio no comprende la ejecución operativa de los controles, la realización de auditorías internas ni el proceso de certificación, conforme a las delimitaciones establecidas en el Capítulo I.

3.3 Población y muestra

La población está constituida por el conjunto de activos de información de la EMMAIPC-EP, que comprende los noventa y un activos tecnológicos registrados en el

inventario patrimonial institucional con corte al 24 de junio de 2026, las aplicaciones y servicios en la nube identificados en el portafolio institucional, las fuentes de datos asociadas a los procesos administrativos, financieros, documentales y operativos, así como el talento humano vinculado a la administración de dichos recursos.

La muestra es de tipo no probabilístico intencional, seleccionada en función de la criticidad de los activos para la continuidad de los procesos institucionales y de la disponibilidad de documentación técnica y contractual suficiente para su análisis. Bajo este criterio se incorporaron los sistemas Flectra ERP 3.0 y e-Doc Manager, la infraestructura de servidor, red y almacenamiento, los servicios en la nube contratados, los sistemas biométricos y de rastreo satelital, y las fuentes de datos calificadas con criticidad alta o crítica.

En cuanto al talento humano, se trabajó con la totalidad del personal técnico asignado a la Unidad de Tecnologías de la Información y Comunicación, constituida por un único servidor con el cargo de Analista de Tecnologías de la Información y Comunicación, por lo que en este componente no existe muestreo sino censo. Al tratarse de una muestra no probabilística, los hallazgos no son generalizables a otras entidades públicas y deben interpretarse como un análisis específico del caso estudiado; no obstante, esta aproximación es pertinente para un estudio de carácter descriptivo y propositivo orientado al diseño de una solución institucional.

3.4 Técnicas e instrumentos de recolección de información

La recolección de información se sustentó principalmente en el análisis documental, complementado con observación estructurada y entrevista al informante clave del área tecnológica. La Tabla 6 presenta las fuentes documentales institucionales utilizadas y su aporte al diagnóstico.

Tabla 6

Fuentes documentales institucionales utilizadas

Documento	Fecha	Aporte al diagnóstico
Listado de ubicación de activos fijos: equipos, sistemas y paquetes informáticos	24/06/2026	Inventario patrimonial, ubicación, custodios, estado, vida útil y valor histórico de los activos tecnológicos.

Documento	Fecha	Aporte al diagnóstico
Plan Estratégico Institucional 2026–2030	Agosto 2025	Estructura organizacional, cadena de valor, catálogo de servicios, objetivos, riesgos e indicadores institucionales.
Informe de determinación de la necesidad para infraestructura cloud de Flectra ERP	Julio 2026	Estado del ERP, módulos, infraestructura contratada, dependencia del proveedor, brechas y riesgos identificados.
Términos de referencia del servicio cloud de Flectra ERP	Julio 2026	Integraciones, necesidades de migración, control institucional, seguridad, respaldos y continuidad.
Certificado anual de suscripción de e-Doc Manager	10/07/2026	Licencias, vigencia, soporte, actualizaciones, respaldos y condiciones del servicio.
Acta de entrega–recepción definitiva de e-Doc Manager	13/07/2026	Proveedor, orden de compra, valor, plazo, número de usuarios y recepción del servicio.

Nota. Elaboración propia con base en el Diagnóstico Integral de Tecnologías de la Información de la EMMAIPC-EP (2026a).

A partir de estas fuentes, la Tabla 7 sintetiza las técnicas e instrumentos aplicados y su vinculación con los objetivos específicos de la investigación. Los tres instrumentos principales se presentan completos en los anexos: la guía de entrevista semiestructurada al responsable de la Unidad de TIC (Anexo 2), la ficha de inventario de activos de información (Anexo 3) y la lista de verificación de cumplimiento de las cláusulas 4 a 10 y de los controles del Anexo A de la norma ISO/IEC 27001:2022 (Anexo 4).

Tabla 7

Técnicas e instrumentos de recolección de información

Técnica	Instrumento	Propósito	Objetivo
Revisión de literatura científica y normativa	Matriz de registro bibliográfico	Fundamentar conceptualmente la seguridad de la información, la gestión de riesgos y los requisitos de la norma.	OE1
Análisis documental institucional	Ficha de análisis documental	Identificar activos, sistemas, contratos, proveedores, procesos y responsabilidades.	OE2
Observación estructurada	Ficha de inventario de activos de información	Registrar categoría, estado, antigüedad, custodio, criticidad y ubicación de los activos.	OE2
Entrevista semiestructurada	Guía de entrevista al Analista TIC	Validar información técnica, prácticas vigentes, controles existentes y limitaciones operativas.	OE2
Lista de verificación normativa	Checklist de las cláusulas 4 a 10 y de los controles del Anexo A	Determinar el grado de cumplimiento y las brechas frente a la norma.	OE2 y OE3

Técnica	Instrumento	Propósito	Objetivo
Análisis de riesgos	Matriz de identificación, valoración y tratamiento de riesgos	Determinar el nivel de riesgo de los activos críticos y seleccionar controles.	OE3
Valoración de madurez	Escala de capacidad de 0 a 5 por dominio	Establecer la línea base de madurez de la seguridad de la información.	OE2 y OE4

Nota. Elaboración propia.

3.5 Tratamiento de la información

La información recolectada fue organizada, clasificada y tabulada en matrices que permitieron su análisis sistemático. Los activos tecnológicos se clasificaron por categoría, estado de conservación, fecha de adquisición, vida útil registrada, valor histórico y unidad custodia, obteniéndose frecuencias absolutas y relativas. Las aplicaciones se organizaron en un portafolio que registra estado, cobertura funcional, criticidad y riesgo de obsolescencia. Los contratos y servicios tercerizados se consolidaron en una matriz de proveedores con objeto, instrumento, vigencia, valor y nivel de criticidad.

Con el propósito de garantizar la trazabilidad y la honestidad metodológica del diagnóstico, cada dato fue calificado según su grado de confiabilidad, conforme a los criterios descritos en la Tabla 8. Este procedimiento evita atribuir certeza a información que no consta en la documentación disponible y delimita con precisión el alcance de las conclusiones.

Tabla 8

Criterios de confiabilidad aplicados a la información

Criterio	Descripción	Tratamiento en el análisis
Información verificada	Dato que consta expresamente en documentos institucionales, contractuales o patrimoniales.	Se utiliza como evidencia directa para el diagnóstico y la valoración de riesgos.
Información pendiente de validación técnica	Dato identificado parcialmente que requiere comprobación en campo o confirmación del proveedor.	Se registra con la observación "por verificar" y se incorpora como requerimiento de levantamiento.
Elemento no identificado	Componente, control o registro que no aparece en la documentación disponible.	Se declara como brecha y se traslada al análisis de riesgos y a la propuesta.

Nota. Elaboración propia con base en el Diagnóstico Integral de Tecnologías de la Información de la EMMAIPC-EP (2026a).

El tratamiento cuantitativo comprendió el cálculo de porcentajes de participación por estado y por categoría de activo, la determinación del porcentaje de activos con vida útil patrimonial superada, la consolidación de valores históricos por año de adquisición y la obtención del promedio aritmético de los niveles de madurez asignados a cada dominio. Finalmente, se aplicó la triangulación entre fuentes documentales, observación e información proporcionada por el Analista TIC, con el fin de contrastar los datos y reducir el sesgo derivado del uso de una sola fuente.

3.6 Selección de la metodología para la gestión de riesgos

En el Capítulo II se describieron tres metodologías reconocidas para la gestión de riesgos de seguridad de la información: ISO/IEC 27005:2022, MAGERIT v3 y OCTAVE Allegro. Para seleccionar la más adecuada al contexto de la EMMAIPC-EP se definieron seis criterios de decisión, derivados de los requisitos de la norma ISO/IEC 27001:2022 y de las condiciones reales de la institución. La Tabla 9 presenta la valoración comparativa, en la que se emplea una escala cualitativa de tres niveles: alto, medio y bajo.

Tabla 9

Matriz de selección de la metodología de gestión de riesgos

Criterio de selección	ISO/IEC 27005:2022	MAGERIT v3	OCTAVE Allegro
Alineación directa con los requisitos de la ISO/IEC 27001:2022	Alta: fue concebida como guía del proceso de riesgos del SGSI.	Media: se alinea a la ISO 31000 y requiere adaptación.	Media: enfoque organizacional, no estructurado por cláusulas.
Trazabilidad con el Anexo A y la Declaración de Aplicabilidad	Alta: vinculación nativa entre riesgos y controles del Anexo A.	Media: exige mapeo adicional entre salvaguardas y controles.	Baja: no contempla la Declaración de Aplicabilidad.
Dependencia de registros históricos de incidentes	Baja: admite valoración cualitativa por juicio experto.	Media: la estimación cuantitativa se robustece con datos históricos.	Baja: se sustenta en talleres y percepción del personal.
Recursos humanos y tiempo requeridos	Medios: proceso acotado y escalable.	Altos: catálogo extenso y valoración en cinco dimensiones.	Medios: requiere disponibilidad del personal para talleres.
Adecuación a una unidad de TI con un solo servidor técnico	Alta: puede aplicarse con apoyo de responsables funcionales.	Baja: demanda equipo multidisciplinario y herramienta especializada.	Media: depende de la participación sostenida de varias áreas.
Aporte al cumplimiento del marco normativo ecuatoriano	Alta: el EGSI toma como referencia la familia ISO/IEC 27000.	Media: aporte indirecto mediante el análisis de activos.	Media: aporte indirecto.

Nota. Elaboración propia.

Del análisis comparativo se desprende que la metodología ISO/IEC 27005:2022 constituye la opción más adecuada para el presente trabajo. Su selección se fundamenta en tres razones principales. En primer lugar, su integración nativa con la estructura de cláusulas y con el Anexo A de la ISO/IEC 27001:2022 garantiza la trazabilidad entre los riesgos identificados, los controles seleccionados y la Declaración de Aplicabilidad, documento exigido por el numeral 6.1.3 de la norma. En segundo lugar, la institución no dispone de registros históricos de incidentes de seguridad, condición reconocida entre las limitaciones de la investigación, lo que restringe la aplicación de estimaciones cuantitativas como las previstas por MAGERIT. En tercer lugar, la Unidad de Tecnologías de la Información y Comunicación cuenta con un solo servidor técnico, escenario en el que un proceso extenso de talleres o un catálogo de valoración de alta complejidad resultaría inviable.

No obstante, se incorpora como complemento el criterio de valoración de activos en dimensiones de seguridad propuesto por MAGERIT, restringido a las dimensiones de confidencialidad, integridad y disponibilidad, por su utilidad para justificar de manera explícita el nivel de importancia asignado a cada activo de información.

3.7 Fases para el diseño del SGSI basado en la norma ISO/IEC 27001:2022

El diseño del Sistema de Gestión de Seguridad de la Información se estructuró en cinco fases secuenciales, articuladas con los requisitos de las cláusulas 4 a 10 de la norma ISO/IEC 27001:2022 y con las etapas del ciclo PHVA descrito en el Capítulo II. La Tabla 10 detalla cada fase, su correspondencia normativa y el entregable resultante.

Tabla 10

Fases metodológicas para el diseño del SGSI

Fase	Actividades principales	Referencia normativa	Entregable
Fase 1. Diagnóstico y determinación del contexto	Análisis del contexto interno y externo, partes interesadas, requisitos legales, definición del alcance y evaluación del estado actual frente a la norma.	Cláusula 4; cláusula 5.2	Informe de diagnóstico, alcance del SGSI y análisis de brechas
Fase 2. Identificación y valoración de activos de información	Elaboración del inventario de activos, asignación de propietarios y custodios, y valoración en confidencialidad, integridad y disponibilidad.	Cláusula 6.1.2; ISO/IEC 27005:2022	Inventario valorado de activos de información

Fase	Actividades principales	Referencia normativa	Entregable
Fase 3. Análisis y evaluación de riesgos	Identificación de amenazas y vulnerabilidades, estimación de probabilidad e impacto, cálculo del nivel de riesgo y comparación con los criterios de aceptación.	Cláusula 6.1.2; ISO/IEC 27005:2022	Matriz de riesgos y mapa de calor
Fase 4. Tratamiento de riesgos y selección de controles	Definición de opciones de tratamiento, selección de controles del Anexo A conforme a la ISO/IEC 27002:2022, determinación de responsables y estimación del riesgo residual.	Cláusula 6.1.3; Anexo A	Plan de tratamiento de riesgos y Declaración de Aplicabilidad
Fase 5. Definición de políticas y modelo de implementación	Elaboración de la política general y de las políticas específicas, procedimientos, indicadores de desempeño y modelo de implementación bajo el ciclo PHVA.	Cláusulas 5, 7, 8, 9 y 10	Manual de políticas del SGSI y modelo de implementación

Nota. Elaboración propia con base en la norma ISO/IEC 27001:2022.

Las fases uno y dos se desarrollan parcialmente en el presente capítulo, mediante el diagnóstico de la situación actual y el levantamiento preliminar de activos; las fases tres, cuatro y cinco se desarrollan íntegramente en el Capítulo IV.

3.8 Contexto organizacional de la EMMAIPC-EP

3.8.1 Caracterización institucional

La EMMAIPC-EP presta servicios públicos de aseo integral en el ámbito territorial de los cuatro cantones mancomunados. Su gestión comprende procesos de barrido, recolección, transporte, disposición final y gestión ambiental, sustentados en procesos administrativos, financieros, documentales y tributarios que dependen de activos tecnológicos, sistemas de información, servicios en la nube, conectividad y datos institucionales.

El Plan Estratégico Institucional 2026–2030 define la estructura organizacional, el catálogo de servicios, la cadena de valor, los objetivos estratégicos, los indicadores y los riesgos institucionales, y constituye el marco de referencia con el cual debe alinearse el Sistema de Gestión de Seguridad de la Información propuesto. La continuidad de los servicios que presta la empresa depende de manera directa de la disponibilidad de sus sistemas de emisión, facturación y recaudación, así como de la integridad de la información de contribuyentes, contratos y catastro de residuos sólidos.

3.8.2 Estructura y capacidad de la Unidad de Tecnologías de la Información y Comunicación

La documentación institucional identifica a la Dirección Administrativa Financiera como área de adscripción y a la Unidad de Tecnologías de la Información y Comunicación como unidad técnica responsable de la gestión de infraestructura, sistemas, requerimientos y administración contractual de los servicios tecnológicos. La unidad está conformada por un único servidor público con el cargo de Analista de Tecnologías de la Información y Comunicación.

El inventario patrimonial asigna a este cargo quince activos tecnológicos, entre los que se encuentran el servidor institucional, el conmutador de núcleo, los conmutadores de acceso, los puntos de acceso inalámbrico, el rack, la unidad de almacenamiento en red, los sistemas de protección eléctrica y el sistema Flectra. Esta concentración de activos coincide con la concentración de responsabilidades técnicas críticas y configura una dependencia operativa de una sola persona, sin que la documentación evidencie segregación de funciones, personal de reemplazo, roles diferenciados de administración de infraestructura, aplicaciones, bases de datos o seguridad de la información, ni procedimientos documentados que permitan la continuidad del servicio ante su ausencia.

Adicionalmente, no se identifica en la estructura institucional un rol formalmente designado para la seguridad de la información, condición que la norma ISO/IEC 27001:2022 exige en su cláusula 5.3 relativa a roles, responsabilidades y autoridades de la organización.

3.9 Diagnóstico de la situación actual de la seguridad de la información

El diagnóstico se realizó sobre la información institucional disponible con corte al 30 de julio de 2026 y permitió establecer la línea base del estado de los activos de información, la infraestructura tecnológica, el portafolio de aplicaciones, la arquitectura de datos, los mecanismos de respaldo y el nivel de madurez de la seguridad de la información.

3.9.1 Inventario y estado de los activos tecnológicos

El inventario patrimonial registra noventa y un activos tecnológicos, con un valor histórico acumulado de USD 73.870,09. La Tabla 11 presenta su composición por categoría.

Tabla 11

Composición del inventario tecnológico por categoría

Categoría	Cantidad	Categoría	Cantidad
Computadores portátiles	22	Relojes biométricos	4
Impresoras	14	UPS y protección eléctrica	4
Dispositivos de rastreo satelital	11	Monitor y digitalización	2
Computadores de escritorio	10	Servidor	1
Almacenamiento	9	Software Flectra	1
Escáneres y equipos de diagnóstico	7	Total	91
Redes y rack	6		

Nota. Elaboración propia a partir del inventario patrimonial de activos fijos de la EMMAIPC-EP, corte al 24 de junio de 2026.

El estado de conservación y el ciclo de vida de los activos se presentan en la Tabla 12. Cincuenta y cuatro activos, equivalentes al 59,3 % del total, superaron la vida útil registrada en el inventario, con un valor histórico acumulado de USD 35.379,51.

Tabla 12

Estado de conservación y vida útil de los activos tecnológicos

Estado	Cantidad	Participación	Activos con vida útil superada
Bueno	53	58,2 %	18
Regular	18	19,8 %	16
Malo	19	20,9 %	19
Reposición	1	1,1 %	1
Total	91	100,0 %	54

Nota. Elaboración propia a partir del inventario patrimonial de la EMMAIPC-EP (2026b).

El 41,8 % de los activos se encuentra en estado regular, malo o en reposición, condición que compromete de manera directa la disponibilidad de los recursos que soportan los procesos institucionales. Respecto de los equipos de usuario final, la Tabla

13 evidencia que la mitad de los treinta y dos computadores registrados presenta un estado regular o malo, pese a la renovación efectuada en el año 2024.

Tabla 13

Estado de los equipos de usuario final

Tipo de equipo	Total	Bueno	Regular	Malo
Computadores de escritorio	10	7	0	3
Computadores portátiles	22	9	10	3
Total	32	16	10	6

Nota. Elaboración propia a partir del inventario patrimonial de la EMMAIPC-EP (2026b).

Desde la perspectiva de la seguridad de la información, la permanencia de equipos adquiridos entre los años 2009 y 2018 implica riesgos asociados a la imposibilidad de recibir actualizaciones de seguridad del sistema operativo, a la ausencia de soporte del fabricante y a la mayor probabilidad de fallas que afecten la disponibilidad e integridad de la información almacenada localmente.

3.9.2 Infraestructura de servidor, red y almacenamiento

La institución dispone de un único servidor físico, cuyas características registradas se detallan en la Tabla 14.

Tabla 14

Características del servidor institucional

Campo	Detalle
Código patrimonial	070
Equipo	Servidor HPE ML110 Gen10
Configuración registrada	16 GB de memoria RAM, disco de 1 TB, sistema operativo Windows Server 2016
Fecha de adquisición	20 de septiembre de 2019
Estado de conservación	Bueno
Vida útil registrada	3 años; superada al corte del inventario
Valor histórico	USD 3.052,00
Custodio	Analista de Tecnologías de la Información y Comunicación

Nota. Elaboración propia a partir del inventario patrimonial de la EMMAIPC-EP (2026b).

No se dispone de documentación que precise los servicios que ejecuta el servidor, su nivel de utilización, el estado de los discos, la política de actualizaciones, las

dependencias con otros sistemas ni la vigencia de la garantía, información indispensable para valorar adecuadamente el riesgo asociado a este activo.

La infraestructura de red fue fortalecida en abril de 2025 con la incorporación de un rack de piso, un conmutador de núcleo de capa 3 de cuarenta y ocho puertos y un punto de acceso de interiores. La Tabla 15 detalla los equipos de red identificados.

Tabla 15

Infraestructura de red y comunicaciones identificada

Código	Equipo	Marca	Estado	Adquisición
105	Conmutador de núcleo L3 de 48 puertos	HPE	Bueno	02/04/2025
106	Punto de acceso de interiores	HPE	Bueno	02/04/2025
104	Rack de piso	NEXXT	Bueno	02/04/2025
067	Punto de acceso dual-radio	UBIQUITI	Bueno	14/12/2018
068	Punto de acceso dual-radio	UBIQUITI	Reposición	14/12/2018
069	Conmutador de 24 puertos	HP	Bueno	22/04/2013

Nota. Elaboración propia a partir del inventario patrimonial de la EMMAIPC-EP (2026b).

La documentación no registra la existencia de un enrutador principal, un cortafuegos perimetral, el detalle de los enlaces de comunicación contratados, el direccionamiento lógico, la segmentación mediante redes virtuales, mecanismos de acceso remoto seguro, esquemas de redundancia ni herramientas de monitoreo. Tampoco se dispone de diagramas físicos ni lógicos de la red. Esta ausencia constituye una brecha crítica frente a los controles tecnológicos de la norma ISO/IEC 27002:2022 relativos a la seguridad de las redes y a la segregación en redes.

En materia de almacenamiento, el activo principal es una unidad de almacenamiento en red de cuatro bahías con un disco de 10 TB, adquirida en abril de 2025 y registrada en estado bueno, con un valor de USD 1.376,00. Complementariamente se registran ocho discos duros internos y externos distribuidos entre distintas unidades administrativas, de los cuales tres se encuentran en estado malo. La dispersión de información institucional en discos externos asignados a custodios individuales, sin cifrado ni control documentado, representa un riesgo relevante para la confidencialidad de la información.

3.9.3 Portafolio de aplicaciones y servicios en la nube

El portafolio de aplicaciones identificado se presenta en la Tabla 16, con indicación de su estado, cobertura funcional y criticidad.

Tabla 16

Portafolio de aplicaciones y sistemas de información

Código	Sistema	Estado	Cobertura funcional	Criticidad
APP-01	Flectra ERP 3.0	Producción	Core, Tesorería, Recaudación, Rentas, Contactos, Residuos Sólidos y Facturación Electrónica	Crítica
APP-02	e-Doc Manager	Activo	Creación, registro, tramitación, consulta y archivo de documentos físicos y digitales	Alta
APP-03	Portal web institucional	Por verificar	Información pública, transparencia y comunicación institucional	Media
APP-04	Sistema biométrico	Deteriorado	Control de asistencia del personal en las cuatro zonas operativas	Alta
APP-05	Sistema de rastreo satelital	Por verificar	Monitoreo de vehículos y maquinaria	Alta
APP-06	Jaltest	Regular	Diagnóstico de vehículos y maquinaria	Media
APP-07	Sistema de videovigilancia	Por verificar	Seguridad física y grabación	Media

Nota. Elaboración propia con base en el Diagnóstico Integral de Tecnologías de la Información de la EMMAIPC-EP (2026a).

Flectra ERP 3.0 constituye el sistema crítico de la institución. Fue puesto en producción el 11 de febrero de 2026, cuenta con garantía funcional hasta el 11 de febrero de 2027 y mantiene integraciones con dos plataformas externas de pago y recaudación. Su valor registrado como activo asciende a USD 9.500,00. Por su parte, e-Doc Manager opera bajo modalidad de software como servicio para veintitrés usuarios, con vigencia desde el 28 de junio de 2026 hasta el 27 de junio de 2027, e incluye respaldos, mantenimiento, parches y soporte funcional remoto en horario ocho por cinco.

La Tabla 17 resume las condiciones de los servicios en la nube identificados y el riesgo asociado a cada uno.

Tabla 17

Servicios en la nube y riesgo asociado

Servicio	Administración	Condición identificada	Riesgo
Flectra ERP	Infraestructura en nube pública bajo cuenta	Instancia con cuatro núcleos virtuales, 24 GB de memoria y	Muy alto: la institución no ejerce control directo sobre

Servicio	Administración	Condición identificada	Riesgo
	corporativa del proveedor implementador	sistema operativo Ubuntu Server 22.04 LTS, alojada en región extranjera	la cuenta, las credenciales, los respaldos ni la recuperación
e-Doc Manager	Servidores virtuales provistos y administrados por el proveedor del servicio	Propiedad de la información reconocida a favor de la EMMAIPC-EP según el certificado de suscripción	Alto: dependencia del proveedor; requiere plan de reversibilidad y prueba de exportación
Portal institucional	Proveedor no identificado en la documentación	Hosting, plataforma y responsable técnico no documentados	Medio: inventario técnico y contractual pendiente

Nota. Elaboración propia con base en el Diagnóstico Integral de Tecnologías de la Información de la EMMAIPC-EP (2026a).

La situación de Flectra ERP configura la brecha más crítica identificada. Al encontrarse la infraestructura bajo una cuenta corporativa de titularidad del proveedor, la EMMAIPC-EP no ejerce control administrativo sobre las credenciales privilegiadas, la configuración de seguridad, las copias de respaldo ni los procedimientos de recuperación del sistema que soporta la emisión, facturación y recaudación institucional. Esta condición contraviene los controles de la norma ISO/IEC 27002:2022 relativos a la seguridad en el uso de servicios en la nube y a la gestión de la seguridad de la información en las relaciones con proveedores.

3.9.4 Arquitectura de datos y asignación de responsabilidades

Se identificaron nueve fuentes de información institucional, cuya criticidad y responsabilidad funcional preliminar se detallan en la Tabla 18. La institución no dispone de un modelo formal de gobierno de datos que designe propietarios, custodios y administradores funcionales, ni de indicadores de calidad de datos en las dimensiones de completitud, exactitud, unicidad, consistencia, actualización, trazabilidad, integridad y disponibilidad.

Tabla 18

Fuentes de información institucional y criticidad

Fuente de información	Datos principales	Responsable preliminar	Criticidad
Flectra – Contactos y Residuos Sólidos	Usuarios, contribuyentes, contratos, medidores y servicios	Por formalizar	Crítica
Flectra – Rentas, Facturación, Recaudación y Tesorería	Emisiones, facturas, pagos, cartera y movimientos	Dirección Administrativa Financiera	Crítica

Fuente de información	Datos principales	Responsable preliminar	Criticidad
e-Doc Manager	Oficios, memorandos, solicitudes, anexos y expedientes	Unidades administrativas	Alta
Inventario de activos	Código, marca, serie, estado, ubicación, custodio y valor	Administrativo Financiero y Bodega	Alta
Rastreo satelital	Posición, recorridos y eventos de vehículos	Dirección Técnica	Alta
Sistemas biométricos	Registros de asistencia del personal	Talento Humano	Alta
Jaltest	Diagnóstico de vehículos y maquinaria	Unidad de Mantenimiento	Media
Videovigilancia	Grabaciones de seguridad física	Por definir	Media

Nota. Elaboración propia con base en el Diagnóstico Integral de Tecnologías de la Información de la EMMAIPC-EP (2026a).

La ausencia de propietarios formalmente designados es particularmente relevante para el diseño del SGSI, dado que la norma ISO/IEC 27001:2022 requiere que cada activo de información cuente con un propietario responsable de autorizar su uso, definir sus reglas de acceso y aprobar el tratamiento de los riesgos asociados. Adicionalmente, el tratamiento de datos de contribuyentes y de registros de asistencia del personal implica el procesamiento de datos personales, lo que activa las obligaciones establecidas en la Ley Orgánica de Protección de Datos Personales.

3.9.5 Respaldos y continuidad

La institución dispone de dos mecanismos de respaldo identificados: la unidad de almacenamiento en red adquirida en 2025 y los respaldos incluidos contractualmente en el servicio e-Doc Manager. Sin embargo, el estado de formalización de los procedimientos de copia y recuperación presenta vacíos significativos, según se detalla en la Tabla 19.

Tabla 19

Estado de los mecanismos de respaldo y recuperación

Información	Mecanismo de respaldo	Frecuencia	Prueba de restauración
Flectra ERP	Por verificar con el proveedor	Por verificar	No documentada
e-Doc Manager	Respaldos en línea y periódicos incluidos en el contrato	Durante la vigencia de la suscripción	No documentada
Archivos institucionales	Almacenamiento en red, por validar	Por definir	No documentada

Información	Mecanismo de respaldo	Frecuencia	Prueba de restauración
Configuraciones de equipos de red	Repositorio por definir	Posterior a cada cambio	No documentada

Nota. Elaboración propia con base en el Diagnóstico Integral de Tecnologías de la Información de la EMMAIPC-EP (2026a).

No existe una política institucional de respaldos que establezca alcance, frecuencia, retención, cifrado, custodia de copias externas, objetivos de tiempo de recuperación ni objetivos de punto de recuperación. Tampoco se registran pruebas de restauración ejecutadas ni evidencias documentales de su realización, lo que impide verificar la capacidad real de recuperación de los sistemas críticos ante un incidente.

3.9.6 Nivel de madurez de la seguridad de la información

Para establecer la línea base de madurez se aplicó una escala de capacidad de cero a cinco niveles, descrita en la Tabla 20, sobre diez dominios de gestión relacionados con la seguridad de la información. La valoración tiene carácter documental y preliminar, y no sustituye una evaluación formal bajo marcos como COBIT o CMMI.

Tabla 20

Escala de valoración de madurez aplicada

Nivel	Denominación	Interpretación
0	Inexistente	No se identifica práctica ni evidencia documental.
1	Inicial	La actividad se ejecuta de manera reactiva y depende de personas.
2	Gestionado parcialmente	Existen activos, responsables o documentos, pero falta estandarización y medición.
3	Definido	Existen procedimientos institucionales aprobados y aplicados.
4	Medido	Se dispone de indicadores y controles; las decisiones se basan en resultados.
5	Optimizado	Existe mejora continua, automatización y revisión sistemática.

Nota. Elaboración propia con base en el Diagnóstico Integral de Tecnologías de la Información de la EMMAIPC-EP (2026a).

Los resultados obtenidos por dominio se presentan en la Tabla 21.

Tabla 21

Valoración preliminar de madurez por dominio

Dominio	Nivel	Justificación
Gobierno y planificación de TI	1	Existe un Plan Estratégico Institucional, pero no se identifica plan estratégico de TI, comité, cartera de proyectos ni indicadores propios.
Gestión de activos	2	El inventario patrimonial está actualizado; faltan campos técnicos, criticidad, mantenimiento y ciclo de vida.
Infraestructura y red	2	Existen servidor, almacenamiento en red y equipos de red recientes; faltan arquitectura, monitoreo y gestión de configuración.
Gestión de aplicaciones	2	Los dos sistemas principales están documentados; falta portafolio completo y gestión de ciclo de vida.
Datos e información	1	Se identifican fuentes y propiedad contractual de datos; no existe gobierno integral ni métricas de calidad.
Soporte y gestión de servicios	1	No se identifica mesa de ayuda, catálogo de servicios, acuerdos de nivel de servicio internos ni base de conocimiento.
Seguridad de la información	1	Los riesgos se reconocen en documentos contractuales; no existen políticas, controles ni indicadores formales.
Continuidad y respaldos	2	Existen almacenamiento en red y respaldos del proveedor; no se documentan política, objetivos de recuperación ni pruebas.
Proveedores y contratos	2	Existen procesos, administradores y contratos; falta registro consolidado, acuerdos de nivel de servicio y evaluación.
Medición y mejora	1	El Plan Estratégico contempla indicadores institucionales, pero no se identifican indicadores propios de tecnología.
Promedio general	1,5	Nivel inicial con prácticas parcialmente gestionadas.

Nota. Elaboración propia con base en el Diagnóstico Integral de Tecnologías de la Información de la EMMAIPC-EP (2026a).

El promedio general de 1,5 sobre 5 ubica a la institución en un nivel inicial con prácticas parcialmente gestionadas. El dominio de seguridad de la información alcanza el nivel más bajo de la escala aplicada, junto con gobierno de TI, gestión de datos, soporte de servicios y medición, lo que confirma la pertinencia del diseño de un Sistema de Gestión de Seguridad de la Información como mecanismo de formalización institucional.

3.10 Indicadores de línea base

A partir del diagnóstico se consolidaron los indicadores que constituyen la línea base sobre la cual se medirá el aporte de la propuesta. La Tabla 22 sintetiza estos valores.

Tabla 22

Indicadores de línea base de la seguridad de la información

Indicador	Valor a julio de 2026
Activos tecnológicos registrados	91
Valor histórico total de los activos	USD 73.870,09
Activos en estado regular, malo o en reposición	38 (41,8 %)
Activos con vida útil patrimonial superada	54 (59,3 %), por USD 35.379,51
Equipos de usuario final en estado regular o malo	16 de 32 (50,0 %)
Sistemas biométricos operativos	0 de 4
Aplicaciones críticas para la continuidad institucional	2 (Flectra ERP y e-Doc Manager)
Servicios en la nube bajo cuenta administrativa institucional	0 de 2
Políticas de seguridad de la información aprobadas	0
Procedimientos de respaldo documentados	0
Pruebas de restauración ejecutadas y evidenciadas	0
Registros históricos de incidentes de seguridad	No disponibles
Inventario técnico de activos de información	No disponible
Diagramas físico y lógico de red	No disponibles
Rol de seguridad de la información designado	No designado
Personal técnico asignado a la Unidad de TIC	1 servidor
Nivel de madurez preliminar	1,5 / 5
Riesgos y brechas priorizadas identificadas	11 (2 de nivel muy alto, 6 alto y 3 medio-alto)

Nota. Elaboración propia con base en el Diagnóstico Integral de Tecnologías de la Información de la EMMAIPC-EP (2026a).

3.11 Análisis e interpretación de los resultados

El diagnóstico evidencia que la EMMAIPC-EP dispone de una base tecnológica funcional, reforzada por las inversiones efectuadas entre 2024 y 2026 en equipos de usuario final, infraestructura de red, almacenamiento y sistemas de información. Sin embargo, esta capacidad instalada coexiste con una gestión de la seguridad de la

información de carácter informal, reactiva y dependiente de una sola persona, sin políticas aprobadas, sin controles documentados y sin indicadores que permitan medir su desempeño.

Al contrastar los hallazgos con los cuatro temas de controles establecidos en la norma ISO/IEC 27002:2022, se obtiene el panorama de brechas presentado en la Tabla 23.

Tabla 23

Brechas identificadas frente a los temas de controles de la ISO/IEC 27002:2022

Tema de controles	Brechas identificadas	Prioridad
Controles organizacionales (37 controles)	Ausencia de política de seguridad de la información; roles y responsabilidades no definidos; inventario de activos de información inexistente; falta de clasificación de la información; gestión de proveedores sin cláusulas de seguridad ni acuerdos de nivel de servicio; ausencia de gestión de incidentes y de continuidad; falta de control institucional sobre el servicio en la nube crítico.	Muy alta
Controles de personas (8 controles)	No se evidencian acuerdos de confidencialidad, procedimientos de alta y baja de accesos, programas de concienciación ni segregación de funciones en la unidad técnica.	Alta
Controles físicos (14 controles)	No se documentan controles de acceso al área que aloja el servidor y los equipos de red; dos de los cuatro sistemas de protección eléctrica se encuentran en estado malo; existen activos con vida útil superada sin plan de baja segura ni borrado de información.	Alta
Controles tecnológicos (34 controles)	No se identifica cortafuegos perimetral, segmentación de red, gestión de identidades y accesos privilegiados, gestión de vulnerabilidades y parches, registro y monitoreo de eventos, cifrado de la información ni respaldos verificados mediante pruebas de restauración.	Muy alta

Nota. Elaboración propia con base en la norma ISO/IEC 27002:2022 y el diagnóstico institucional.

La interpretación de estos resultados permite establecer tres conclusiones parciales. En primer lugar, las brechas de mayor severidad no son de naturaleza tecnológica sino organizacional: la institución carece del marco normativo interno, de los roles y de los procedimientos que dan sentido a los controles técnicos, por lo que la adquisición de equipamiento adicional no resolvería por sí sola la exposición identificada.

En segundo lugar, la dependencia respecto de terceros constituye el riesgo individual más alto. El sistema que sostiene la emisión, facturación y recaudación institucional opera sobre una infraestructura cuya cuenta administrativa pertenece al proveedor, lo que implica que la disponibilidad y la recuperabilidad de la información tributaria de la empresa dependen de decisiones y controles ajenos a la institución.

En tercer lugar, la concentración de funciones críticas en un único servidor técnico, sin segregación de responsabilidades, personal de reemplazo ni documentación de procedimientos, configura un riesgo de continuidad que afecta simultáneamente a los tres principios de la seguridad de la información, dado que la ausencia temporal o definitiva de ese servidor comprometería la capacidad de administrar accesos, restaurar respaldos y responder ante incidentes.

3.12 Implicaciones para el diseño del Sistema de Gestión de Seguridad de la Información

Los resultados del diagnóstico determinan las prioridades que orientan el diseño desarrollado en el Capítulo IV. El alcance del SGSI debe centrarse en los procesos administrativos, financieros, documentales y tributarios soportados por Flectra ERP y e-Doc Manager, así como en la infraestructura de servidor, red y almacenamiento que los sustenta, por ser los activos cuya afectación compromete de manera directa la continuidad de los servicios institucionales.

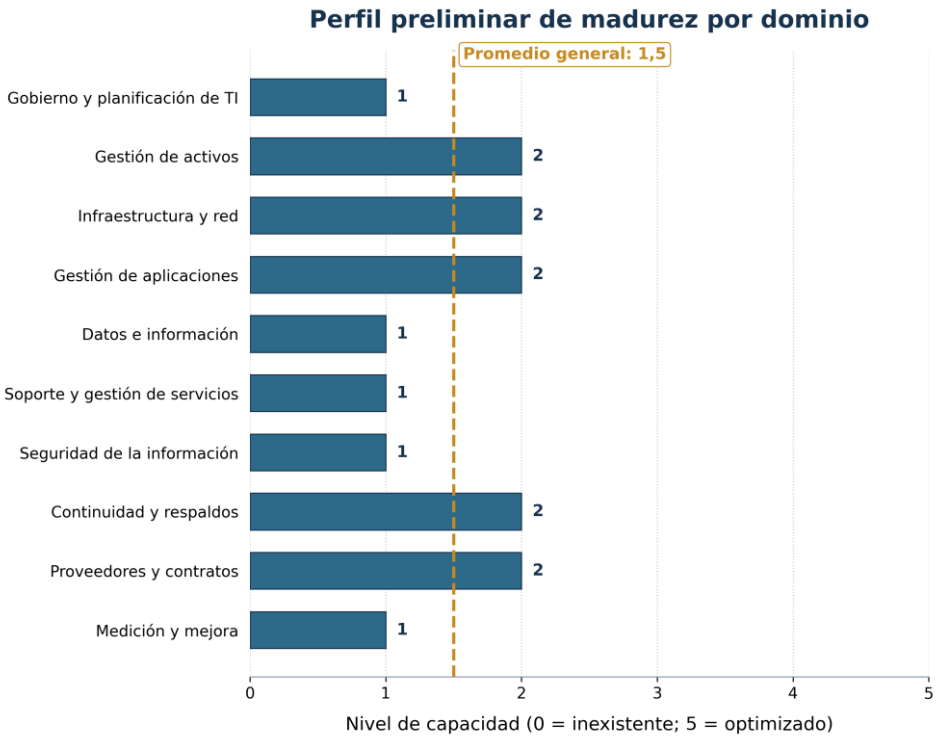
El inventario valorado de activos de información debe construirse a partir del inventario patrimonial existente, incorporando los campos técnicos ausentes y la valoración en las dimensiones de confidencialidad, integridad y disponibilidad. El análisis de riesgos debe abordar de manera prioritaria la dependencia respecto de los servicios en la nube, la ausencia de respaldos verificados, la concentración de funciones en la unidad técnica y el estado de obsolescencia de los activos.

La selección de controles debe privilegiar los controles organizacionales y de personas, por ser los que presentan mayor brecha y menor requerimiento de inversión, sin desatender los controles tecnológicos asociados a la seguridad de redes, la gestión de accesos y la protección de las copias de respaldo. Finalmente, el modelo de implementación bajo el ciclo PHVA debe incorporar indicadores que permitan medir el avance respecto de la línea base establecida en la Tabla 22, de modo que la institución

pueda verificar objetivamente el progreso del sistema una vez que decida su implementación.

Figura 5

Perfil preliminar de madurez de la seguridad de la información en la EMMAIPC-EP.



Nota. Elaboración propia con base en EMMAIPC-EP (2026a).

CAPÍTULO IV

4 PROPUESTA

4.1 Título de la propuesta

Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2022 para la EMMAIPC-EP.

4.2 Presentación

El presente capítulo desarrolla la propuesta de diseño del Sistema de Gestión de Seguridad de la Información para la EMMAIPC-EP, construida sobre los resultados del diagnóstico presentado en el Capítulo III. La propuesta se estructura conforme a las fases metodológicas definidas en la Tabla 10 y aplica la metodología ISO/IEC 27005:2022 para la gestión de riesgos, seleccionada mediante la matriz de decisión de la Tabla 9.

El desarrollo comprende la determinación del alcance del sistema, el inventario valorado de activos de información, el análisis y evaluación de riesgos, el plan de tratamiento con la selección de controles del Anexo A de la norma, la Declaración de Aplicabilidad, el cuerpo de políticas institucionales y el modelo de implementación bajo el ciclo Planificar, Hacer, Verificar y Actuar. El capítulo concluye con la verificación de la cobertura riesgo–control, la comprobación del cumplimiento de los requisitos normativos.

Conforme a las delimitaciones establecidas en el Capítulo I, la propuesta comprende el diseño documental del sistema y no su ejecución operativa, la realización de auditorías internas ni el proceso de certificación.

4.3 Objetivo de la propuesta

Diseñar un Sistema de Gestión de Seguridad de la Información conforme a los requisitos de la norma ISO/IEC 27001:2022, que permita a la EMMAIPC-EP gestionar de manera sistemática los riesgos sobre sus activos de información y fortalecer la confidencialidad, integridad y disponibilidad de la información institucional.

De manera específica, la propuesta busca:

- Establecer el alcance, el contexto y las partes interesadas del Sistema de Gestión de Seguridad de la Información.
- Elaborar el inventario valorado de los activos de información críticos de la institución.
- Determinar el nivel de riesgo de dichos activos y definir los criterios de aceptación aplicables.
- Seleccionar los controles del Anexo A que reducen los riesgos a niveles aceptables y documentarlos en la Declaración de Aplicabilidad.
- Definir el cuerpo de políticas, la estructura de roles y el modelo de implementación con sus indicadores de desempeño.

4.4 Justificación de la propuesta

El diagnóstico determinó un nivel de madurez preliminar de 1,5 sobre 5 y evidenció la ausencia total de políticas de seguridad aprobadas, procedimientos de respaldo documentados, pruebas de restauración y un rol formalmente designado para la seguridad de la información. Simultáneamente, identificó que el sistema que sostiene la emisión, facturación y recaudación institucional opera sobre una infraestructura en la nube cuya cuenta administrativa pertenece a un tercero.

Esta combinación configura una exposición que no se resuelve mediante adquisiciones tecnológicas aisladas, sino mediante la implantación de un marco de gestión que asigne responsabilidades, establezca reglas verificables y permita medir su cumplimiento. El diseño de un Sistema de Gestión de Seguridad de la Información responde a esa necesidad y, adicionalmente, contribuye al cumplimiento de las obligaciones que la Ley Orgánica de Protección de Datos Personales impone a la institución en su calidad de responsable del tratamiento de datos de contribuyentes y de su propio personal, así como a los lineamientos del Esquema Gubernamental de Seguridad de la Información aplicables al sector público ecuatoriano.

4.5 Fase 1: Contexto, partes interesadas y alcance del SGSI

4.5.1 Contexto interno y externo

En cumplimiento del numeral 4.1 de la norma, se determinaron las cuestiones internas y externas pertinentes para el propósito del sistema. En el ámbito interno, la institución presenta una unidad técnica conformada por un solo servidor público, una infraestructura tecnológica heterogénea en la que coexisten activos recientes con equipos que superaron su vida útil, dos sistemas críticos operados bajo modalidad de servicio contratado y un Plan Estratégico Institucional 2026–2030 que constituye el marco de alineación de cualquier iniciativa tecnológica.

En el ámbito externo, la institución está sujeta al régimen jurídico de las empresas públicas, a la Ley Orgánica de Protección de Datos Personales, al Esquema Gubernamental de Seguridad de la Información y al control de los organismos competentes; asimismo, depende de proveedores externos para la operación de sus dos sistemas principales, del servicio de conectividad y del suministro eléctrico, factores que condicionan directamente la disponibilidad de la información.

4.5.2 Partes interesadas y requisitos

Conforme al numeral 4.2 de la norma, la Tabla 24 identifica las partes interesadas pertinentes y sus requisitos en materia de seguridad de la información.

Tabla 24

Partes interesadas y requisitos de seguridad de la información

Parte interesada	Requisito identificado	Origen del requisito
Gerencia General y Directorio	Continuidad de los servicios institucionales y protección del patrimonio informativo.	Plan Estratégico Institucional 2026–2030
Contribuyentes y usuarios del servicio	Confidencialidad y exactitud de sus datos personales, contratos y estados de cuenta.	Ley Orgánica de Protección de Datos Personales
Personal de la institución	Protección de los datos personales y de los registros de asistencia; reglas claras de uso de los recursos tecnológicos.	LOPDP; normativa interna
Dirección Administrativa Financiera	Integridad y disponibilidad de la información de emisión, facturación, recaudación y tesorería.	Normativa financiera pública

Parte interesada	Requisito identificado	Origen del requisito
Organismos de control del Estado	Disponibilidad, integridad y conservación de registros sujetos a control y auditoría.	Normativa de control gubernamental
Entidad rectora de gobierno digital	Aplicación de los lineamientos de seguridad de la información del sector público.	Esquema Gubernamental de Seguridad de la Información
Proveedores de servicios tecnológicos	Condiciones contractuales claras sobre seguridad, niveles de servicio, propiedad de la información y reversibilidad.	Instrumentos contractuales vigentes
Municipios mancomunados	Confiabilidad de la información reportada sobre la prestación del servicio.	Convenio de mancomunidad

Nota. Elaboración propia con base en la norma ISO/IEC 27001:2022, numeral 4.2.

4.5.3 Declaración de alcance del SGSI

El alcance del Sistema de Gestión de Seguridad de la Información de la EMMAIPC-EP comprende los procesos administrativos, financieros, tributarios y documentales soportados por los sistemas Flectra ERP 3.0 y e-Doc Manager, así como la infraestructura de servidor, red, almacenamiento y equipos de usuario final que los sustenta, en las instalaciones de la matriz institucional y en las cuatro zonas operativas. La Tabla 25 precisa las inclusiones y exclusiones.

Tabla 25

Alcance del Sistema de Gestión de Seguridad de la Información

Dimensión	Incluido	Excluido
Procesos	Registro de usuarios y contratos, catastro de residuos, determinación y emisión de tasas, facturación electrónica, recaudación, tesorería y gestión documental.	Procesos operativos de barrido, recolección y disposición final en sus aspectos no informáticos.
Sistemas	Flectra ERP 3.0, e-Doc Manager, sistemas biométricos, rastreo satelital y portal institucional.	Plataformas de terceros no contratadas por la institución.
Infraestructura	Servidor institucional, equipos de red, almacenamiento en red, protección eléctrica, equipos de usuario final y servicios en la nube contratados.	Infraestructura propia de los municipios mancomunados.

Dimensión	Incluido	Excluido
Ubicaciones	Matriz institucional y unidades técnicas de las zonas A, B, C y D.	Instalaciones de proveedores, salvo por las obligaciones contractuales de seguridad.
Información	Datos de contribuyentes, contratos, emisiones, facturación, recaudación, expedientes documentales, registros de asistencia y datos de flota.	Información de carácter estrictamente personal de los servidores no vinculada a procesos institucionales.

Nota. Elaboración propia con base en la norma ISO/IEC 27001:2022, numeral 4.3.

4.6 Fase 2: Inventario valorado de activos de información

4.6.1 Escala de valoración

La valoración de los activos se realizó en las tres dimensiones de seguridad establecidas por la norma, mediante la escala ordinal de cinco niveles descrita en la Tabla 26. El valor del activo corresponde al mayor de los tres valores dimensionales, criterio que garantiza que la protección se dimensione en función de la propiedad más sensible de cada activo.

Tabla 26

Escala de valoración de activos de información

Nivel	Denominación	Confidencialidad	Integridad	Disponibilidad
1	Muy bajo	Información pública.	Un error no genera consecuencias.	La indisponibilidad no afecta procesos.
2	Bajo	Uso interno sin sensibilidad.	Un error se detecta y corrige fácilmente.	Tolera indisponibilidad de varios días.
3	Medio	Divulgación causaría molestia administrativa.	Un error afecta un proceso puntual.	Tolera indisponibilidad de hasta un día.
4	Alto	Divulgación afectaría a personas o a la institución.	Un error afecta decisiones o reportes oficiales.	Tolera indisponibilidad de pocas horas.
5	Muy alto	Divulgación implicaría infracción a la LOPDP o daño reputacional grave.	Un error compromete la validez de actos administrativos o tributarios.	La indisponibilidad detiene la prestación del servicio.

Nota. Elaboración propia con base en la norma ISO/IEC 27005:2022 y el criterio dimensional de MAGERIT v3.

4.6.2 Inventario valorado

La Tabla 27 presenta el inventario de activos de información construido a partir del inventario patrimonial institucional y del portafolio de aplicaciones identificado en el

diagnóstico, agrupado por tipo de activo conforme a la clasificación de la ISO/IEC 27005:2022.

Tabla 27

Inventario valorado de activos de información

Código	Activo de información	Tipo	C	I	D	Valor	Propietario propuesto
AC-01	Base de datos de contribuyentes, contratos y catastro de residuos	Información	5	5	5	5	Dirección Técnica
AC-02	Registros de emisión, facturación, recaudación y cartera	Información	5	5	5	5	Dirección Administrativa Financiera
AC-03	Expedientes y documentos institucionales	Información	4	5	4	5	Secretaría General
AC-04	Registros de asistencia del personal	Información	4	4	3	4	Dirección de Talento Humano
AC-05	Datos de recorridos y eventos de la flota	Información	3	3	3	3	Dirección Técnica
AC-06	Inventario patrimonial de activos	Información	3	4	3	4	Dirección Administrativa Financiera
AC-07	Copias de respaldo institucionales	Información	5	5	4	5	Unidad de TIC
AC-08	Configuraciones de los equipos de red	Información	4	4	4	4	Unidad de TIC
AC-09	Aplicación Flectra ERP 3.0	Software	5	5	5	5	Dirección Administrativa Financiera
AC-10	Aplicación e-Doc Manager	Software	4	4	4	4	Secretaría General
AC-11	Portal web institucional	Software	2	4	3	4	Comunicación Social
AC-12	Servidor institucional HPE ML110 Gen10	Hardware	4	4	4	4	Unidad de TIC
AC-13	Instancia en la nube que aloja Flectra ERP	Servicio	5	5	5	5	Unidad de TIC
AC-14	Almacenamiento en red de cuatro bahías	Hardware	5	5	4	5	Unidad de TIC
AC-15	Equipos de red: conmutadores y puntos de acceso	Hardware	3	4	5	5	Unidad de TIC
AC-16	Equipos de usuario final (32 computadores)	Hardware	4	3	3	4	Unidad de TIC
AC-17	Sistemas biométricos de control de asistencia	Hardware	3	4	2	4	Dirección de Talento Humano
AC-18	Servicio de conectividad a internet	Servicio	2	2	5	5	Unidad de TIC
AC-19	Suministro eléctrico y sistemas de respaldo de energía	Servicio	1	2	5	5	Dirección Administrativa Financiera

Código	Activo de información	Tipo	C	I	D	Valor	Propietario propuesto
AC-20	Conocimiento técnico del personal de la Unidad de TIC	Personas	4	4	5	5	Dirección Administrativa Financiera
AC-21	Área física que aloja el servidor y el rack de comunicaciones	Instalaciones	4	3	4	4	Unidad de TIC

Nota. Elaboración propia con base en el inventario patrimonial de la EMMAIPC-EP (2026b). y la norma ISO/IEC 27005:2022.

Del total de veintiún activos de información inventariados, once alcanzan el valor máximo de la escala y nueve el nivel alto, lo que confirma que la mayor parte de los recursos incluidos en el alcance sostiene procesos cuya interrupción o alteración afectaría de manera directa la prestación del servicio público o el cumplimiento de obligaciones legales.

4.7 Fase 3: Análisis y evaluación de riesgos

4.7.1 Criterios de probabilidad, impacto y aceptación

El nivel de riesgo se determinó mediante el producto entre la probabilidad de ocurrencia y el impacto sobre el activo, conforme a las escalas descritas en la Tabla 28.

Tabla 28

Escalas de probabilidad e impacto

Nivel	Probabilidad	Impacto
1	Muy baja: no se han registrado eventos y existen controles efectivos.	Muy bajo: efecto imperceptible en el proceso.
2	Baja: podría ocurrir excepcionalmente.	Bajo: afectación menor y recuperable en el día.
3	Media: podría ocurrir alguna vez al año.	Medio: interrupción parcial de un proceso institucional.
4	Alta: es probable que ocurra varias veces al año.	Alto: interrupción de un proceso crítico o afectación a datos personales.
5	Muy alta: ocurre con frecuencia o la condición ya está presente.	Muy alto: detención del servicio, pérdida irrecuperable de información o incumplimiento legal.

Nota. Elaboración propia con base en la norma ISO/IEC 27005:2022.

La combinación de ambas escalas genera la matriz de calor presentada en la Tabla 29, que clasifica el riesgo en cuatro niveles: bajo, de 1 a 4; medio, de 5 a 9; alto, de 10 a 14; y muy alto, de 15 a 25.

Tabla 29

Matriz de nivel de riesgo

Probabilidad	Impacto 1	Impacto 2	Impacto 3	Impacto 4	Impacto 5
5 – Muy alta	5 Medio	10 Alto	15 Muy alto	20 Muy alto	25 Muy alto
4 – Alta	4 Bajo	8 Medio	12 Alto	16 Muy alto	20 Muy alto
3 – Media	3 Bajo	6 Medio	9 Medio	12 Alto	15 Muy alto
2 – Baja	2 Bajo	4 Bajo	6 Medio	8 Medio	10 Alto
1 – Muy baja	1 Bajo	2 Bajo	3 Bajo	4 Bajo	5 Medio

Nota. Elaboración propia.

El criterio de aceptación del riesgo se estableció en un valor igual o menor a seis. Los riesgos que superen ese umbral requieren tratamiento obligatorio; los riesgos residuales que permanezcan por encima del umbral deberán ser aceptados formalmente por la Gerencia General y sometidos a seguimiento trimestral, conforme al numeral 6.1.3 literal f de la norma.

4.7.2 Matriz de identificación y evaluación de riesgos

La Tabla 30 presenta los dieciséis riesgos identificados sobre los activos de información incluidos en el alcance, derivados de las brechas determinadas en el diagnóstico.

Tabla 30

Matriz de identificación y evaluación de riesgos

ID	Activo	Amenaza	Vulnerabilidad	P	I	R	Nivel
RG-01	AC-13, AC-09	Pérdida de control o indisponibilidad del servicio en la nube	La cuenta administrativa de la infraestructura pertenece al proveedor	4	5	20	Muy alto
RG-02	AC-07, AC-01, AC-02	Pérdida irrecuperable de información	Ausencia de política de respaldos y de pruebas de restauración	4	5	20	Muy alto
RG-03	AC-15, AC-12	Intrusión externa en la red institucional	No se documenta cortafuegos perimetral ni segmentación de red	4	5	20	Muy alto
RG-04	AC-20	Indisponibilidad de la administración tecnológica	Concentración de funciones críticas en un solo servidor técnico	4	4	16	Muy alto

ID	Activo	Amenaza	Vulnerabilidad	P	I	R	Nivel
RG-05	AC-09, AC-10, AC-13	Uso indebido de credenciales privilegiadas	Ausencia de gestión de identidades y de revisión de accesos	3	5	15	Muy alto
RG-06	AC-16, AC-12	Falla de equipos y pérdida de disponibilidad	54 activos con vida útil superada y sin soporte del fabricante	4	3	12	Alto
RG-07	AC-09, AC-12, AC-16	Explotación de vulnerabilidades conocidas	Ausencia de gestión de vulnerabilidades y de actualización de parches	3	4	12	Alto
RG-08	AC-01, AC-02	Fuga de información y datos personales	Información dispersa en discos externos sin cifrado ni control	3	4	12	Alto
RG-09	AC-04, AC-17	Pérdida de integridad de los registros de asistencia	Los cuatro dispositivos biométricos se encuentran en estado malo	4	3	12	Alto
RG-10	AC-09, AC-10	Interrupción del servicio por incumplimiento del proveedor	Contratos sin cláusulas de seguridad ni acuerdos de nivel de servicio	3	4	12	Alto
RG-11	AC-09, AC-13	Incidentes no detectados oportunamente	Ausencia de registro y monitoreo de eventos de seguridad	4	3	12	Alto
RG-12	AC-16, AC-01	Suplantación de identidad y error humano	Ausencia de programa de concienciación en seguridad	4	3	12	Alto
RG-13	AC-01, AC-04	Tratamiento indebido de datos personales	Ausencia de propietarios de datos y de clasificación de la información	3	4	12	Alto
RG-14	AC-21, AC-12	Acceso físico no autorizado a los equipos	No se documentan controles de acceso al área de servidores	2	4	8	Medio
RG-15	AC-19, AC-12	Interrupción del suministro eléctrico	Dos de los cuatro sistemas de protección eléctrica están en estado malo	3	3	9	Medio
RG-16	AC-09, AC-10	Interrupción por vencimiento de suscripciones y garantías	Ausencia de calendario institucional de renovaciones	2	4	8	Medio

Nota. Elaboración propia con base en el diagnóstico institucional y la norma ISO/IEC 27005:2022.

4.7.3 Resultados de la evaluación

La distribución de los riesgos por nivel se presenta en la Tabla 31. Ningún riesgo identificado se ubica en el nivel bajo y la totalidad supera el umbral de aceptación establecido, lo que confirma la necesidad de tratamiento para los dieciséis casos.

Tabla 31

Distribución de los riesgos identificados por nivel

Nivel de riesgo	Cantidad	Participación	Decisión
Muy alto (15–25)	5	31,2 %	Tratamiento inmediato y prioritario
Alto (10–14)	8	50,0 %	Tratamiento en el primer año
Medio (5–9)	3	18,8 %	Tratamiento programado
Bajo (1–4)	0	0,0 %	No aplica
Total	16	100,0 %	

Nota. Elaboración propia.

Los cinco riesgos de nivel muy alto se concentran en tres condiciones estructurales: la dependencia respecto de un tercero para la operación del sistema crítico, la ausencia de un esquema verificado de respaldo y recuperación, y la falta de controles perimetrales y de gestión de accesos. Estas tres condiciones concentran, por sí solas, la mayor parte de la exposición institucional y determinan el orden de prioridad del plan de tratamiento.

4.8 Fase 4: Tratamiento de riesgos y selección de controles

4.8.1 Opciones de tratamiento aplicadas

Para cada riesgo se seleccionó una de las cuatro opciones previstas por la norma ISO/IEC 27005:2022: modificar el riesgo mediante la aplicación de controles, compartirlo con un tercero, evitarlo eliminando la actividad que lo genera o retenerlo cuando su nivel resulte aceptable. En el presente diseño predomina la modificación del riesgo, dado que las actividades que lo originan son consustanciales a la prestación del servicio público y no pueden ser eliminadas.

4.8.2 Plan de tratamiento de riesgos

La Tabla 32 presenta el plan de tratamiento, con los controles del Anexo A de la norma ISO/IEC 27001:2022 seleccionados para cada riesgo, el responsable de su implementación y el riesgo residual estimado tras la aplicación de los controles.

Tabla 32

Plan de tratamiento de riesgos y controles seleccionados

ID	Opción	Controles del Anexo A seleccionados	Responsable	Riesgo residual
RG-01	Modificar	A.5.19, A.5.20, A.5.21, A.5.22, A.5.23, A.8.13	Dirección Administrativa Financiera y Unidad de TIC	5 – Medio
RG-02	Modificar	A.5.29, A.5.30, A.5.33, A.8.13, A.8.14	Unidad de TIC	5 – Medio
RG-03	Modificar	A.8.20, A.8.21, A.8.22, A.8.23, A.8.16	Unidad de TIC	8 – Medio
RG-04	Modificar	A.5.2, A.5.3, A.5.4, A.5.37, A.6.5	Gerencia General y Talento Humano	8 – Medio
RG-05	Modificar	A.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.5	Unidad de TIC	5 – Medio
RG-06	Modificar	A.5.9, A.7.13, A.7.14, A.8.1	Unidad de TIC y Bodega	6 – Medio
RG-07	Modificar	A.8.7, A.8.8, A.8.9, A.8.19, A.8.32	Unidad de TIC	6 – Medio
RG-08	Modificar	A.5.12, A.5.13, A.5.14, A.7.10, A.8.10, A.8.12, A.8.24	Unidad de TIC y propietarios de datos	4 – Bajo
RG-09	Modificar	A.5.9, A.7.8, A.7.13, A.8.1	Dirección de Talento Humano y Unidad de TIC	3 – Bajo
RG-10	Compartir y modificar	A.5.19, A.5.20, A.5.22, A.5.31	Procuraduría Síndica y Unidad de TIC	6 – Medio
RG-11	Modificar	A.5.7, A.5.24, A.5.25, A.5.26, A.5.27, A.8.15, A.8.16	Unidad de TIC	6 – Medio
RG-12	Modificar	A.6.3, A.6.6, A.6.8, A.7.7, A.8.23	Dirección de Talento Humano y Unidad de TIC	6 – Medio
RG-13	Modificar	A.5.9, A.5.10, A.5.12, A.5.34, A.5.36	Propietarios de datos y Unidad de TIC	6 – Medio
RG-14	Modificar	A.7.1, A.7.2, A.7.3, A.7.4, A.7.6	Unidad de TIC y Dirección Administrativa Financiera	4 – Bajo
RG-15	Modificar	A.7.5, A.7.11, A.7.12, A.8.14	Dirección Administrativa Financiera	3 – Bajo
RG-16	Modificar	A.5.20, A.5.22, A.5.31, A.5.37	Unidad de TIC y Compras Públicas	4 – Bajo

Nota. Elaboración propia con base en el Anexo A de la norma ISO/IEC 27001:2022.

Tras la aplicación de los controles, catorce de los dieciséis riesgos alcanzan un nivel residual igual o inferior al umbral de aceptación establecido. Los riesgos RG-03, relativo a la seguridad perimetral de la red, y RG-04, relativo a la concentración de funciones en la unidad técnica, permanecen en un valor residual de ocho, por encima del umbral, debido a que su reducción completa depende respectivamente de una inversión en equipamiento de seguridad y de una decisión de fortalecimiento del talento humano

que exceden el alcance del diseño. Ambos deberán ser aceptados formalmente por la Gerencia General y sometidos a seguimiento trimestral hasta que las condiciones institucionales permitan su tratamiento definitivo.

4.8.3 Declaración de Aplicabilidad

La Declaración de Aplicabilidad constituye el documento exigido por el numeral 6.1.3 literal d de la norma y registra los controles aplicables, su justificación y el estado de implementación. La Tabla 33 presenta el resumen por tema de controles.

Tabla 33

Resumen de la Declaración de Aplicabilidad por tema de controles

Tema de controles	Total	Aplicables	Excluidos	Implementados	No implementados
A.5 Controles organizacionales	37	37	0	2	35
A.6 Controles de personas	8	8	0	1	7
A.7 Controles físicos	14	14	0	3	11
A.8 Controles tecnológicos	34	27	7	4	23
Total	93	86	7	10	76

Nota. Elaboración propia con base en el Anexo A de la norma ISO/IEC 27001:2022 y el diagnóstico institucional.

De los noventa y tres controles del Anexo A, ochenta y seis resultan aplicables al alcance definido, lo que representa el 92,5 %. Únicamente diez controles se encuentran implementados de manera total o parcial al momento del diagnóstico, correspondientes en su mayoría a medidas físicas y a servicios incluidos contractualmente en las plataformas contratadas, lo que evidencia un grado de cumplimiento del 11,6 % respecto de los controles aplicables. La Tabla 34 detalla los controles excluidos y su justificación.

Tabla 34

Controles excluidos de la Declaración de Aplicabilidad

Control	Denominación	Justificación de la exclusión
A.8.4	Acceso al código fuente	La institución no desarrolla ni mantiene código fuente propio; los sistemas son adquiridos como servicio.
A.8.25	Ciclo de vida de desarrollo seguro	No se ejecutan actividades de desarrollo de software dentro del alcance.

Control	Denominación	Justificación de la exclusión
A.8.27	Principios de ingeniería y arquitectura de sistemas seguros	No se diseñan ni construyen sistemas de información propios.
A.8.28	Codificación segura	No existe actividad de programación dentro del alcance definido.
A.8.29	Pruebas de seguridad en desarrollo y aceptación	No se realizan pruebas de desarrollo; la aceptación se rige por los procedimientos contractuales.
A.8.31	Separación de los entornos de desarrollo, prueba y producción	La institución no administra entornos de desarrollo ni de prueba.
A.8.33	Información de prueba	No se generan ni utilizan conjuntos de datos de prueba dentro del alcance.

Nota. Elaboración propia con base en el Anexo A de la norma ISO/IEC 27001:2022.

Se advierte que el control A.8.30, relativo al desarrollo subcontratado, se mantiene aplicable, dado que los sistemas Flectra ERP y e-Doc Manager fueron provistos por terceros bajo instrumentos contractuales.

4.9 Fase 5: Políticas y modelo de implementación

4.9.1 Política general de seguridad de la información

La EMMAIPC-EP reconoce la información como un activo estratégico para la prestación del servicio público de aseo integral y se compromete a preservar su confidencialidad, integridad y disponibilidad mediante un Sistema de Gestión de Seguridad de la Información conforme a la norma ISO/IEC 27001:2022. Para ello, la institución asume los siguientes compromisos:

- Cumplir los requisitos legales, reglamentarios y contractuales aplicables, en particular la Ley Orgánica de Protección de Datos Personales y el Esquema Gubernamental de Seguridad de la Información.
- Gestionar los riesgos de seguridad de la información mediante un proceso sistemático de identificación, análisis, evaluación y tratamiento.
- Asignar propietarios a los activos de información y responsabilidades definidas para su protección.

- Proporcionar los recursos necesarios para la operación, el mantenimiento y la mejora continua del sistema.
- Promover la concienciación y la formación del personal en materia de seguridad de la información.
- Revisar periódicamente el desempeño del sistema y adoptar las acciones correctivas que correspondan.

La política será aprobada por la Gerencia General mediante resolución, comunicada a todo el personal y revisada al menos una vez al año o cuando se produzcan cambios significativos en el contexto institucional.

4.9.2 Políticas específicas del SGSI

La política general se desarrolla mediante ocho políticas específicas, cuyo contenido esencial y vinculación con los controles del Anexo A se detalla en la Tabla 35.

Tabla 35

Políticas específicas del Sistema de Gestión de Seguridad de la Información

Política	Contenido esencial	Controles asociados
POL-01. Gestión de activos de información	Inventario, propietarios, clasificación, etiquetado, uso aceptable y devolución de activos.	A.5.9 a A.5.13
POL-02. Control de acceso	Gestión de identidades, información de autenticación, derechos de acceso, revisión periódica y accesos privilegiados.	A.5.15 a A.5.18; A.8.2; A.8.5
POL-03. Respaldo y recuperación	Alcance, frecuencia, retención, cifrado, custodia externa, objetivos de recuperación y pruebas de restauración documentadas.	A.8.13; A.8.14; A.5.33
POL-04. Seguridad de redes y comunicaciones	Arquitectura, segmentación, filtrado, acceso remoto, gestión de configuraciones y monitoreo.	A.8.20 a A.8.23; A.8.9
POL-05. Relación con proveedores y servicios en la nube	Cláusulas de seguridad, niveles de servicio, propiedad de la información, reversibilidad y seguimiento del proveedor.	A.5.19 a A.5.23
POL-06. Gestión de incidentes de seguridad	Reporte, clasificación, respuesta, registro, evidencia y aprendizaje de los incidentes.	A.5.24 a A.5.28; A.6.8

Política	Contenido esencial	Controles asociados
POL-07. Seguridad del personal	Acuerdos de confidencialidad, concienciación, responsabilidades al cese, escritorio y pantalla despejados.	A.6.2 a A.6.6; A.7.7
POL-08. Protección de datos personales	Bases de licitud, finalidad, minimización, derechos del titular, encargados del tratamiento y notificación de vulneraciones.	A.5.34; A.5.31; A.5.36

Nota. Elaboración propia con base en el Anexo A de la norma ISO/IEC 27001:2022.

4.9.3 Roles y responsabilidades

El numeral 5.3 de la norma exige la asignación formal de roles y responsabilidades. Considerando que la Unidad de Tecnologías de la Información y Comunicación cuenta con un solo servidor público, la estructura propuesta en la Tabla 36 distribuye las responsabilidades entre las direcciones existentes, sin crear nuevas unidades administrativas.

Tabla 36

Estructura de roles y responsabilidades del SGSI

Rol	Asignación propuesta	Responsabilidades principales
Alta dirección	Gerencia General	Aprobar la política, el alcance y los criterios de aceptación del riesgo; asignar recursos; aceptar formalmente los riesgos residuales.
Comité de Seguridad de la Información	Gerencia General, Dirección Administrativa Financiera, Dirección Técnica, Talento Humano, Procuraduría Síndica y Unidad de TIC	Revisar el desempeño del sistema, priorizar el tratamiento de riesgos y resolver conflictos de recursos. Sesiona trimestralmente.
Responsable de Seguridad de la Información	Servidor designado mediante acción de personal, con dedicación parcial	Coordinar la operación del sistema, mantener la Declaración de Aplicabilidad, gestionar incidentes y reportar indicadores.
Propietarios de activos de información	Directores y responsables de proceso según la Tabla 27	Autorizar el uso y el acceso, aprobar la clasificación y validar el tratamiento de los riesgos de sus activos.
Custodio técnico	Unidad de TIC	Administrar la infraestructura, aplicar los controles técnicos, ejecutar respaldos y mantener los registros de eventos.

Rol	Asignación propuesta	Responsabilidades principales
Administrador de contratos tecnológicos	Unidad de TIC en coordinación con Compras Públicas y Procuraduría Síndica	Verificar el cumplimiento de las cláusulas de seguridad y de los niveles de servicio pactados.
Usuarios de la información	Todo el personal institucional	Cumplir las políticas, proteger sus credenciales y reportar los eventos de seguridad que detecten.

Nota. Elaboración propia con base en la norma ISO/IEC 27001:2022, numeral 5.3.

4.9.4 Modelo de implementación bajo el ciclo PHVA

El modelo de implementación organiza las actividades del sistema en las cuatro etapas del ciclo de mejora continua, conforme se detalla en la Tabla 37.

Tabla 37

Modelo de implementación del SGSI bajo el ciclo PHVA

Etapa	Actividades	Requisitos de la norma	Evidencia
Planificar	Aprobar la política y el alcance; conformar el comité; designar el responsable de seguridad; validar el inventario de activos y la matriz de riesgos; aprobar la Declaración de Aplicabilidad y el plan de tratamiento.	Cláusulas 4, 5 y 6	Resolución de aprobación, actas del comité, matriz de riesgos y Declaración de Aplicabilidad
Hacer	Implementar los controles priorizados; ejecutar el programa de concienciación; documentar procedimientos operativos; gestionar la transferencia del control de la infraestructura en la nube.	Cláusulas 7 y 8	Procedimientos aprobados, registros de capacitación y actas de transferencia
Verificar	Medir los indicadores de desempeño; ejecutar pruebas de restauración y revisiones de accesos; realizar la auditoría interna y la revisión por la dirección.	Cláusulas 9.1, 9.2 y 9.3	Informe de indicadores, informe de auditoría interna y acta de revisión por la dirección
Actuar	Registrar no conformidades, ejecutar acciones correctivas, actualizar la valoración de riesgos y ajustar los controles.	Cláusula 10	Registro de no conformidades y plan de acciones correctivas

Nota. Elaboración propia con base en la norma ISO/IEC 27001:2022.

4.9.5 Cronograma de implementación

La Tabla 38 propone un cronograma de doce meses, ordenado según la prioridad establecida por el nivel de riesgo.

Tabla 38

Cronograma propuesto de implementación

Periodo	Actividades	Riesgos atendidos	Producto
Meses 1–3	Aprobación de la política y del alcance; conformación del comité; designación del responsable de seguridad; validación del inventario de activos y de la matriz de riesgos.	Base del sistema	Resolución de creación del SGSI
Meses 2–4	Transferencia del control administrativo de la infraestructura en la nube; incorporación de cláusulas de seguridad y niveles de servicio en los contratos vigentes.	RG-01, RG-10, RG-16	Acta de transferencia y adendas contractuales
Meses 3–5	Aprobación de la política de respaldos; ejecución y documentación de la primera prueba de restauración de los sistemas críticos.	RG-02	Informe de prueba de restauración
Meses 4–7	Levantamiento de la arquitectura de red; implementación de segmentación, filtrado y registro de eventos; gestión de accesos privilegiados.	RG-03, RG-05, RG-11	Diagramas de red y matriz de accesos
Meses 5–8	Clasificación de la información; designación formal de propietarios; cifrado y control de medios extraíbles; adecuación al régimen de datos personales.	RG-08, RG-13	Catálogo de información clasificada
Meses 6–9	Programa de concienciación; suscripción de acuerdos de confidencialidad; documentación de procedimientos operativos y de segregación de funciones.	RG-04, RG-12	Registros de capacitación y procedimientos
Meses 7–10	Plan de renovación y baja segura de activos obsoletos; reposición de biométricos y de sistemas de protección eléctrica; gestión de parches.	RG-06, RG-07, RG-09, RG-15	Plan de renovación aprobado
Meses 9–11	Implementación de controles de acceso físico al área de servidores y del procedimiento de gestión de incidentes.	RG-14, RG-11	Procedimiento de incidentes
Mes 12	Medición de indicadores, auditoría interna y revisión por la dirección.	Todos	Informe de desempeño del SGSI

Nota. Elaboración propia.

4.9.6 Recursos requeridos

La Tabla 39 identifica los recursos necesarios para la implementación, clasificados según su implicación presupuestaria. La mayor parte de los controles priorizados corresponde a medidas organizativas que no requieren inversión, sino decisión administrativa y dedicación de tiempo del personal existente.

Tabla 39

Recursos requeridos para la implementación

Recurso	Descripción	Implicación presupuestaria
Talento humano	Designación del responsable de seguridad con dedicación parcial y participación del comité.	Sin costo adicional: reasignación de funciones
Normativa interna	Elaboración y aprobación de la política general, ocho políticas específicas y procedimientos operativos.	Sin costo adicional
Transferencia del servicio en la nube	Migración o cesión de la cuenta administrativa de la infraestructura que aloja el sistema financiero.	Requiere estudio de mercado y certificación presupuestaria
Seguridad perimetral	Adquisición e implementación de cortafuegos y segmentación de la red institucional.	Requiere estudio de mercado
Renovación de activos críticos	Reposición de cuatro dispositivos biométricos, dos sistemas de protección eléctrica y equipos en estado malo.	Requiere estudio de mercado
Capacitación	Programa anual de concienciación en seguridad de la información y protección de datos personales.	Costo bajo: capacitadores internos o convenios interinstitucionales
Herramientas de gestión	Registro de eventos, mesa de ayuda e inventario técnico.	Costo bajo: existen alternativas de código abierto

Nota. Elaboración propia. Los valores monetarios deberán establecerse mediante estudio de mercado conforme a la normativa de contratación pública.

4.9.7 Indicadores de desempeño

Conforme al numeral 9.1 de la norma, la Tabla 40 define los indicadores que permitirán evaluar el desempeño del sistema, tomando como punto de partida la línea base establecida en la Tabla 22 del Capítulo III.

Tabla 40

Indicadores de desempeño del SGSI

Indicador	Fórmula	Línea base	Meta año 1	Frecuencia
Cobertura de políticas aprobadas	Políticas aprobadas / políticas planificadas	0 de 9	9 de 9	Semestral
Implementación de controles aplicables	Controles implementados / controles aplicables	11,6 %	60 %	Trimestral

Indicador	Fórmula	Línea base	Meta año 1	Frecuencia
Activos de información con propietario asignado	Activos con propietario / total de activos	0 %	100 %	Semestral
Pruebas de restauración exitosas	Pruebas exitosas / pruebas programadas	0 de 0	4 de 4	Trimestral
Revisión de derechos de acceso	Revisiones ejecutadas / revisiones programadas	0 %	100 %	Trimestral
Personal capacitado en seguridad	Servidores capacitados / total de servidores	0 %	80 %	Anual
Incidentes registrados y cerrados	Incidentes cerrados / incidentes registrados	No medible	90 %	Mensual
Riesgos con nivel residual aceptable	Riesgos aceptables / total de riesgos	0 de 16	14 de 16	Semestral
Contratos con cláusulas de seguridad	Contratos adecuados / contratos vigentes	0 %	100 %	Semestral
Nivel de madurez de seguridad de la información	Valoración por dominio	1,5 / 5	3,0 / 5	Anual

Nota. Elaboración propia con base en la norma ISO/IEC 27001:2022, numeral 9.1.

4.10 Validación de la propuesta

4.10.1 Verificación de la cobertura riesgo–control

La primera verificación consistió en comprobar que cada riesgo identificado cuente con al menos un control del Anexo A asignado y que cada control seleccionado responda efectivamente a un riesgo evaluado. Los dieciséis riesgos de la Tabla 30 tienen controles asignados en la Tabla 32, lo que representa una cobertura del 100 %. En sentido inverso, los ochenta y seis controles declarados aplicables se vinculan con al menos un riesgo, con una política específica o con un requisito legal identificado en la Tabla 24, sin que se registren controles seleccionados sin justificación.

4.10.2 Verificación del cumplimiento de los requisitos de la norma

La segunda verificación contrastó los productos generados por la propuesta con los requisitos de las cláusulas 4 a 10 de la norma ISO/IEC 27001:2022, conforme se detalla en la Tabla 41.

Tabla 41

Verificación del cumplimiento de los requisitos de la norma

Cláusula	Requisito	Producto de la propuesta	Estado
4. Contexto	Comprensión de la organización, de las partes	Tablas 24 y 25 y sus secciones correspondientes	Cubierto en el diseño

Cláusula	Requisito	Producto de la propuesta	Estado
	interesadas y determinación del alcance.		
5. Liderazgo	Política, roles, responsabilidades y compromiso de la dirección.	Política general y Tabla 36	Cubierto en el diseño
6. Planificación	Valoración y tratamiento de riesgos, Declaración de Aplicabilidad y objetivos.	Tablas 27, 30, 32, 33 y 34	Cubierto en el diseño
7. Apoyo	Recursos, competencia, concienciación, comunicación e información documentada.	Tablas 35 y 39	Cubierto en el diseño
8. Operación	Ejecución de los procesos y del plan de tratamiento de riesgos.	Tabla 38	Planificado; corresponde a la implementación
9. Evaluación del desempeño	Seguimiento, medición, auditoría interna y revisión por la dirección.	Tablas 37 y 40	Instrumentos diseñados; ejecución posterior
10. Mejora	No conformidades, acciones correctivas y mejora continua.	Etapa Actuar del modelo; Tabla 37	Instrumentos diseñados; ejecución posterior

Nota. Elaboración propia con base en la norma ISO/IEC 27001:2022.

La verificación evidencia que la propuesta cubre documentalmente la totalidad de los requisitos de las cláusulas 4 a 7, correspondientes a la etapa de planificación del sistema, y provee los instrumentos necesarios para las cláusulas 8 a 10, cuya materialización depende de la decisión institucional de implementar el sistema y excede las delimitaciones del presente trabajo.

4.11 Resultados de la propuesta

El desarrollo de la propuesta permitió obtener siete productos verificables: la declaración de alcance y contexto del sistema, el inventario valorado de veintiún activos de información, la matriz de dieciséis riesgos evaluados, el plan de tratamiento con la selección de controles del Anexo A, la Declaración de Aplicabilidad con ochenta y seis controles aplicables, el cuerpo de nueve políticas institucionales y el modelo de implementación con su cronograma e indicadores.

La Tabla 42 contrasta la situación diagnosticada con la situación esperada tras la implementación del sistema, tomando como referencia los indicadores de línea base establecidos en el Capítulo III.

Tabla 42

Comparación entre la línea base y la situación esperada

Aspecto	Situación diagnosticada	Situación esperada con el SGSI
Marco normativo interno	Ninguna política de seguridad aprobada.	Una política general y ocho políticas específicas aprobadas por resolución.
Gestión de riesgos	Inexistente; sin registro de incidentes ni valoración de activos.	Proceso documentado con inventario valorado, matriz de riesgos y criterios de aceptación.
Controles del Anexo A	10 controles implementados de 86 aplicables (11,6 %).	Meta del 60 % de controles aplicables implementados al primer año.
Respaldo y recuperación	Sin política, sin objetivos de recuperación y sin pruebas documentadas.	Política aprobada, objetivos definidos y pruebas trimestrales documentadas.
Control del servicio crítico en la nube	Cuenta administrativa bajo titularidad del proveedor.	Cuenta y credenciales bajo control institucional, con plan de reversibilidad.
Responsabilidades	Sin rol de seguridad designado y con concentración de funciones.	Comité conformado, responsable designado y propietarios de activos asignados.
Protección de datos personales	Sin clasificación de la información ni medidas específicas.	Información clasificada y política de protección de datos alineada a la LOPDP.
Medición	Sin indicadores propios de seguridad de la información.	Diez indicadores con línea base, meta y frecuencia de medición definidas.
Nivel de madurez	1,5 sobre 5.	Meta de 3,0 sobre 5 al término del primer año de implementación.

Nota. Elaboración propia.

Los resultados obtenidos permiten afirmar que la propuesta dota a la EMMAIPC-EP de un marco de gestión completo en su dimensión documental, con trazabilidad verificable entre los activos de información, los riesgos que los afectan, los controles seleccionados para tratarlos y los indicadores que permitirán medir su desempeño. Su materialización queda supeditada a la aprobación de la Gerencia General y a la asignación de los recursos identificados en la Tabla 39.

Figura 6

Trazabilidad de los productos del diseño del Sistema de Gestión de Seguridad de la Información.



Nota. Elaboración propia con base en International Organization for Standardization e International Electrotechnical Commission (2022b) y EMMAIPC-EP (2026a).

CONCLUSIONES

En relación con el primer objetivo específico, la revisión de la literatura científica y normativa permitió construir el marco teórico que fundamenta el diseño. Se establecieron la confidencialidad, la integridad y la disponibilidad como ejes de la seguridad de la información, se caracterizó la estructura de la norma ISO/IEC 27001:2022 en sus cláusulas 4 a 10 y sus noventa y tres controles del Anexo A, y la comparación de tres metodologías de gestión de riesgos sobre seis criterios sustentó la selección de la ISO/IEC 27005:2022, por su alineación con el Anexo A, por admitir valoración cualitativa ante la ausencia de registros históricos de incidentes y por su viabilidad en una unidad técnica conformada por un solo servidor público.

En relación con el segundo objetivo específico, el diagnóstico documental y el análisis del entorno tecnológico identificaron noventa y un activos tecnológicos por un valor histórico de USD 73.870,09, de los cuales el 41,8 % se encuentra en estado regular, malo o en reposición y el 59,3 % superó su vida útil, y un nivel de madurez preliminar de 1,5 sobre 5, sin políticas de seguridad aprobadas, sin procedimientos de respaldo documentados ni probados y sin un rol de seguridad de la información designado. Sobre esta base se evaluaron dieciséis riesgos, cinco de nivel muy alto, ocho de nivel alto y tres de nivel medio; el de mayor severidad corresponde al sistema de facturación y recaudación alojado en la nube bajo una cuenta administrativa de titularidad del proveedor.

En relación con el tercer objetivo específico, el diseño del Sistema de Gestión de Seguridad de la Información se concretó en un inventario valorado de veintiún activos de información, un plan de tratamiento que asigna controles del Anexo A a la totalidad de los riesgos identificados, una política general, ocho políticas específicas alineadas a la ISO/IEC 27002:2022 y una Declaración de Aplicabilidad con ochenta y seis controles aplicables y siete exclusiones justificadas por la ausencia de desarrollo de software en el alcance. El cumplimiento inicial del 11,6 % respecto de los controles aplicables constituye la línea base de medición del sistema.

En relación con el cuarto objetivo específico, el modelo de implementación bajo el ciclo PHVA organiza las actividades del sistema en un cronograma de doce meses ordenado por nivel de riesgo, con una estructura de siete roles que distribuye las responsabilidades entre las direcciones existentes sin crear nuevas unidades administrativas y diez indicadores de desempeño con línea base, meta y frecuencia de

medición. La mayor parte de los controles priorizados corresponde a medidas organizativas que no requieren inversión, sino decisión administrativa, lo que hace viable la implementación en una empresa pública de tamaño reducido.

En relación con el quinto objetivo específico, la validación realizada fue de carácter interno y documental. La cobertura entre riesgos y controles alcanza el 100 % y la verificación normativa evidenció que la propuesta cubre documentalmente los requisitos de las cláusulas 4 a 7 de la norma ISO/IEC 27001:2022 y provee los instrumentos de las cláusulas 8 a 10. Tras la aplicación de los controles, catorce de los dieciséis riesgos alcanzan un nivel residual dentro del umbral de aceptación; los dos restantes, relativos a la seguridad perimetral de la red y a la concentración de funciones en la unidad técnica, requieren aceptación formal de la Gerencia General por depender de decisiones de inversión y de talento humano.

RECOMENDACIONES

- A la Universidad Católica de Cuenca, Extensión Cañar, y en particular a la Carrera de Ingeniería de Sistemas de Información, se recomienda dar continuidad a este trabajo mediante proyectos de titulación y de vinculación con la sociedad que aborden la fase de implementación y la auditoría interna del sistema diseñado, y replicar el estudio en otras empresas públicas municipales y mancomunadas de la provincia, con el fin de contrastar los hallazgos, fortalecer la línea de investigación en seguridad de la información y avanzar hacia un modelo sectorial aplicable a las entidades públicas de tamaño reducido.
- A la EMMAIPC-EP se recomienda que la Gerencia General apruebe mediante resolución la política general de seguridad de la información, el alcance del sistema y la Declaración de Aplicabilidad, y designe formalmente al responsable de seguridad de la información; que gestione de manera prioritaria la transferencia del control administrativo de la infraestructura en la nube que aloja el sistema financiero, incorporando cláusulas de seguridad, niveles de servicio y reversibilidad en los contratos vigentes; que ejecute dentro de los primeros cinco meses una primera prueba documentada de restauración de los sistemas críticos; que documente los procedimientos operativos de la Unidad de TIC para reducir la dependencia de una sola persona; que ejecute el programa anual de concienciación en seguridad de la información y protección de datos personales dirigido a todo el personal; y que mida anualmente los diez indicadores definidos frente a la línea base, con el fin de verificar objetivamente el avance del sistema ante el Comité de Seguridad de la Información.

Bibliografía

Aguilar-Coronel, C. F., & Cuenca-Tapia, J. P. (2025). Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en el estándar ISO/IEC 27001

para la empresa EJEPROY Cía. Ltda. *MQRInvestigar, 9*(1), e361. https://doi.org/10.56048/MQR20225.9.1.2025.e361

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial, Quinto Suplemento N.º 459, 26 de mayo de 2021.

Asamblea Nacional del Ecuador. (2023). *Ley Orgánica para la Transformación Digital y Audiovisual*. Registro Oficial, Suplemento N.º 245, 7 de febrero de 2023.

Apriany, A., & Wibowo, A. (2024). Analysis of the implementation of ISO 27001:2022 and KAMI Index in enhancing the information security management system in consulting firms. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems), 18*(4), 417–428. https://doi.org/10.22146/ijccs.100385

Boné-Andrade, M. F., Pinargote-Bravo, V. J., & Bonilla-Fierro, L. F. (2023). Estrategias de ciberseguridad en entornos de trabajo híbridos y remoto. *Revista Científica Ciencia y Método, 1*(4), 31–43. https://doi.org/10.55813/gaea/rcym/v1/n4/21

Coronel Suárez, I., & Quirumbay Yagual, D. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *Revista Científica y Tecnológica UPSE, 9*(2), 97–108. https://doi.org/10.26423/rctu.v9i2.672

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

Donoso Vargas, D., Calahorrano Recalde, C., & Donoso Vargas, S. (2023). Aplicación del SGSI ISO 27001 en el sistema de rehabilitación social de Ecuador. *Universidad y Sociedad, 15*(2), 274–284. https://rus.ucf.edu.cu/index.php/rus/article/view/3628

EMMAIPC-EP. (2026a). *Diagnóstico integral de tecnologías de la información de la EMMAIPC-EP* [Documento institucional inédito]. Unidad de Tecnologías de la Información y Comunicación.

EMMAIPC-EP. (2026b). *Inventario patrimonial de activos tecnológicos* [Documento institucional inédito]. Dirección Administrativa Financiera.

Guarneros Moreno, I. (2023). *Implementación de políticas de seguridad de información basados en ISO 27001* [Tesis de maestría, Tecnológico de Estudios Superiores de Cuautitlán Izcalli]. Repositorio Institucional del Tecnológico Nacional de México. https://rinacional.tecnm.mx/bitstream/TecNM/6163/1/Guarneros.pdf

International Organization for Standardization & International Electrotechnical Commission. (2022a). *Information security, cybersecurity and privacy protection — Guidance on managing information security risks* (ISO/IEC 27005:2022). https://www.iso.org/standard/80585.html

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

Kamil, Y., Lund, S., & Islam, M. S. (2023). Information security objectives and the output legitimacy of ISO/IEC 27001: Stakeholders' perspective on expectations in private organizations in Sweden. *Information Systems and e-Business Management, 21*(3), 699–722. https://doi.org/10.1007/s10257-023-00646-y

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 information security management standard: How to extract value from data in the IT sector. *Sustainability, 15*(7), 5828. https://doi.org/10.3390/su15075828

Kurniawan, E., Riadi, I., Irmawan, A., & Arusani. (2022). Performance measurement of security academic information system using maturity level. *International Journal of Innovative Science and Research Technology, 7*(4). https://doi.org/10.48550/arXiv.2204.09511

Ministerio de Hacienda y Administraciones Públicas. (2012). *MAGERIT – versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I: Método*. Gobierno de España. https://administracionelectronica.gob.es/ctt/magerit

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2024). *Acuerdo Ministerial N.º MINTEL-MINTEL-2024-0003: Expídese el Esquema Gubernamental de Seguridad de la Información (EGSI)*. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2024/04/Acuerdo-Nro.-MINTEL-MINTEL-2024-0003-Esquema-Gubernamental-Seguridad-de-la-Informacion-EGSI.pdf

Miranda Jiménez, J. N. (2021). *Mapeo sistemático de metodologías de seguridad de la información para el control de la gestión de riesgos informáticos* [Tesis de grado, Universidad Politécnica Salesiana]. Repositorio Institucional UPS. https://dspace.ups.edu.ec/handle/123456789/20966

Nurbojatmiko, N., Khatami Karimiyah, M. S., Asnadi, N. M., & Anisyah, R. (2025). ISO 27001 as information security solution in Society 5.0 era: Systematic literature review [ISO 27001 como solución de seguridad de la información en la era de la Sociedad 5.0: Revisión sistemática de la literatura]. *Sinkron: Jurnal Dan Penelitian Teknik Informatika, 9*(1), 484–492. https://doi.org/10.33395/sinkron.v9i1.14448

Olvera Peña, E. A., Arambarri, J., & Domingo Soriano, S. (2026). Gestión de riesgos en TI según ISO 27001:2022 en una unidad educativa fiscal de Ecuador. *Ciencias y Saberes, 4*(2), 34–47. https://doi.org/10.59602/cys.v4i2.57

Ortega Ovalle, M. T. (2026). ISO/IEC 27001:2022 como estándar internacional para la gestión de la seguridad de la información. *Revista Científica de Salud y Desarrollo Humano, 7*(2), 188–200. https://doi.org/10.61368/r.s.d.h.v7i2.1025

Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry, 142*, 103744. https://doi.org/10.1016/j.compind.2022.103744

SafetyCulture. (2026, 28 de abril). *Análisis de riesgos: Ejemplo y métodos*. https://safetyculture.com/es/temas/analisis-de-riesgos

Universitat Carlemany. (2025, 22 de diciembre). *Seguridad informática: Qué es, principios, tipos y ejemplos prácticos*. https://www.universitatcarlemany.com/actualidad/blog/seguridad-informatica-que-es

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, 8*(5), 12956–12979. https://doi.org/10.37811/cl_rcm.v8i6.14758

Anexo 1: Formato del Anteproyecto.

A. TÍTULO
Diseño de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la empresa EMMAIPC-EP

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
		Inteligencia de Negocios	
		Sistemas de Información	
		Gobierno y administración de tecnologías de información	
		Auditoría Informática	
		Seguridad Informática	**x**
		Redes y comunicación	
		Arquitectura de Hardware	

Tecnologías de Información y Comunicación	**Ciencias exactas, naturales y tecnológicas**	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 constituye uno de los activos estratégicos más valiosos de cualquier organización, ya que de su disponibilidad, integridad y confidencialidad dependen los procesos administrativos, operativos y financieros. La transformación digital ha ampliado el volumen de datos gestionados y, con ello, la superficie de exposición a amenazas como accesos no autorizados, fuga o alteración de datos, errores humanos y ataques informáticos. En este escenario, la adopción de estándares internacionales de seguridad de la información se ha convertido en un requisito de confianza y continuidad operativa para las organizaciones (Podrecca et al., 2022).

El sector público es particularmente sensible a estos riesgos, debido a la cantidad de datos ciudadanos e institucionales que administra y a la frecuente ausencia de marcos formales de gestión. En muchas organizaciones públicas, la falta de políticas de seguridad documentadas, controles implementados o procedimientos de respuesta a incidentes bien definidos socavan la confidencialidad, integridad y disponibilidad de la información (Villarreal Morales et al., 2024). En el contexto ecuatoriano, normativas como la Ley Orgánica de Protección de Datos Personales (LOPDP) y el Esquema Gubernamental de Seguridad de la Información (EGSI) obligan a las entidades del sector público a proteger la información que administran.

A través de sus sistemas, la Empresa Pública Municipal de Manejo de Residuos, Gestión Integral de Residuos Sólidos y Actividades Complementarias del cantón Cañar (EMMAIPC-EP) maneja datos administrativos, operativos y financieros críticos que respaldan la ejecución de sus funciones. Sin embargo, la gestión de la seguridad de la información en la institución se realiza de manera informal, sin un Sistema de Gestión de Seguridad de la Información (SGSI) formal basado en estándares internacionales, lo que limita su capacidad para identificar, analizar y mitigar los riesgos asociados a sus activos

de información. La infraestructura tecnológica que respalda esta información está conformada principalmente por servidores, los sistemas o aplicativos de gestión administrativa y financiera, las bases de datos institucionales, la red interna y los equipos de cómputo del personal, elementos sobre los cuales no se han implementado controles formales de seguridad. Asimismo, la institución no dispone de un registro formal de incidentes de seguridad que permita dimensionar su exposición real; en caso de haberse presentado eventos como pérdida de datos, caídas del sistema, accesos no autorizados o infecciones por malware, describirlos brevemente en este apartado. La ausencia de un enfoque estructurado, como el que propone la norma ISO/IEC 27001:2022, impide establecer controles y lineamientos adecuados para la protección de la información (International Organization for Standardization; International Electrotechnical Commission, 2022).

Esta situación puede derivar en vulnerabilidades que afecten la continuidad de las operaciones, ocasionen pérdida de información relevante o comprometan la confianza institucional. Asimismo, la falta de políticas y procedimientos definidos dificulta una respuesta oportuna ante incidentes de seguridad, al no existir directrices claras de actuación.

Este problema plantea la siguiente pregunta de investigación: ¿Cómo diseñar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2022 que permita fortalecer la confidencialidad, integridad y disponibilidad de los activos de información de la EMMAIPC-EP?

D. OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2022 para la EMMAIPC-EP, mediante el diagnóstico de la situación actual, la gestión de riesgos sobre los activos de información y la definición de controles de seguridad, con el fin de fortalecer la confidencialidad, integridad y disponibilidad de la información institucional.

E. OBJETIVOS ESPECÍFICOS
1. Construir el marco teórico relacionado con la seguridad de la información, la gestión de riesgos y la norma ISO/IEC 27001:2022, mediante la revisión de literatura científica y normativa vigente, para fundamentar conceptualmente el diseño del Sistema de Gestión de Seguridad de la Información en EMMAIPC-EP.
2. Identificar los activos de información y riesgos de seguridad en la empresa EMMAIPC-EP, mediante un diagnóstico documental y análisis del entorno tecnológico, para determinar las principales vulnerabilidades que afectan la información institucional.
3. Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022, a través de la definición de controles, políticas y procedimientos alineados a la norma ISO/IEC 27002:2022, para mejorar la protección de los activos de información.
4. Proponer un modelo de implementación del SGSI basado en el ciclo PHVA, mediante la integración de la gestión de riesgos y el seguimiento de controles, para fortalecer la seguridad de la información y la continuidad operativa en EMMAIPC-EP.

F. JUSTIFICACIÓN
El presente proyecto se justifica en la creciente necesidad de las organizaciones de proteger adecuadamente sus activos de información frente a un entorno caracterizado por el incremento de amenazas cibernéticas, fallas operativas y riesgos asociados al manejo de datos digitales. Aquí, la integración de la información ha sido enfatizada como un activo importante. Su gestión influye en la sostenibilidad de las operaciones, la efectividad de la organización y su capacidad para tomar decisiones informadas. Respecto a la empresa EMMAIPC-EP, no contar con un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO/IEC 27001:2022 representa una brecha considerable. Los controles informales, la falta de un enfoque estructurado para la

gestión de riesgos y la protección general de la información, en términos de confidencialidad, integridad y disponibilidad, carecen de madurez, formalidad y alineación estratégica.

La empresa podrá aplicar una metodología sistemática y preventiva a la gestión de la seguridad de la información de acuerdo con estándares internacionales reconocidos. La implementación futura del SGSI diseñado ayudará a reducir riesgos y a mejorar la resiliencia de la organización, así como a fortalecer la continuidad de los procesos esenciales.

Este estudio también tiene valor académico y práctico. Demuestra cómo se puede aplicar un marco regulatorio internacional en la vida real. Como resultado, se presenta una propuesta metodológica que puede ser la base para implementar sistemas de seguridad en otras organizaciones del sector público.

Entre los beneficiarios del proyecto se encuentran la propia EMMAIPC-EP y su personal, así como la ciudadanía cuya información administra la institución; de manera indirecta, otras entidades del sector público podrán tomar esta propuesta como referencia. Por lo tanto, desde ambas perspectivas, desarrollar este proyecto es importante debido a la mejora que esto brindaría a la gestión de la seguridad de la información en EMMAIPC-EP.

G. ALCANCE

Este proyecto tiene como objetivo analizar y diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 para EMMAIPC-EP. Para ello, el desarrollo del proyecto contempla las siguientes etapas: primero, se diagnosticará la situación actual de la seguridad de la información. A continuación, se identificarán y clasificarán los activos de información críticos. Posteriormente, se evaluarán los riesgos planteados por amenazas y vulnerabilidades en función de su probabilidad e impacto. Finalmente, se desarrollarán políticas de seguridad, controles y procedimientos en conjunto con los controles de seguridad del Anexo A de la norma ISO/IEC 27001:2022.

Este estudio solo incluye el diseño de una propuesta para un Sistema de Gestión de Seguridad de la Información (SGSI) y excluye la implementación operativa de la

propuesta, cualquier compra o instalación de herramientas y/o infraestructura tecnológica, así como las auditorías de certificación. Esta propuesta formalizará una base estructurada que sirva como referencia para las futuras fases de implementación y para la mejora continua y el fortalecimiento del sistema de seguridad de la institución.

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.

Sistema de Gestión de Seguridad de la Información (SGSI)

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un enfoque integral para gestionar la seguridad de la información que incluye todos los procesos, procedimientos y herramientas que una organización puede usar para identificar, evaluar y controlar los riesgos de seguridad. Un SGSI tiene como objetivo facilitar la mejora continua de la postura de seguridad de una organización.

ISO/IEC 27001:2022 establece que los procesos de gestión de riesgos y mejora continua integrados en el ciclo PDCA de una organización, con respecto al SGSI, adaptados para alinearse con los objetivos estratégicos de la Organización, conducirán a las mejores prácticas posibles para la gestión de la seguridad de la información en la Organización (International Organization for Standardization & International Electrotechnical Commission, 2022).

ISO/IEC 27001:2022

ISO/IEC 27001:2022 define los requisitos para que las empresas establezcan, implementen, mantengan y mejoren el SGSI, y es una norma internacional. Esta norma se centra en la gestión de riesgos. Esto incluye, pero no se limita a, identificar cuáles son los activos de información, evaluar qué amenazas y vulnerabilidades potenciales existen y qué controles implementar para reducir el riesgo (International Organization for Standardization & International Electrotechnical Commission, 2022).

Ali (2026) señala que ha habido una evolución en la versión ISO/IEC 27001:2022, ya que es posible una mayor flexibilidad en la implementación del SGSI y es probable que esté mejor alineada con ecosistemas digitales complejos. Además, esta norma permite a las organizaciones cumplir con sus obligaciones regulatorias y mejorar la confianza de sus interesados.

ISO/IEC 27002:2022

Junto con ISO/IEC 27001, la ISO/IEC 27002:2022 describe un conjunto de controles de mejores prácticas para la seguridad de la información. Los controles se enmarcan dentro de varios dominios y abarcan los aspectos organizativos, de personal, físicos y tecnológicos.

Su propósito principal es actuar como referencia para la aplicación de controles de seguridad en el SGSI y ayudar a determinar qué controles aplicar en función del grado de riesgo. De acuerdo con la ISO/IEC (2022), esta norma permite estandarizar la implementación de controles de seguridad en diferentes tipos de organizaciones.

Gestión de riesgos de seguridad de la información

La gestión de riesgos es un proceso fundamental dentro de la seguridad de la información que consiste en identificar, analizar y evaluar los riesgos asociados a los activos de información, con el objetivo de aplicar tratamientos adecuados.

Este proceso incluye la identificación de amenazas, la evaluación de vulnerabilidades y el análisis del impacto potencial sobre la organización. Según ISO/IEC 27001:2022, la gestión de riesgos permite priorizar la implementación de controles de seguridad en función del nivel de exposición de cada activo (International Organization for Standardization & International Electrotechnical Commission, 2022).

NIST (2024) complementa este enfoque indicando que la gestión de riesgos debe integrarse con estrategias de ciberseguridad más amplias, que incluyan capacidades de detección, respuesta y recuperación ante incidentes.

Confidencialidad, integridad y disponibilidad (CIA Triad)

El modelo CIA constituye el fundamento teórico de la seguridad de la información:

- Confidencialidad: garantiza que la información solo sea accesible por usuarios autorizados.
- Integridad: asegura que la información no sea alterada de manera no autorizada o accidental.
- Disponibilidad: asegura que la información esté accesible cuando se requiera.

Este modelo es ampliamente utilizado en marcos de seguridad como ISO/IEC 27001 y NIST CSF, ya que permite estructurar los objetivos de protección de la información en cualquier organización (ControlCase, s. f.).

Ciclo PHVA (Planificar – Hacer – Verificar – Actuar)

El ciclo PHVA es un modelo de mejora continua aplicado en los sistemas de gestión, incluido el SGSI. Este modelo permite estructurar la gestión de la seguridad en cuatro fases:

- Planificar: identificar riesgos y definir controles.
- Hacer: implementar los controles definidos.
- Verificar: evaluar la eficacia de los controles.
- Actuar: realizar mejoras continuas al sistema.

Según Ali (2026), el uso del ciclo PHVA en ISO/IEC 27001 permite asegurar que el sistema de seguridad evolucione continuamente en función de los cambios del entorno tecnológico y las nuevas amenazas emergentes.

Ciberseguridad y marcos de control

La ciberseguridad comprende las prácticas, tecnologías y procesos diseñados para proteger sistemas, redes y datos frente a ataques digitales. En la actualidad, las organizaciones adoptan marcos de referencia como ISO/IEC 27001 y el NIST Cybersecurity Framework 2.0 para estructurar sus estrategias de seguridad.

Diseñado para ayudar a las organizaciones a incurrir en pérdidas por riesgos cibernéticos de manera más efectiva, el NIST CSF 2.0 (2024) ofrece una categorización más detallada de las funciones cibernéticas. Estas comprenden las cinco funciones de identificar, proteger, detectar, responder y recuperar.

I. TRABAJOS RELACIONADOS

A nivel internacional, Kitsios et al. (2023) analizaron las razones que llevan a las organizaciones del sector de tecnologías de la información a adoptar la norma ISO/IEC 27001 y los beneficios obtenidos tras su certificación. Mediante un estudio de caso en una empresa del sector, los autores documentaron el proceso completo de adecuación a la norma e identificaron que la implementación permite estructurar políticas, mejorar la gestión de riesgos y fortalecer la confianza de los socios estratégicos. Este estudio aporta al presente proyecto la evidencia de que la norma ISO/IEC 27001 genera valor organizacional más allá del cumplimiento formal; sin embargo, se desarrolla en una empresa privada del sector tecnológico, contexto distinto al de una empresa pública municipal con recursos técnicos limitados.

Domínguez-Domínguez et al. (2023) evaluaron el sistema de gestión de seguridad de la información de una institución de educación superior mexicana, midiendo el grado de conocimiento administrativo, la capacitación del talento humano, el compromiso directivo y la eficacia de la gestión del riesgo con base en la norma ISO/IEC 27001. Aplicaron un instrumento cuantitativo a una población de 81 sujetos, integrada por 66 administrativos y 15 miembros del departamento de tecnologías de la información. Los resultados evidenciaron que las principales debilidades no son de naturaleza tecnológica sino organizacional, hallazgo directamente pertinente para esta investigación, ya que la EMMAIPC-EP presenta una situación equivalente; no obstante, el estudio se limita a diagnosticar sin proponer un diseño de sistema.

Kurniawan et al. (2022) midieron el desempeño de la seguridad de un sistema de información académica mediante niveles de madurez, evaluando 15 objetivos de control y 45 controles de seguridad distribuidos en cinco cláusulas de la familia ISO/IEC 27000. Emplearon un enfoque cualitativo descriptivo con triangulación entre entrevistas, observación y revisión documental, y determinaron un nivel de madurez de 2 sobre 5, por debajo del nivel esperado. Este antecedente aporta la metodología de valoración por niveles de madurez y el uso de la triangulación como mecanismo de validación, ambos aplicables al diagnóstico de la EMMAIPC-EP; su limitación radica en que se restringe a la medición y no desarrolla el tratamiento de los riesgos identificados.

A nivel nacional, Donoso Vargas et al. (2023) aplicaron un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 en el sistema de rehabilitación social del Ecuador, específicamente sobre los mecanismos electrónicos de monitoreo de personas con medidas sustitutivas. El estudio definió los controles necesarios para proteger la información georreferenciada de los ciudadanos monitoreados y demostró la viabilidad de aplicar la norma en el sector público ecuatoriano bajo el marco legal vigente. Su aporte a esta investigación es la validación de la norma en instituciones públicas nacionales sujetas a la protección de datos personales; sin embargo, se centra en un sistema de monitoreo especializado y no en los procesos administrativos y financieros de una empresa municipal.

A nivel local, Aguilar Coronel y Cuenca Tapia (2025), de la Universidad Católica de Cuenca, diseñaron un Sistema de Gestión de Seguridad de la Información basado en el estándar ISO/IEC 27001 para la empresa EJEPROY Cía. Ltda. El diseño se estructuró en cinco fases que comprenden la definición del alcance, la obtención del aval de la alta gerencia, la elaboración del inventario de activos de información, el análisis de riesgos y la selección de controles. Este trabajo constituye el antecedente más cercano al presente proyecto por su alcance metodológico y su origen institucional; la diferencia radica en que se desarrolla sobre una empresa privada de construcción, mientras que la presente investigación aborda una empresa pública municipal mancomunada sujeta al Esquema Gubernamental de Seguridad de la Información y a la Ley Orgánica de Protección de Datos Personales.

J. METODOLOGÍA

El estudio adopta un enfoque cualitativo y cuantitativo. Implica un análisis del estado actual de la seguridad de la información en la empresa EMMAIPC-EP y utiliza enfoques de identificación de activos y análisis de riesgos, análisis de controles de seguridad, y también evalúa el nivel de riesgo de seguridad e impacto. Este enfoque permite comprender tanto las condiciones organizacionales como la valoración objetiva de los riesgos asociados a la información.

El nivel de investigación es descriptivo – analítico, ya que permite caracterizar el entorno de seguridad de la información de la institución, identificar sus principales

vulnerabilidades y analizar el comportamiento de los riesgos tecnológicos en función de su impacto sobre los activos de información. Asimismo, se evalúa la relación entre los procesos organizacionales y la necesidad de implementar un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001:2022.

La presente investigación se desarrollará mediante el análisis documental de la situación actual de la EMMAIPC-EP, considerando sus procesos administrativos, operativos y tecnológicos relacionados con la gestión de la información. Se realizará la identificación y clasificación de activos de información críticos, seguido del análisis de amenazas y vulnerabilidades mediante una matriz de riesgos basada en probabilidad e impacto.

Posteriormente, se diseñará una propuesta de Sistema de Gestión de Seguridad de la Información (SGSI) alineado a la norma ISO/IEC 27001:2022, incluyendo la definición de políticas, controles y procedimientos basados en el Anexo A de la norma ISO/IEC 27002:2022. Finalmente, se estructurará un modelo de mejora continua basado en el ciclo PHVA (Planificar – Hacer – Verificar – Actuar), con el fin de garantizar la sostenibilidad del sistema de seguridad propuesto.

K. CRONOGRAMA DE ACTIVIDADES

N°	ACTIVIDAD	MES						
		I	II	III	IV	V	VI	MEDIOS DE VERIFICACIÓN
1	Revisión bibliográfica sobre seguridad de la información, gestión de riesgos y las normas ISO/IEC 27001:2022 y 27002:2022	X	X					Matriz de revisión bibliográfica y marco teórico
2	Diagnóstico documental de la situación actual de la seguridad de la información en la EMMAIPC-EP (procesos		X	X				Informe de diagnóstico situacional

	administrativos, operativos y tecnológicos)							
3	Identificación y clasificación de activos de información críticos			X				Inventario de activos de información
4	Análisis de amenazas y vulnerabilidades y valoración de riesgos mediante matriz de probabilidad e impacto			X	X			Matriz de riesgos
5	Diseño del SGSI: definición de políticas, controles y procedimientos alineados al Anexo A de ISO/IEC 27002:2022				X	X		Documento de diseño del SGSI y declaración de aplicabilidad (SoA)
6	Propuesta del modelo de implementación y mejora continua basado en el ciclo PHVA					X		Modelo de implementación PHVA
7	Redacción de conclusiones y recomendaciones y consolidación del informe final de tesis						X	Documento final de tesis

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. Danny Patricio Andrade Cárdenas
ESTUDIANTE 1	Kevin Alexander Cantos Espinoza

N. FIRMAS DE RESPONSABILIDAD	
Lugar:	Cañar
Fecha:	28 de abril del 2026

Firmas:

Nombre: Ing. Danny Patricio Andrade Cárdenas CC: 0301340287 **Director del Proyecto**	Nombre: Kevin Alexander Cantos Espinoza C.C.: 0302390018 **Estudiante / Egresado**

O. APROBACIÓN

Firmas:

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

P. REFERENCIAS

Aguilar Coronel, C. F., & Cuenca Tapia, J. P. (2025). Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en el estándar ISO/IEC 27001 para la empresa EJEPROY Cía. Ltda. *MQRInvestigar*.

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

ControlCase. (s. f.). *What is ISO 27001? A detailed, simple, and straightforward guide*. https://www.controlcase.com/what-is-iso-27001/

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

Donoso Vargas, D., Calahorrano Recalde, C., & Donoso Vargas, S. (2023). Aplicación del SGSI ISO 27001 en el sistema de rehabilitación social de Ecuador. *Universidad y Sociedad, 15*(2), 274–284.

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

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

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 information security management standard: How to extract value from data in the IT sector. *Sustainability, 15*, 5828. https://doi.org/10.3390/su15075828

Kurniawan, E., Riadi, I., Irmawan, A., & Arusani. (2022). Performance measurement of security academic information system using maturity level. *International Journal of Innovative Science and Research Technology, 7*(4).

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: Guía de entrevista semiestructurada al responsable de la Unidad de Tecnologías de la Información y Comunicación.

Instrumento de recolección de información. Técnica: entrevista semiestructurada. Objetivo específico al que responde: OE2 (identificar los activos de información y riesgos de seguridad de la EMMAIPC-EP).

Campo	Registro
Institución	Empresa Pública Municipal Mancomunada de Aseo Integral de los cantones Cañar, Biblián, El Tambo y Suscal (EMMAIPC-EP)
Entrevistado (cargo)	Analista / responsable de la Unidad de Tecnologías de la Información y Comunicación
Entrevistador	Kevin Alexander Cantos Espinosa
Fecha y duración	
Objetivo	Validar la información técnica obtenida en la revisión documental, conocer las prácticas vigentes, los controles existentes y las limitaciones operativas de la seguridad de la información.
Instrucciones	Las preguntas son abiertas y sirven de guía; el entrevistador puede profundizar según las respuestas. Se registran las respuestas textuales y, cuando exista, la evidencia documental que las respalda. La información se califica según los criterios de confiabilidad de la Tabla 8 (verificada, pendiente de validación técnica o no identificada).

N.º	Pregunta	Respuesta / observaciones	Evidencia solicitada
A. Organización y gobierno de la seguridad de la información			
1	¿Existe una política de seguridad de la información aprobada formalmente? ¿Quién la aprobó y en qué fecha?		Resolución o documento de política
2	¿Se ha designado un responsable de seguridad de la información o un comité con esa función?		Acción de personal, resolución
3	¿Cuántas personas conforman la Unidad de TIC y qué funciones cumple cada una? ¿Existe un manual de funciones?		Orgánico funcional, manual de puestos
4	¿La unidad cuenta con procedimientos operativos documentados (respaldos, altas y bajas de usuarios, mantenimiento, atención de incidentes)?		Procedimientos escritos
B. Activos de información e inventario			
5	¿Se mantiene un inventario de activos tecnológicos y de información? ¿Quién lo actualiza y con qué periodicidad?		Inventario patrimonial, registros de la unidad
6	¿Se clasifica la información según su sensibilidad (pública, interna, confidencial)? ¿Con qué criterio?		Política o procedimiento de clasificación
7	¿Qué activos considera críticos para la operación de la empresa y por qué?		Listado priorizado
8	¿Qué equipos han superado su vida útil y cuáles presentan fallas recurrentes?		Inventario con fechas de adquisición
C. Infraestructura tecnológica y red			
9	Describa los servidores, equipos de red, enlaces de Internet y cobertura de la red inalámbrica de la institución.		Diagrama de red, inventario

N.º	Pregunta	Respuesta / observaciones	Evidencia solicitada
10	¿Existe un firewall perimetral o segmentación de la red? ¿Quién lo administra y cuándo se actualizó por última vez?		Configuración, contrato de soporte
11	¿El cuarto de equipos cuenta con control de acceso físico, UPS, climatización y protección contra incendios?		Fotografías, registros de acceso
D. Aplicaciones, servicios en la nube y proveedores			
12	¿Qué sistemas de información utiliza la empresa (facturación y recaudación, contabilidad, talento humano, gestión documental) y dónde se alojan (servidor local o nube)?		Portafolio de aplicaciones, contratos
13	¿Quién administra cada sistema y quién posee las credenciales de administrador, en especial de los servicios alojados en la nube?		Registro de cuentas administrativas
14	¿Qué contratos vigentes existen con proveedores tecnológicos? ¿Incluyen cláusulas de seguridad, confidencialidad, niveles de servicio y devolución de la información?		Contratos, órdenes de servicio
E. Control de acceso			
15	¿Cómo se gestionan las altas, modificaciones y bajas de usuarios en los sistemas y en la red?		Procedimiento, solicitudes de acceso
16	¿Existen cuentas compartidas o genéricas? ¿Se exige una política de contraseñas y doble factor de autenticación?		Configuración de sistemas
17	¿Se revisan periódicamente los privilegios asignados al personal?		Registros de revisión
F. Respaldos y continuidad			
18	¿Qué información se respalda, con qué frecuencia, en qué medio y dónde se almacenan las copias?		Procedimiento y bitácora de respaldos
19	¿Se ha realizado alguna prueba documentada de restauración? ¿Cuándo y con qué resultado?		Registro de pruebas
20	¿Existe un plan de continuidad o de recuperación ante desastres para los sistemas críticos?		Plan documentado
G. Incidentes, vulnerabilidades y protección técnica			
21	¿Se han presentado incidentes de seguridad (malware, pérdida de datos, accesos no autorizados, caídas de servicio)? ¿Cómo se gestionaron?		Informes, correos, bitácoras
22	¿Existe un procedimiento y un registro formal de incidentes de seguridad?		Procedimiento, registro
23	¿Cómo se gestionan el antivirus, las actualizaciones y los parches de seguridad en servidores y estaciones de trabajo?		Consola de antivirus, políticas de actualización
H. Personal, concienciación y cumplimiento normativo			
24	¿El personal ha recibido capacitación en seguridad de la información o en protección de datos personales?		Registros de capacitación
25	¿Se firman acuerdos de confidencialidad y existe un proceso de retiro de accesos cuando un servidor se desvincula?		Acuerdos, procedimiento de salida

N.º	Pregunta	Respuesta / observaciones	Evidencia solicitada
26	¿La institución conoce y aplica las obligaciones de la LOPDP y del EGSI? ¿Se ha designado un delegado de protección de datos?		Designación, informes
27	¿Cuáles son, a su criterio, las principales limitaciones (presupuesto, personal, conocimiento) y necesidades de la seguridad de la información en la empresa?		Observaciones del entrevistado

Cierre de la entrevista: se agradece la colaboración, se acuerda la entrega de la evidencia solicitada y se informa que la información será utilizada exclusivamente con fines académicos para el diseño del SGSI.

Anexo 3: Ficha de inventario de activos de información.

Instrumento de recolección de información. Técnica: observación estructurada y análisis documental. Objetivo específico al que responde: OE2. Se llena una ficha por cada activo identificado; los datos sirven para construir el inventario valorado (Tabla 17) y la matriz de riesgos (Tabla 30).

Campo	Registro / instructivo
Código del activo	Identificador único asignado en el inventario (p. ej., AI-01).
Nombre del activo	
Categoría	Información / Software / Hardware / Servicios / Personas / Instalaciones
Descripción	Función que cumple y contenido o alcance del activo.
Proceso al que apoya	Facturación y recaudación, contabilidad, talento humano, operación de aseo, gestión documental, otro.
Propietario (responsable)	Dirección o unidad que decide sobre el uso del activo.
Custodio	Persona o unidad que lo administra u opera diariamente.
Ubicación	Física (oficina, cuarto de equipos) o lógica (servidor, nube, proveedor).
Fecha de adquisición o puesta en servicio	
Vida útil registrada (años) / situación	Vigente / Superada
Estado de conservación	Bueno / Regular / Malo / En reposición
Valor histórico (USD)	Según inventario patrimonial, cuando aplique.
Valoración de confidencialidad (1 a 5)	Impacto si la información se divulga a personas no autorizadas.
Valoración de integridad (1 a 5)	Impacto si la información se altera o destruye sin autorización.
Valoración de disponibilidad (1 a 5)	Impacto si el activo deja de estar disponible.
Valor total y criticidad	Suma C+I+D: 13 a 15 Alta; 9 a 12 Media; 3 a 8 Baja.
Clasificación de la información	Pública / Interna / Confidencial
Dependencias	Otros activos de los que depende (servidor, red, proveedor, energía).
Controles existentes	Medidas de protección aplicadas actualmente.
Grado de confiabilidad del dato	Verificado / Pendiente de validación técnica / No identificado
Observaciones	

Escala de valoración de impacto (confidencialidad, integridad y disponibilidad)

Valor	Nivel	Descripción del impacto para la institución
1	Muy bajo	Sin afectación apreciable a la operación ni a terceros.
2	Bajo	Afectación menor, resuelta con recursos propios en el día.
3	Medio	Interrupción parcial de un proceso o afectación a un grupo de usuarios.
4	Alto	Interrupción de un proceso crítico, pérdida de información relevante o incumplimiento legal.
5	Muy alto	Paralización de la recaudación o de la operación, exposición masiva de datos personales o sanciones.

Registro resumido del inventario (una fila por activo)

Código	Nombre del activo	Categoría	Propietario	Custodio	Estado	C	I	D	Criticidad

Anexo 4: Lista de verificación de cumplimiento de la norma ISO/IEC 27001:2022.

Instrumento de recolección de información. Técnica: lista de verificación normativa. Objetivos específicos a los que responde: OE2 y OE3. Escala de cumplimiento: Cumple (C) = requisito implementado y con evidencia; Parcial (P) = existen prácticas sin documentar o incompletas; No cumple (NC) = no existe; No aplica (NA) = excluido con justificación en la Declaración de Aplicabilidad.

Parte A. Requisitos de las cláusulas 4 a 10

Cláusula	Requisito	C/P/NC	Evidencia encontrada	Observaciones
4.1	Comprensión de la organización y de su contexto			
4.2	Comprensión de las necesidades y expectativas de las partes interesadas			
4.3	Determinación del alcance del SGSI			
4.4	Sistema de gestión de seguridad de la información			
5.1	Liderazgo y compromiso de la alta dirección			
5.2	Política de seguridad de la información			
5.3	Roles, responsabilidades y autoridades			
6.1.1	Acciones para abordar riesgos y oportunidades: generalidades			
6.1.2	Evaluación de riesgos de seguridad de la información			
6.1.3	Tratamiento de riesgos y Declaración de Aplicabilidad			
6.2	Objetivos de seguridad de la información y planificación para lograrlos			
6.3	Planificación de los cambios			
7.1	Recursos			
7.2	Competencia			
7.3	Toma de conciencia			
7.4	Comunicación			
7.5	Información documentada			
8.1	Planificación y control operacional			
8.2	Evaluación de riesgos de seguridad de la información			
8.3	Tratamiento de riesgos de seguridad de la información			
9.1	Seguimiento, medición, análisis y evaluación			
9.2	Auditoría interna			
9.3	Revisión por la dirección			
10.1	Mejora continua			
10.2	No conformidad y acción correctiva			

Parte B. Controles del Anexo A (ISO/IEC 27002:2022)

Control	Nombre del control	Aplica (Sí/No)	Estado (C/P/NC)	Evidencia / observaciones
A.5	**Controles organizacionales (37)**			
A.5.1	Políticas de seguridad de la información			
A.5.2	Roles y responsabilidades de seguridad de la información			
A.5.3	Segregación de funciones			
A.5.4	Responsabilidades de la dirección			
A.5.5	Contacto con las autoridades			
A.5.6	Contacto con grupos de interés especial			
A.5.7	Inteligencia de amenazas			
A.5.8	Seguridad de la información en la gestión de proyectos			
A.5.9	Inventario de información y otros activos asociados			
A.5.10	Uso aceptable de la información y otros activos asociados			
A.5.11	Devolución de activos			
A.5.12	Clasificación de la información			
A.5.13	Etiquetado de la información			
A.5.14	Transferencia de información			
A.5.15	Control de acceso			
A.5.16	Gestión de identidades			
A.5.17	Información de autenticación			
A.5.18	Derechos de acceso			
A.5.19	Seguridad de la información en las relaciones con proveedores			
A.5.20	Abordar la seguridad de la información en los acuerdos con proveedores			
A.5.21	Gestión de la seguridad de la información en la cadena de suministro de TIC			
A.5.22	Seguimiento, revisión y gestión de cambios de los servicios de proveedores			
A.5.23	Seguridad de la información para el uso de servicios en la nube			
A.5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información			
A.5.25	Evaluación y decisión sobre eventos de seguridad de la información			
A.5.26	Respuesta a incidentes de seguridad de la información			
A.5.27	Aprendizaje de los incidentes de seguridad de la información			
A.5.28	Recopilación de evidencias			
A.5.29	Seguridad de la información durante la disrupción			
A.5.30	Preparación de las TIC para la continuidad del negocio			
A.5.31	Requisitos legales, estatutarios, reglamentarios y contractuales			
A.5.32	Derechos de propiedad intelectual			

Control	Nombre del control	Aplica (Sí/No)	Estado (C/P/NC)	Evidencia / observaciones
A.5.33	Protección de registros			
A.5.34	Privacidad y protección de la información de identificación personal			
A.5.35	Revisión independiente de la seguridad de la información			
A.5.36	Cumplimiento de políticas, reglas y normas de seguridad de la información			
A.5.37	Procedimientos operativos documentados			
A.6	**Controles de personas (8)**			
A.6.1	Selección			
A.6.2	Términos y condiciones de empleo			
A.6.3	Concienciación, educación y formación en seguridad de la información			
A.6.4	Proceso disciplinario			
A.6.5	Responsabilidades tras la finalización o cambio de empleo			
A.6.6	Acuerdos de confidencialidad o no divulgación			
A.6.7	Trabajo remoto			
A.6.8	Notificación de eventos de seguridad de la información			
A.7	**Controles físicos (14)**			
A.7.1	Perímetros de seguridad física			
A.7.2	Entrada física			
A.7.3	Seguridad de oficinas, despachos e instalaciones			
A.7.4	Monitoreo de la seguridad física			
A.7.5	Protección contra amenazas físicas y ambientales			
A.7.6	Trabajo en áreas seguras			
A.7.7	Escritorio limpio y pantalla limpia			
A.7.8	Ubicación y protección de los equipos			
A.7.9	Seguridad de los activos fuera de las instalaciones			
A.7.10	Medios de almacenamiento			
A.7.11	Servicios de suministro			
A.7.12	Seguridad del cableado			
A.7.13	Mantenimiento de los equipos			
A.7.14	Eliminación segura o reutilización de los equipos			
A.8	**Controles tecnológicos (34)**			
A.8.1	Dispositivos de usuario final			
A.8.2	Derechos de acceso privilegiado			
A.8.3	Restricción de acceso a la información			
A.8.4	Acceso al código fuente			
A.8.5	Autenticación segura			
A.8.6	Gestión de la capacidad			
A.8.7	Protección contra el malware			

Control	Nombre del control	Aplica (Sí/No)	Estado (C/P/NC)	Evidencia / observaciones
A.8.8	Gestión de las vulnerabilidades técnicas			
A.8.9	Gestión de la configuración			
A.8.10	Eliminación de información			
A.8.11	Enmascaramiento de datos			
A.8.12	Prevención de fuga de datos			
A.8.13	Respaldo de la información			
A.8.14	Redundancia de las instalaciones de procesamiento de información			
A.8.15	Registro de eventos			
A.8.16	Actividades de monitoreo			
A.8.17	Sincronización de relojes			
A.8.18	Uso de programas utilitarios privilegiados			
A.8.19	Instalación de software en sistemas operativos			
A.8.20	Seguridad de las redes			
A.8.21	Seguridad de los servicios de red			
A.8.22	Segregación de las redes			
A.8.23	Filtrado web			
A.8.24	Uso de criptografía			
A.8.25	Ciclo de vida de desarrollo seguro			
A.8.26	Requisitos de seguridad de las aplicaciones			
A.8.27	Principios de arquitectura e ingeniería de sistemas seguros			
A.8.28	Codificación segura			
A.8.29	Pruebas de seguridad en desarrollo y aceptación			
A.8.30	Desarrollo externalizado			
A.8.31	Separación de los entornos de desarrollo, prueba y producción			
A.8.32	Gestión de cambios			
A.8.33	Información de prueba			
A.8.34	Protección de los sistemas de información durante las pruebas de auditoría			

Resumen del cumplimiento: controles aplicables ____ ; implementados ____ ; parciales ____ ; no implementados ____ ; porcentaje de cumplimiento = (implementados + 0,5 × parciales) / aplicables × 100.

Anexo 5: Manual de Políticas del Sistema de Gestión de Seguridad de la Información de la EMMAIPC-EP.

EMPRESA PÚBLICA MUNICIPAL MANCOMUNADA DE ASEO INTEGRAL DE LOS CANTONES CAÑAR, BIBLIÁN, EL TAMBO Y SUSCAL
EMMAIPC-EP

MANUAL

MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Basado en la norma ISO/IEC 27001:2022

Código:	MP-SGSI-EMMAIPC-EP-001
Versión:	1.0
Fecha de la versión:	Por definir
Clasificación de la información:	Uso interno
Estado:	Propuesta sujeta a aprobación de la Gerencia General

Cañar – Ecuador

Registro de firmas

Tabla 1. Registro de firmas

Creado por/ Modificado por	Revisado por	Aprobado por
Responsable de Seguridad de la Información	Comité de Seguridad de la Información	Gerencia General
Fecha:	**Fecha:**	**Fecha:**

El presente manual entra en vigencia a partir de su aprobación mediante resolución de la Gerencia General y su comunicación formal a todo el personal de la institución. Toda copia impresa se considera documento no controlado.

Historial de modificaciones

Tabla 2. Historial de modificaciones

Fecha	Versión	Creado por/ Modificado por	Descripción de la modificación
Por definir	1.0	Autor del trabajo de titulación	Emisión inicial del manual como producto del diseño del SGSI.

Identificación del documento

Tabla 3. Identificación del documento

Campo	Detalle
Título	Manual de Políticas del Sistema de Gestión de Seguridad de la Información
Código	MP-SGSI-EMMAIPC-EP-001
Versión	1.0
Estado	Propuesta sujeta a aprobación de la Gerencia General
Clasificación	Uso interno
Ámbito de aplicación	Todas las unidades administrativas y operativas de la EMMAIPC-EP

Campo	Detalle
Norma de referencia	ISO/IEC 27001:2022; controles del Anexo A conforme a la ISO/IEC 27002:2022
Periodicidad de revisión	Anual, o ante cambios significativos en el contexto institucional

Índice

1. OBJETO **4**
2. ALCANCE **4**
3. MARCO LEGAL Y NORMATIVO **4**
4. DEFINICIONES **5**
5. ROLES Y RESPONSABILIDADES **6**
6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN **7**
7. POLÍTICAS ESPECÍFICAS **8**
POL-01. Gestión de activos de información 8
POL-02. Control de acceso 9
POL-03. Respaldo y recuperación de la información 10
POL-04. Seguridad de redes y comunicaciones 10
POL-05. Relación con proveedores y servicios en la nube 11
POL-06. Gestión de incidentes de seguridad de la información 12
POL-07. Seguridad del personal 13
POL-08. Protección de datos personales 14
8. CUMPLIMIENTO, EXCEPCIONES Y RÉGIMEN DISCIPLINARIO **16**
9. SEGUIMIENTO Y MEDICIÓN **16**
10. VIGENCIA, REVISIÓN Y ACTUALIZACIÓN **17**
ANEXO. MATRIZ DE TRAZABILIDAD POLÍTICA – RIESGO – CONTROL **18**
1. OBJETO **3**
2. ALCANCE **3**
3. MARCO LEGAL Y NORMATIVO **3**
4. DEFINICIONES **3**
5. ROLES Y RESPONSABILIDADES **3**
6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN **3**
7. POLÍTICAS ESPECÍFICAS **3**
POL-01. Gestión de activos de información 3
POL-02. Control de acceso 3
POL-03. Respaldo y recuperación de la información 3
POL-04. Seguridad de redes y comunicaciones 3
POL-05. Relación con proveedores y servicios en la nube 3
POL-06. Gestión de incidentes de seguridad de la información 3
POL-07. Seguridad del personal 3
POL-08. Protección de datos personales 3
8. CUMPLIMIENTO, EXCEPCIONES Y RÉGIMEN DISCIPLINARIO **3**
9. SEGUIMIENTO Y MEDICIÓN **3**
10. VIGENCIA, REVISIÓN Y ACTUALIZACIÓN **3**
ANEXO. MATRIZ DE TRAZABILIDAD POLÍTICA – RIESGO – CONTROL **3**

1. OBJETO

Establecer el conjunto de políticas de seguridad de la información que rigen la protección de los activos de información de la Empresa Pública Municipal Mancomunada de Aseo Integral de los cantones Cañar, Biblián, El Tambo y Suscal, con el fin de preservar su confidencialidad, integridad y disponibilidad, gestionar de manera sistemática los riesgos que los afectan y dar cumplimiento a las obligaciones legales y reglamentarias aplicables a la institución.

Este manual constituye el instrumento normativo interno del Sistema de Gestión de Seguridad de la Información y desarrolla los requisitos establecidos en las cláusulas 5, 6, 7 y 8 de la norma ISO/IEC 27001:2022.

2. ALCANCE

Las disposiciones de este manual son de cumplimiento obligatorio para todos los servidores públicos de la EMMAIPC-EP, cualquiera sea su modalidad de vinculación, así como para contratistas, proveedores, pasantes y terceros que accedan a la información o a los recursos tecnológicos institucionales.

El alcance comprende los procesos administrativos, financieros, tributarios y documentales soportados por los sistemas Flectra ERP 3.0 y e-Doc Manager, la infraestructura de servidor, red, almacenamiento y equipos de usuario final que los sustenta, los servicios en la nube contratados, y las instalaciones de la matriz institucional y de las cuatro zonas operativas.

Se excluyen del alcance los aspectos no informáticos de los procesos operativos de barrido, recolección y disposición final de residuos, la infraestructura propia de los municipios mancomunados, y la información de carácter estrictamente personal de los servidores no vinculada a procesos institucionales.

3. MARCO LEGAL Y NORMATIVO

El presente manual se sustenta en las siguientes disposiciones legales y técnicas:

- Constitución de la República del Ecuador, en lo relativo al derecho a la protección de datos de carácter personal.
- Ley Orgánica de Protección de Datos Personales y su reglamento, respecto de las obligaciones de la institución como responsable del tratamiento.
- Ley Orgánica de Transparencia y Acceso a la Información Pública.
- Ley Orgánica de Empresas Públicas, en lo referente al régimen jurídico institucional.
- Esquema Gubernamental de Seguridad de la Información, aplicable a las entidades del sector público.
- Normas de Control Interno para las entidades y organismos del sector público, en materia de tecnología de la información.

- Norma ISO/IEC 27001:2022, requisitos del sistema de gestión de seguridad de la información.
- Norma ISO/IEC 27002:2022, directrices de implementación de los controles del Anexo A.
- Norma ISO/IEC 27005:2022, orientación para la gestión de riesgos de seguridad de la información.
- Plan Estratégico Institucional de la EMMAIPC-EP 2026–2030.

4. DEFINICIONES

Tabla 4. Términos empleados en el presente manual

Término	Definición
Activo de información	Todo recurso que contiene o procesa información con valor para la institución: bases de datos, aplicaciones, equipos, servicios, instalaciones y personas.
Confidencialidad	Propiedad por la cual la información no se pone a disposición de personas o procesos no autorizados.
Integridad	Propiedad de exactitud y completitud de la información.
Disponibilidad	Propiedad de ser accesible y utilizable por una entidad autorizada cuando lo requiera.
Propietario del activo	Servidor con la responsabilidad de autorizar el uso del activo, definir sus reglas de acceso y aprobar el tratamiento de sus riesgos.
Custodio	Unidad o servidor encargado de la administración técnica y la aplicación de los controles sobre el activo.
Riesgo	Efecto de la incertidumbre sobre los objetivos de seguridad de la información, determinado por la combinación de probabilidad e impacto.
Riesgo residual	Nivel de riesgo que subsiste tras la aplicación de los controles.
Incidente de seguridad	Evento o serie de eventos que compromete la confidencialidad, integridad o disponibilidad de la información.
Datos personales	Información concerniente a una persona natural identificada o identificable.
Declaración de Aplicabilidad	Documento que registra los controles del Anexo A aplicables, su justificación y estado de implementación.
SGSI	Sistema de Gestión de Seguridad de la Información.

5. ROLES Y RESPONSABILIDADES

En cumplimiento del numeral 5.3 de la norma ISO/IEC 27001:2022, y considerando que la Unidad de Tecnologías de la Información y Comunicación está conformada por un solo servidor público, las responsabilidades del sistema se distribuyen entre las direcciones existentes conforme se detalla a continuación, sin crear nuevas unidades administrativas.

Tabla 5. Estructura de roles del SGSI

Rol	Asignación	Responsabilidades principales
Alta dirección	Gerencia General	Aprobar el presente manual, el alcance del sistema y los criterios de aceptación del riesgo; asignar recursos; aceptar formalmente los riesgos residuales que superen el umbral establecido.
Comité de Seguridad de la Información	Gerencia General, Dirección Administrativa Financiera, Dirección Técnica, Talento Humano, Procuraduría Síndica y Unidad de TIC	Revisar el desempeño del sistema, priorizar el tratamiento de riesgos, aprobar excepciones y resolver conflictos de recursos. Sesiona de manera trimestral y de forma extraordinaria ante incidentes graves.
Responsable de Seguridad de la Información	Servidor designado mediante acción de personal, con dedicación parcial	Coordinar la operación del sistema, mantener actualizada la Declaración de Aplicabilidad y la matriz de riesgos, gestionar los incidentes, ejecutar el programa de concienciación y reportar los indicadores al Comité.
Propietarios de activos de información	Directores y responsables de proceso	Autorizar el uso y el acceso a sus activos, aprobar su clasificación, validar el tratamiento de sus riesgos y solicitar oportunamente las altas y bajas de acceso.
Custodio técnico	Unidad de Tecnologías de la Información y Comunicación	Administrar la infraestructura, aplicar los controles técnicos, ejecutar y verificar los respaldos, mantener los registros de eventos y atender los requerimientos de acceso autorizados.
Administrador de contratos tecnológicos	Unidad de TIC en coordinación con Compras Públicas y Procuraduría Síndica	Verificar el cumplimiento de las cláusulas de seguridad, los niveles de servicio y las condiciones de reversibilidad pactadas con los proveedores.
Usuarios de la información	Todo el personal, contratistas y terceros autorizados	Cumplir las políticas del presente manual, proteger las credenciales asignadas y reportar de inmediato los eventos de seguridad que detecten.

6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La EMMAIPC-EP reconoce la información como un activo estratégico para la prestación del servicio público de aseo integral y declara su compromiso de preservar la confidencialidad, integridad y disponibilidad de la información que genera, procesa, almacena y transmite, mediante un Sistema de Gestión de Seguridad de la Información conforme a la norma ISO/IEC 27001:2022.

Para materializar este compromiso, la institución asume los siguientes principios:

1. Cumplir los requisitos legales, reglamentarios y contractuales aplicables en materia de seguridad de la información y protección de datos personales.
2. Gestionar los riesgos de seguridad de la información mediante un proceso sistemático y documentado de identificación, análisis, evaluación y tratamiento.
3. Asignar un propietario a cada activo de información y establecer responsabilidades definidas para su protección.
4. Otorgar los accesos conforme a los principios de mínimo privilegio y necesidad de conocer.
5. Garantizar la continuidad de los procesos institucionales críticos mediante respaldos verificados y mecanismos de recuperación probados.
6. Proporcionar los recursos humanos, tecnológicos y financieros necesarios para la operación, el mantenimiento y la mejora continua del sistema.
7. Promover la concienciación y la formación permanente del personal en materia de seguridad de la información.
8. Gestionar los incidentes de seguridad de manera oportuna, documentada y orientada al aprendizaje institucional.
9. Establecer condiciones contractuales de seguridad, niveles de servicio y reversibilidad con todos los proveedores de servicios tecnológicos.
10. Medir periódicamente el desempeño del sistema mediante indicadores y adoptar las acciones correctivas que correspondan.

El incumplimiento de esta política y de las políticas específicas que la desarrollan será tratado conforme al régimen disciplinario aplicable y, cuando corresponda, conforme a la responsabilidad civil, administrativa o penal prevista en el ordenamiento jurídico.

7. POLÍTICAS ESPECÍFICAS

La política general se desarrolla mediante ocho políticas específicas de aplicación obligatoria, que se presentan a continuación.

POL-01. Gestión de activos de información

Objetivo. Garantizar que todos los activos de información de la institución se encuentren identificados, valorados, clasificados y bajo la responsabilidad de un propietario designado.

Alcance. Aplica a la totalidad de los activos de información incluidos en el alcance del SGSI, en cualquier soporte y durante todo su ciclo de vida.

Lineamientos:

11. La institución mantendrá un inventario de activos de información actualizado, que registre como mínimo el código, la denominación, el tipo, el propietario, el custodio, la ubicación, la valoración en confidencialidad, integridad y disponibilidad, y el estado del activo.
12. El inventario de activos de información se mantendrá conciliado con el inventario patrimonial de bienes, sin sustituirlo; cada uno responde a finalidades distintas.
13. Todo activo de información contará con un propietario formalmente designado, responsable de autorizar su uso, aprobar su clasificación y validar el tratamiento de sus riesgos.
14. La información se clasificará en los niveles pública, de uso interno, confidencial y reservada, atendiendo al impacto de su divulgación no autorizada y al régimen legal aplicable.
15. Los documentos y medios que contengan información confidencial o reservada serán etiquetados de forma visible, y su manipulación, transmisión y almacenamiento se sujetarán a las medidas definidas para su nivel.
16. El uso de los recursos tecnológicos institucionales se limitará a fines relacionados con las funciones asignadas; queda prohibida la instalación de software sin autorización de la Unidad de TIC.
17. Al cesar en funciones, todo servidor devolverá los activos asignados y sus accesos serán revocados de manera inmediata, conforme al procedimiento de baja.
18. Los activos que superen su vida útil o resulten obsoletos serán dados de baja previo borrado seguro o destrucción física de los medios de almacenamiento, dejando constancia documental del procedimiento.
19. El inventario será revisado al menos una vez al año y actualizado cada vez que se produzcan altas, bajas o cambios de custodio.

Responsable de su aplicación: Propietarios de activos, con apoyo de la Unidad de TIC y de la Dirección Administrativa Financiera.

Controles asociados del Anexo A de la norma ISO/IEC 27001:2022: A.5.9, A.5.10, A.5.11, A.5.12, A.5.13, A.7.10, A.7.14, A.8.1.

POL-02. Control de acceso

Objetivo. Asegurar que el acceso a la información y a los recursos tecnológicos se otorgue únicamente a personas autorizadas, en la medida estrictamente necesaria para el desempeño de sus funciones.

Alcance. Aplica a todos los accesos lógicos y remotos a sistemas, bases de datos, servicios en la nube, equipos y redes de la institución.

Lineamientos:

20. El acceso se otorgará bajo los principios de mínimo privilegio y necesidad de conocer, previa solicitud formal del propietario del activo y autorización del jefe inmediato.
21. Cada usuario dispondrá de una identidad única e intransferible; queda prohibido el uso de cuentas compartidas o genéricas, salvo excepción justificada y aprobada por el Comité de Seguridad de la Información.
22. Las contraseñas tendrán una longitud mínima de doce caracteres, combinarán mayúsculas, minúsculas, números y caracteres especiales, y no reutilizarán las cinco anteriores.
23. Las contraseñas son personales y confidenciales; su divulgación, préstamo o registro en soportes visibles constituye una falta a la presente política.
24. En los sistemas que lo permitan, en particular Flectra ERP y e-Doc Manager, se habilitará el segundo factor de autenticación para las cuentas con privilegios administrativos.
25. Las cuentas con privilegios administrativos serán nominativas, se otorgarán de forma excepcional, se registrarán en un inventario específico y su uso quedará sujeto a registro de eventos.
26. Los derechos de acceso serán revisados de manera trimestral por el propietario del activo, quien dejará constancia documental de la revisión y solicitará las revocaciones que correspondan.
27. Las altas, modificaciones y bajas de acceso se ejecutarán dentro de las veinticuatro horas siguientes a la notificación de vinculación, cambio de funciones o desvinculación remitida por la Dirección de Talento Humano.
28. El acceso remoto a los recursos institucionales se realizará únicamente a través de canales cifrados autorizados por la Unidad de TIC.
29. Las sesiones inactivas se bloquearán automáticamente transcurridos quince minutos y los intentos fallidos de autenticación bloquearán la cuenta tras cinco intentos consecutivos.

Responsable de su aplicación: Unidad de TIC, con autorización de los propietarios de activos y notificación de la Dirección de Talento Humano.

Controles asociados del Anexo A de la norma ISO/IEC 27001:2022: A.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.3, A.8.5.

POL-03. Respaldo y recuperación de la información

Objetivo. Garantizar la disponibilidad e integridad de la información institucional mediante copias de respaldo suficientes, protegidas y verificadas, que permitan su recuperación ante cualquier incidente.

Alcance. Aplica a la información contenida en Flectra ERP, e-Doc Manager, archivos institucionales, configuraciones de equipos de red y cualquier otro activo calificado como crítico o de criticidad alta.

Lineamientos:

30. Se ejecutarán respaldos diarios incrementales y semanales completos de la información de los sistemas críticos, y respaldos posteriores a cada cambio en las configuraciones de los equipos de red.
31. Se conservará un mínimo de treinta respaldos diarios, doce semanales y doce mensuales, sin perjuicio de los plazos de conservación que establezca la normativa de archivo aplicable.
32. Se aplicará el esquema de al menos tres copias de la información en dos medios distintos, con una copia fuera de las instalaciones de la matriz institucional.
33. Los respaldos que contengan datos personales o información clasificada como confidencial o reservada serán cifrados tanto en tránsito como en reposo.
34. Se establecen como objetivos de recuperación un tiempo máximo de cuatro horas y una pérdida máxima de información de veinticuatro horas para los sistemas de emisión, facturación y recaudación, valores que serán ratificados o ajustados por el Comité de Seguridad de la Información.
35. Se ejecutará al menos una prueba trimestral de restauración por cada sistema crítico, de la cual se levantará un informe que registre la fecha, el alcance, el tiempo empleado, el resultado y las observaciones detectadas.
36. Un respaldo cuya restauración no haya sido verificada mediante prueba documentada no se considerará un respaldo válido para efectos de esta política.
37. Cuando el respaldo esté a cargo de un proveedor, la institución exigirá evidencia periódica de su ejecución y la posibilidad de solicitar una exportación completa de la información en formato utilizable.
38. El acceso a los medios de respaldo se restringirá al custodio técnico y al Responsable de Seguridad de la Información, y quedará registrado.

Responsable de su aplicación: Unidad de TIC, con verificación del Responsable de Seguridad de la Información.

Controles asociados del Anexo A de la norma ISO/IEC 27001:2022: A.8.13, A.8.14, A.5.29, A.5.30, A.5.33.

POL-04. Seguridad de redes y comunicaciones

Objetivo. Proteger la infraestructura de red institucional y la información transmitida a través de ella frente a accesos no autorizados, interceptación e interrupciones del servicio.

Alcance. Aplica a la red cableada e inalámbrica de la matriz y de las zonas operativas, a los equipos de comunicación, a los enlaces contratados y a los accesos remotos.

Lineamientos:

39. La institución mantendrá actualizados los diagramas físico y lógico de la red, así como el registro del direccionamiento, los enlaces contratados y las configuraciones vigentes.
40. Se implementará un cortafuegos perimetral que controle el tráfico entrante y saliente bajo el principio de denegación por defecto, permitiendo únicamente los servicios expresamente autorizados.
41. La red se segmentará mediante redes virtuales que separen, como mínimo, el segmento administrativo, el segmento de servidores, el segmento de invitados y el segmento de dispositivos de control como biométricos y videovigilancia.
42. La red inalámbrica de invitados estará aislada de la red institucional y no permitirá el acceso a sistemas internos.
43. Toda modificación en la configuración de los equipos de red requerirá autorización previa, quedará documentada y se respaldará inmediatamente después de su aplicación.
44. Se habilitará el registro de eventos de los equipos de red y de los servidores, con una conservación mínima de seis meses, y se revisará al menos de forma mensual.
45. Las credenciales por defecto de todo equipo de comunicaciones serán modificadas antes de su puesta en producción.
46. La transmisión de información clasificada como confidencial o reservada se realizará exclusivamente por canales cifrados.
47. Los equipos de comunicación que no cuenten con soporte del fabricante serán identificados y programados para su reemplazo dentro del plan anual de renovación.

Responsable de su aplicación: Unidad de TIC.

Controles asociados del Anexo A de la norma ISO/IEC 27001:2022: A.8.20, A.8.21, A.8.22, A.8.23, A.8.9, A.8.15, A.8.16.

POL-05. Relación con proveedores y servicios en la nube

Objetivo. Asegurar que la información institucional gestionada por terceros mantenga los niveles de protección exigidos por la institución y que esta conserve el control efectivo sobre sus activos.

Alcance. Aplica a todo contrato, convenio u orden de compra que implique el acceso, procesamiento, almacenamiento o administración de información o recursos tecnológicos de la institución.

Lineamientos:

48. Todo instrumento contractual de servicios tecnológicos incorporará cláusulas de confidencialidad, niveles de servicio medibles, obligaciones de seguridad, notificación de incidentes y condiciones de reversibilidad y devolución de la información.

49. La titularidad de la información institucional alojada o procesada por terceros corresponde en todo caso a la EMMAIPC-EP y así deberá constar expresamente en el contrato.
50. Las cuentas administrativas de los servicios en la nube que alojen información institucional estarán a nombre de la EMMAIPC-EP, y la institución conservará las credenciales de administración principal.
51. Cuando por razones técnicas o contractuales la administración recaiga transitoriamente en el proveedor, la Unidad de TIC gestionará su transferencia dentro del plazo aprobado por la Gerencia General y mantendrá un registro de la excepción.
52. Se mantendrá un registro consolidado de proveedores tecnológicos que incluya el objeto, el instrumento, el administrador del contrato, la vigencia, el nivel de criticidad y la fecha de renovación.
53. Se llevará un calendario institucional de vencimientos de garantías, licencias y suscripciones, con alerta anticipada de al menos sesenta días.
54. El administrador del contrato evaluará semestralmente el cumplimiento de los niveles de servicio y de las obligaciones de seguridad, y dejará constancia documental de la evaluación.
55. Antes de la finalización de cualquier contrato se ejecutará una prueba de exportación completa de la información, verificando que el formato entregado sea utilizable por la institución.
56. El acceso remoto de proveedores a los sistemas institucionales será nominativo, temporal, autorizado por escrito y sujeto a registro de actividad.

Responsable de su aplicación: Administrador del contrato tecnológico, con asesoría de Procuraduría Síndica y verificación de la Unidad de TIC.

Controles asociados del Anexo A de la norma ISO/IEC 27001:2022: A.5.19, A.5.20, A.5.21, A.5.22, A.5.23, A.8.30.

POL-06. Gestión de incidentes de seguridad de la información

Objetivo. Establecer un procedimiento uniforme para el reporte, la clasificación, la respuesta y el registro de los incidentes de seguridad, que permita reducir su impacto y prevenir su recurrencia.

Alcance. Aplica a todo evento que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad de la información institucional, incluidos los que involucren datos personales.

Lineamientos:

57. Todo servidor, contratista o tercero está obligado a reportar de inmediato cualquier evento sospechoso al Responsable de Seguridad de la Información, mediante el canal institucional definido.
58. El reporte oportuno y de buena fe no dará lugar a sanción, aun cuando el evento haya tenido origen en un error del propio reportante.

59. Los incidentes se clasificarán en cuatro niveles de severidad: crítico, alto, medio y bajo, atendiendo al impacto sobre los procesos institucionales y a la afectación de datos personales.
60. Los incidentes críticos serán atendidos de forma inmediata y comunicados a la Gerencia General dentro de las dos horas siguientes a su confirmación.
61. Cuando el incidente involucre una vulneración de datos personales, se activará el procedimiento de notificación a la autoridad de protección de datos y a los titulares afectados dentro de los plazos establecidos por la Ley Orgánica de Protección de Datos Personales.
62. Se conservará y protegerá la evidencia digital asociada al incidente, preservando su integridad y su cadena de custodia para efectos de investigación o acción legal.
63. Todo incidente quedará registrado en la bitácora institucional de incidentes, con su descripción, causa raíz, acciones ejecutadas, tiempo de resolución y lecciones aprendidas.
64. El Responsable de Seguridad de la Información presentará un informe trimestral de incidentes al Comité, con el análisis de tendencias y las acciones preventivas propuestas.
65. Las causas raíz identificadas darán lugar a acciones correctivas registradas y verificadas conforme a la cláusula 10 de la norma.

Responsable de su aplicación: Responsable de Seguridad de la Información, con apoyo de la Unidad de TIC.

Controles asociados del Anexo A de la norma ISO/IEC 27001:2022: A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.6.8, A.5.7.

POL-07. Seguridad del personal

Objetivo. Reducir los riesgos derivados del factor humano mediante la definición de responsabilidades, la suscripción de compromisos de confidencialidad y la formación continua del personal.

Alcance. Aplica a todo el personal de la institución en las fases previa, durante y posterior a la relación laboral o contractual.

Lineamientos:

66. Toda vinculación laboral o contractual incluirá la suscripción de un acuerdo de confidencialidad cuya vigencia se extenderá más allá de la terminación de la relación.
67. Las responsabilidades en materia de seguridad de la información se incorporarán a los perfiles de puesto y a los contratos de servicios.
68. Todo servidor recibirá inducción en seguridad de la información y protección de datos personales dentro de los treinta días siguientes a su incorporación.
69. Se ejecutará un programa anual de concienciación dirigido a la totalidad del personal, que abordará como mínimo el manejo de contraseñas, la identificación de correos fraudulentos, el uso de dispositivos externos y el tratamiento de datos personales.

70. Se aplicará el principio de escritorio y pantalla despejados: los documentos con información confidencial no permanecerán a la vista y las estaciones de trabajo se bloquearán al ausentarse del puesto.
71. En la medida en que la estructura institucional lo permita, se segregarán las funciones de solicitud, autorización y ejecución de los accesos, con el fin de evitar la concentración de facultades incompatibles.
72. Cuando la segregación de funciones no sea posible por la conformación de la unidad técnica, se aplicarán controles compensatorios de registro y revisión periódica por parte de un servidor distinto al ejecutante.
73. Los procedimientos técnicos críticos serán documentados de manera que cualquier servidor con la competencia adecuada pueda ejecutarlos, evitando la dependencia de una sola persona.
74. En el proceso de desvinculación, la Dirección de Talento Humano notificará a la Unidad de TIC con anticipación, a efectos de la revocación de accesos y la devolución de los activos asignados.

Responsable de su aplicación: Dirección de Talento Humano, en coordinación con el Responsable de Seguridad de la Información.

Controles asociados del Anexo A de la norma ISO/IEC 27001:2022: A.6.1, A.6.2, A.6.3, A.6.4, A.6.5, A.6.6, A.6.7, A.7.7.

POL-08. Protección de datos personales

Objetivo. Garantizar que el tratamiento de datos personales efectuado por la institución se ajuste a los principios y obligaciones establecidos en la Ley Orgánica de Protección de Datos Personales.

Alcance. Aplica al tratamiento de datos personales de contribuyentes, usuarios del servicio, servidores públicos, proveedores y cualquier otro titular cuya información sea tratada por la institución.

Lineamientos:

75. El tratamiento de datos personales se realizará únicamente cuando exista una base de licitud válida, principalmente el cumplimiento de una obligación legal o el ejercicio de competencias propias de la institución.
76. Los datos personales se recabarán para finalidades determinadas, explícitas y legítimas, y no serán tratados posteriormente de manera incompatible con dichas finalidades.
77. Se aplicará el principio de minimización: únicamente se recabarán y conservarán los datos estrictamente necesarios para la finalidad perseguida.
78. La institución mantendrá un registro de las actividades de tratamiento que identifique la finalidad, las categorías de titulares y de datos, los destinatarios, los plazos de conservación y las medidas de seguridad aplicadas.
79. Se garantizará el ejercicio de los derechos de acceso, rectificación, actualización, eliminación, oposición, portabilidad y suspensión, mediante un procedimiento y un canal institucional publicados.

80. Los datos personales conservados en los sistemas Flectra ERP, e-Doc Manager y en los dispositivos biométricos contarán con controles de acceso restringido y con cifrado en los respaldos.
81. Toda transferencia o comunicación de datos personales a terceros se sustentará en un instrumento que regule la condición de encargado del tratamiento y las medidas de seguridad exigidas.
82. Los datos personales serán suprimidos o anonimizados una vez cumplida la finalidad que motivó su tratamiento y transcurridos los plazos de conservación legalmente exigibles.
83. Las vulneraciones de seguridad que afecten datos personales se gestionarán conforme a la política POL-06 y serán notificadas en los plazos legales.
84. Toda nueva iniciativa que implique un tratamiento de datos personales de alto riesgo será evaluada previamente por el Responsable de Seguridad de la Información en coordinación con Procuraduría Síndica.

Responsable de su aplicación: Propietarios de datos personales, con asesoría de Procuraduría Síndica y del Responsable de Seguridad de la Información.

Controles asociados del Anexo A de la norma ISO/IEC 27001:2022: A.5.34, A.5.31, A.5.36, A.8.10, A.8.11, A.8.12, A.8.24.

8. CUMPLIMIENTO, EXCEPCIONES Y RÉGIMEN DISCIPLINARIO

El cumplimiento de las políticas contenidas en el presente manual es obligatorio. Su inobservancia será puesta en conocimiento de la autoridad nominadora para el inicio de las acciones administrativas que correspondan, sin perjuicio de la responsabilidad civil o penal derivada de los hechos.

Toda excepción al cumplimiento de una disposición del presente manual deberá ser solicitada por escrito, con justificación técnica y temporalidad definida, y será aprobada por el Comité de Seguridad de la Información. Las excepciones aprobadas se registrarán, se someterán a controles compensatorios y serán revisadas en cada sesión ordinaria del Comité.

El Responsable de Seguridad de la Información verificará periódicamente el cumplimiento de las políticas mediante revisiones documentales y técnicas, cuyos resultados serán incorporados al informe de desempeño del sistema.

9. SEGUIMIENTO Y MEDICIÓN

El desempeño de las políticas contenidas en este manual se medirá mediante los indicadores que se detallan a continuación, cuyos valores se compararán con la línea base establecida en el diagnóstico institucional.

Tabla 6. Indicadores de cumplimiento del manual de políticas

Indicador	Política	Línea base	Meta año 1	Frecuencia
Activos de información con propietario asignado	POL-01	0 %	100 %	Semestral
Revisiones de derechos de acceso ejecutadas	POL-02	0 %	100 %	Trimestral
Pruebas de restauración exitosas	POL-03	0 de 0	4 de 4	Trimestral
Segmentos de red implementados y documentados	POL-04	0	4	Semestral
Contratos con cláusulas de seguridad y niveles de servicio	POL-05	0 %	100 %	Semestral
Incidentes registrados y cerrados	POL-06	No medible	90 %	Mensual
Personal capacitado en seguridad de la información	POL-07	0 %	80 %	Anual
Actividades de tratamiento de datos personales registradas	POL-08	0	Todas	Semestral

10. VIGENCIA, REVISIÓN Y ACTUALIZACIÓN

El presente manual entra en vigencia desde la fecha de su aprobación mediante resolución de la Gerencia General y permanecerá vigente hasta que sea sustituido por una versión posterior.

El manual será revisado al menos una vez al año por el Comité de Seguridad de la Información. Adicionalmente, será revisado de manera extraordinaria cuando se produzcan cambios significativos en la estructura institucional, en la plataforma tecnológica, en el marco legal aplicable, o cuando se registre un incidente de severidad crítica.

Toda modificación generará una nueva versión, que será registrada en la tabla de control de versiones, aprobada por la Gerencia General y comunicada a todo el personal. Las versiones anteriores se conservarán como registro histórico del sistema.

ANEXO. MATRIZ DE TRAZABILIDAD POLÍTICA – RIESGO – CONTROL

La siguiente matriz vincula cada política del presente manual con los riesgos identificados en el análisis de riesgos institucional y con los controles del Anexo A de la norma ISO/IEC 27001:2022 seleccionados para su tratamiento.

Tabla 7. Trazabilidad entre políticas, riesgos y controles

Política	Riesgos que atiende	Controles principales	Responsable
POL-01. Gestión de activos de información	RG-06, RG-08, RG-13	A.5.9 a A.5.13; A.7.14; A.8.1	Propietarios de activos
POL-02. Control de acceso	RG-05, RG-08, RG-12	A.5.15 a A.5.18; A.8.2; A.8.5	Unidad de TIC
POL-03. Respaldo y recuperación	RG-02, RG-01	A.8.13; A.8.14; A.5.29; A.5.30	Unidad de TIC
POL-04. Seguridad de redes y comunicaciones	RG-03, RG-07, RG-11	A.8.20 a A.8.23; A.8.9; A.8.16	Unidad de TIC
POL-05. Proveedores y servicios en la nube	RG-01, RG-10, RG-16	A.5.19 a A.5.23; A.8.30	Administrador del contrato
POL-06. Gestión de incidentes	RG-11, RG-13	A.5.24 a A.5.28; A.6.8	Responsable de Seguridad
POL-07. Seguridad del personal	RG-04, RG-12	A.6.1 a A.6.7; A.7.7	Talento Humano
POL-08. Protección de datos personales	RG-08, RG-09, RG-13	A.5.34; A.5.31; A.5.36; A.8.24	Propietarios de datos

Los riesgos RG-14 y RG-15, relativos al acceso físico al área de servidores y a la interrupción del suministro eléctrico, se atienden mediante los controles físicos A.7.1 a A.7.6, A.7.11 y A.7.12, cuya aplicación corresponde a la Unidad de TIC en coordinación con la Dirección Administrativa Financiera y será desarrollada en el procedimiento específico de seguridad física.

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Kevin Alexander Cantos Espinoza portador de la cédula de ciudadanía Nº **0302390018** En calidad de autor y titular de los derechos patrimoniales del trabajo de titulación **"Diseño de un Sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la empresa EMMAIPC-EP"** 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 éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cañar, 30 **de septiembre de 2026**

Kevin Alexander Cantos Espinoza
C.I. **0302390018**