

**Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en las
normas ISO/IEC 27001 para la Personería Municipal de Armenia**

Lady Johanna Vera Torres

Asesor

Eduard Mantilla Torres

Universidad Nacional Abierta y a Distancia – UNAD

Escuela De Ciencias Básicas, Tecnología E Ingeniería - ECBTI

Especialización en Seguridad Informática

2025

Agradecimientos

Expreso mi más sincero agradecimiento a Dios y todas las personas Universidad Nacional Abierta y a Distancia UNAD, que contribuyeron a la realización de este trabajo de grado. En primer lugar, agradezco a la Personería Municipal de Armenia, por brindarme la oportunidad de desarrollar este proyecto en un entorno propicio para el aprendizaje y la aplicación de conocimientos. Su apoyo institucional y los medios materiales facilitados fueron fundamentales para llevar a cabo este estudio.

De igual manera, extendiendo mi gratitud a los docentes y tutores del programa, quienes, con su orientación académica y valiosas sugerencias, contribuyeron de manera significativa con su tiempo y disposición, ya sea en la revisión de contenidos, correcciones en la escritura o asistencia en aspectos metodológicos.

Dedicatoria

Este trabajo de grado está dedicado con profundo agradecimiento a Dios, mis padres, quienes, con su amor incondicional, esfuerzo y valores inculcados han sido el pilar fundamental en mi formación personal y profesional. A mi esposo, por su apoyo constante, su paciencia y por ser una fuente de motivación en cada paso de este camino.

Asimismo, extendiendo mi gratitud a la Personería Municipal de Armenia quienes brindaron su respaldo y confianza en el desarrollo de este proyecto, cuyo conocimiento, orientación y disposición fueron clave para estructurar esta iniciativa, la cual está diseñada para fortalecer la seguridad de la información en la entidad. Sus enseñanzas y colaboración han sido fundamentales para materializar esta propuesta, contribuyendo a la mejora y protección de los activos digitales de la organización.

Resumen

La seguridad de la información es un pilar clave para las entidades públicas, especialmente en la Personería Municipal de Armenia, donde la protección de datos sensibles fortalece la confianza ciudadana, garantiza el cumplimiento normativo y promueve la transparencia. En este contexto, se diseñó un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO/IEC 27001, adaptado al entorno institucional, tecnológico y normativo de la entidad.

El diagnóstico inicial permitió identificar debilidades técnicas y organizativas, especialmente en la gestión de activos, control de accesos, tratamiento de incidentes, continuidad del negocio y concienciación del personal. A partir de este análisis, se clasificaron los activos de información y se formularon políticas y procedimientos específicos para mitigar riesgos, garantizando la confidencialidad, integridad y disponibilidad de la información.

Además, se incorporó el marco de gobernanza COBIT para fortalecer la articulación entre la seguridad de la información y los objetivos institucionales, asignando funciones mediante una matriz RACI y proponiendo mecanismos de seguimiento y control como auditorías, indicadores y revisiones periódicas.

Los principales resultados incluyen el diseño estructurado del SGSI con su alcance y objetivos, la identificación y clasificación de activos, el análisis de brechas frente a ISO/IEC 27001, el mapa de riesgos, un plan de tratamiento, y un modelo de gobernanza basado en buenas prácticas. Este diseño establece una base sólida para su implementación futura, fomentando una cultura organizacional orientada a la seguridad, la eficiencia operativa y la mejora continua.

Palabras clave: Controles, ISO/IEC 27001, gestión de riesgos, gobernanza de TI, seguridad de la información.

Abstract

Information security is a key pillar for public entities, especially for the Municipal Ombudsman's Office of Armenia, where the protection of sensitive data strengthens citizen trust, ensures regulatory compliance, and promotes institutional transparency. In this context, an Information Security Management System (ISMS) was designed in alignment with the ISO/IEC 27001 standard, tailored to the institutional, technological, and regulatory environment of the entity.

The initial assessment identified technical and organizational weaknesses, particularly in asset management, access control, incident handling, business continuity, and staff awareness. Based on this analysis, information assets were classified, and specific policies and procedures were formulated to mitigate risks, ensuring confidentiality, integrity, and availability of information.

Additionally, the COBIT governance framework was incorporated to strengthen the alignment between information security and institutional objectives, assigning roles through a RACI matrix and proposing monitoring and control mechanisms such as audits, indicators, and periodic reviews.

The main outcomes include a structured ISMS design with defined scope and objectives, asset identification and classification, a gap analysis against ISO/IEC 27001, a risk map, a risk treatment plan, and a governance model based on best practices. This design establishes a solid foundation for future implementation, fostering an organizational culture focused on security, operational efficiency, and continuous improvement.

Keywords: Controls, information security, ISO/IEC 27001, IT governance, risk management.

Tabla de Contenido

Introducción.....	14
Definición del problema	16
Justificación	19
Objetivos.....	21
Objetivo General.....	21
Objetivos Específicos	21
Marco Referencial	22
Antecedentes.....	22
Marco Conceptual.....	26
Control Objectives for Information and Related Technologies COBIT.....	26
Confidencialidad.....	27
Control de Seguridad	27
Disponibilidad.....	27
Infraestructura Tecnológica	28
Integridad.....	28
ISO/IEC 27000	28
ISO/IEC 27001	29
ISO/IEC 27002	30
ISO/IEC 27005	30
Magerit	30
NIST	31
Política de la Seguridad de la Información.....	31

Sistema de Gestión de Seguridad de la Información	31
Marco Teórico	32
Gestión de la Información y su Importancia en las Organizaciones.....	32
Riesgos y Vulnerabilidades en la Gestión de la Información.....	32
La Gestión de Riesgos como Estrategia de Protección de la Información	33
El Sistema de Gestión de Seguridad de la Información (SGSI) y la ISO/IEC 27001	34
Metodología Magerit y su Aplicación en la Gestión de Riesgos	34
Gobernanza de Tecnologías de la Información (TI) y su Relación con el SGSI.....	35
Criterios para la Selección del Marco Normativo de Seguridad	35
Marco Legal.....	37
Marco Contextual	40
Marco Histórico	46
Marco Científico	47
Diseño Metodológico.....	49
Tipo de Investigación	49
Enfoque Investigativo	50
Población y Muestra	51
Variables de la Investigación	52
Técnicas e Instrumentos de Recolección de Información.....	52
Fuentes Primarias	53
Fuentes Secundarias:	53
Metodología de Análisis de Riesgos.....	53
Herramientas de Apoyo	53

Variables Clave.....	54
Hipótesis	56
Desarrollo de los Objetivos	58
Realizar un Diagnóstico del Estado Actual de la Seguridad de la Información en la Personería Municipal de Armenia.....	58
Análisis del Entorno	58
Diagnostico Organizacional.....	60
Inventario de Activos	74
Aplicar una Metodología de Gestión de Riesgos para Identificar, Valorar y Clasificar los Riesgos Asociados a los Activos de Información.....	79
Valoración Cualitativa de los Activos	80
Valoración Cuantitativa de los Activos	90
Amenazas y Vulnerabilidades	94
Mapa de Riesgos.....	119
Plan de Tratamiento de Riesgos	121
Evaluar el Nivel de Madurez de los Controles de Seguridad de la Información Mediante un Análisis GAP Estructurado.....	144
Análisis General del Estado de Madurez.....	165
Análisis del Nivel de Madurez por Controles de Seguridad de la Información	167
Mejoras en la Implementación de Controles de Seguridad	171
Formular las Políticas de Seguridad de la Información, así como el Alcance del SGSI, la Identificación de los Procesos Críticos, los Servicios Involucrados y las Partes Interesadas...	173
Alcance del SGSI.....	174

Procesos	175
Servicios	176
Partes Interesadas	177
Política General de Seguridad y Privacidad de la Información	179
Políticas Específicas de Seguridad y Privacidad de la Información	181
Definir Roles, Responsabilidades y Mecanismos de Seguimiento del SGSI con base en Principios de Gobernanza de TI Establecidos en COBIT	188
Análisis de Principios de COBIT Aplicables al SGSI	189
Identificación y Estructuración de Roles Clave en el SGSI	193
Diseño de Mecanismos de Seguimiento del SGSI	197
Conclusiones	202
Recomendaciones	204
Referencias Bibliográficas	206
Apéndices	211

Lista de Tablas

Tabla 1 Líneas estratégicas, Objetivos Estratégicos	44
Tabla 2 <i>Valores del Cálculo del Coeficiente de Alfa de Cronbach</i>	62
Tabla 3 <i>Índice de Confiabilidad de Alfa de Cronbach</i>	62
Tabla 4 <i>Prueba de esfericidad de Bartlett y el índice KMO</i>	63
Tabla 5 <i>Comunalidades</i>	63
Tabla 6 <i>Correlaciones</i>	65
Tabla 7 <i>Clasificación de Acuerdo con la Confidencialidad</i>	74
Tabla 8 <i>Clasificación de Acuerdo con la Disponibilidad</i>	74
Tabla 9 <i>Clasificación de Acuerdo con la Integridad</i>	75
Tabla 10 <i>Inventario de Activos</i>	77
Tabla 11 <i>Identificación de Activos</i>	81
Tabla 12 <i>Clasificación General y Números de Activos</i>	86
Tabla 13 <i>Clasificación de Activos Según su Valor</i>	86
Tabla 14 <i>Ubicación de los Activos de Información</i>	87
Tabla 15 <i>Resumen de Nivel de Riesgos</i>	87
Tabla 16 <i>Clasificación Según Impacto a la Seguridad</i>	88
Tabla 17 <i>Valoración Cualitativa de los Activos</i>	89
Tabla 18 <i>Valoración Cuantitativa de los Activos</i>	91
Tabla 19 <i>Identificación de Amenazas y Vulnerabilidades</i>	95
Tabla 20 <i>Matriz de APT</i>	106
Tabla 21 <i>Apetito por el Riesgo y Zonas de Admisibilidad</i>	119
Tabla 22 <i>Plan de Tratamiento</i>	122

Tabla 23 <i>Evaluación de Controles ISO 27001 con COBIT</i>	145
Tabla 24 <i>Status Controles ISO 27001</i>	165
Tabla 25 <i>Componentes de COBIT Relevantes para el SGSI</i>	190
Tabla 26 <i>Roles Propuestos para la Personería Municipal de Armenia</i>	194
Tabla 27 <i>Indicador Tiempo Promedio de Respuestas a Incidentes</i>	198
Tabla 28 <i>Indicador Funcionarios Capacitados en Seguridad</i>	198
Tabla 29 <i>Indicador Número de Incidentes Crítico</i>	199
Tabla 30 <i>Porcentaje de Vulnerabilidades sin Mitigar</i>	199
Tabla 31 <i>Numero de Accesos no Autorizados Detectados</i>	200
Tabla 32 <i>Porcentaje de Acciones de Mejora Implementadas</i>	200

Lista de Figuras

Figura 1 <i>Estándares ISO 27000</i>	29
Figura 2 <i>Organigrama Personería de Armenia</i>	42
Figura 3 <i>Mapa de Procesos Personería Municipal de Armenia</i>	43
Figura 4 <i>Diagrama Análisis del Entorno</i>	58
Figura 5 <i>Diagrama Arquitectura Tecnológica</i>	60
Figura 6 <i>Mapa de Correlaciones Conocimiento de Seguridad y Cambio Contraseñas</i>	68
Figura 7 <i>Mapa de Correlaciones Frecuencia de Capacitaciones y Reporte Incidentes</i>	69
Figura 8 <i>Mapa de Correlación Cultura Organizacional y Revisión de Dispositivos</i>	70
Figura 9 <i>Mapa de Correlaciones Conocimiento en Seguridad y Años de Experiencia</i>	71
Figura 10 <i>Mapa de Correlaciones Cargo de Entidad y el Compromiso con la Entidad</i>	72
Figura 11 <i>Mapa de Correlación Cultura Seguridad y Efectividad del Soporte</i>	73
Figura 12 <i>Identificación de Activos</i>	88
Figura 13 <i>Nivel de Madurez Controles ISO 27001</i>	1655

Lista de Apéndices

Apéndice A <i>Carta de Aceptación Proyecto Aplicado</i>	211211
Apéndice B <i>Instrumento de Caracterización de Seguridad Informática</i>	22122

Introducción

La información es un activo estratégico clave para cualquier organización, y su adecuada protección frente a amenazas y vulnerabilidades es fundamental para garantizar su seguridad. La implementación de controles robustos que incluyan políticas, procesos, procedimientos y soluciones tecnológicas (software y hardware) es esencial para preservar la confidencialidad, integridad y disponibilidad de los datos. En el contexto de las entidades gubernamentales, como la Personería Municipal de Armenia, esta protección es aún más relevante, ya que garantiza la continuidad de los servicios públicos, mitiga riesgos y promueve la confianza ciudadana.

La Personería Municipal de Armenia gestiona información altamente sensible relacionada con la defensa de los derechos humanos, tutelas, denuncias, vigilancia administrativa y trámites ciudadanos. Sin embargo, actualmente no cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI) formalmente establecido, lo cual la deja expuesta a riesgos que podrían comprometer la operación institucional y afectar la integridad de sus servicios. Por ello, contar con un SGSI basado en la norma ISO/IEC 27001 permitirá establecer un marco estructurado para la identificación y gestión de riesgos, la implementación de controles de seguridad efectivos y la mejora continua de los procesos relacionados con el tratamiento de la información. Además, contribuirá al cumplimiento de la normatividad vigente en Colombia en materia de protección de datos personales (Ley 1581 de 2012), transparencia (Ley 1712 de 2014) y delitos informáticos (Ley 1273 de 2009), así como a los lineamientos institucionales exigidos por entes de control.

Desde una perspectiva institucional, el SGSI fortalecerá la capacidad de respuesta frente a incidentes, garantizará la continuidad de las operaciones críticas y permitirá una toma de decisiones informada y basada en riesgos reales. Asimismo, aportará al fortalecimiento de la confianza de la ciudadanía al demostrar un compromiso con la protección de la información y la

transparencia institucional. Finalmente, el SGSI será un componente fundamental para apoyar de manera segura y planificada los procesos de transformación digital que adelanta la Personería, en consonancia con las políticas públicas de modernización del Estado.

Este proyecto se enmarca en un contexto nacional en el que los incidentes de seguridad digital en el sector público han evidenciado la vulnerabilidad de las instituciones frente a amenazas cibernéticas. Casos recientes como el ataque de ransomware a SuperGIROS (2023) y el hackeo a la Alcaldía de Bogotá (2022) demuestran la necesidad urgente de establecer mecanismos formales para la gestión de la seguridad. Por tanto, este diseño de SGSI busca no solo fortalecer la protección de los activos informacionales de la Personería, sino también constituirse en un referente para futuras mejoras en la gobernanza de TI y la gestión de riesgos en entidades del sector público.

En el primer capítulo se presenta un análisis de los procesos y sistemas existentes en la Personería Municipal de Armenia, con el objetivo de identificar los riesgos y vulnerabilidades que afectan la seguridad de la información. En el segundo capítulo, se identifican, valoran y clasifican los riesgos asociados a los activos de información, priorizando los más críticos y estableciendo un plan de tratamiento acorde con las necesidades tecnológicas de la entidad. En el tercer capítulo, se realiza un análisis GAP para evaluar los controles de seguridad existentes y proponer mejoras para fortalecer su implementación. El cuarto capítulo está dedicado al desarrollo de las políticas generales y específicas de seguridad de la información, alineadas con la norma ISO/IEC 27001, definiendo el alcance del SGSI, los procesos críticos y las partes interesadas. Finalmente, en el quinto capítulo se establecen los roles y responsabilidades, así como los mecanismos de seguimiento, basados en los principios de gobernanza de TI del marco COBIT, garantizando una gestión transparente y alineada con los objetivos institucionales.

Definición del problema

Las entidades públicas, como la Personería Municipal de Armenia, están cada vez más expuestas a amenazas digitales que pueden comprometer la seguridad de los datos y sistemas, interrumpiendo su funcionamiento y poniendo en riesgo la confidencialidad, integridad y disponibilidad de la información. (Morales, 2019). En este contexto, la Personería gestiona información altamente sensible, incluyendo datos relacionados con la comunidad, procesos administrativos, derechos de petición, tutelas y procedimientos jurídicos. Esta información la hace vulnerable a amenazas como accesos no autorizados, fuga de datos, ciberataques (como ransomware), y fallas en los controles internos de seguridad.

En los últimos años, según (La Red de Investigación en Cibercrimen y Ciberseguridad, 2025), Colombia ha registrado un notable aumento en la cantidad y complejidad de ciberataques dirigidos a entidades públicas. Ministerios, fuerzas armadas y organismos del poder judicial han sido blanco de estas amenazas, lo que ha puesto en evidencia la necesidad urgente de fortalecer la seguridad de la información en el sector público. Entre 2021 y 2023, se identificaron 45 incidentes en 31 entidades gubernamentales, según análisis basados en OSINT (inteligencia de fuentes abiertas) y reportes periodísticos. Estos ataques incluyeron acceso no autorizado y robo de información (35,5 %), interrupción de servicios y ransomware (24,4 %), defacement de sitios web (15,5 %) y otros como DDoS y malware (24,6 %).

De acuerdo con (Portafolio, 2023), un ataque de tipo ransomware a IFX Networks, proveedor de servicios tecnológicos, afectó a 34 entidades públicas, incluyendo el Ministerio de Salud, la Superintendencia de Industria y Comercio, la Superintendencia Nacional de Salud y la Rama Judicial. Este incidente comprometió el acceso a múltiples plataformas digitales y sistemas misionales, interrumpiendo servicios esenciales para la ciudadanía.

Este panorama evidencia la exposición creciente de las entidades públicas a riesgos informáticos que comprometen la confidencialidad, integridad y disponibilidad de la información. Si bien no se han documentado ataques específicos contra la Personería Municipal de Armenia, su función misional implica el tratamiento de datos altamente sensibles relacionados con la gestión de derechos ciudadanos, procesos jurídicos y trámites administrativos. Esto la convierte en un blanco potencial para ciberataques similares.

A pesar de que se han implementado algunas medidas básicas de protección, no existe un diagnóstico integral que evalúe la efectividad de dichas medidas ni que determine el grado de cumplimiento con estándares internacionales en seguridad de la información, como la norma ISO/IEC 27001. Esto ha generado una falta de visibilidad sobre los riesgos actuales y un marco estructurado para su gestión. La ausencia de políticas claras y procedimientos definidos contribuye a un panorama de vulnerabilidad, lo que pone en riesgo los activos informacionales de la entidad.

Por lo anterior, la carencia de un enfoque para gestionar estos riesgos y la ausencia de controles alineados con estándares internacionales aumentan la vulnerabilidad institucional. Por ello, se considera prioritaria la formulación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001, que permita identificar amenazas, evaluar riesgos, y establecer políticas y procedimientos que garanticen una gestión segura y eficiente de los activos de información.

A partir del contexto previamente descrito, se propone el siguiente interrogante que direcciona el desarrollo del presente trabajo:

¿De qué manera el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la norma ISO/IEC 27001, puede contribuir a minimizar los riesgos que

enfrenta la Personería Municipal de Armenia en materia de seguridad digital y fortalecer la protección de su información institucional?

Justificación

En el contexto actual, donde los procesos institucionales están profundamente interrelacionados con la tecnología, la gestión adecuada de la seguridad de la información se ha convertido en un eje fundamental para garantizar la eficiencia, confiabilidad y legitimidad de las entidades públicas. La Personería Municipal de Armenia, como ente garante de los derechos ciudadanos y actor clave en el control y vigilancia de la gestión pública, administra información altamente sensible. Esta incluye datos personales de la ciudadanía, documentos legales, procesos administrativos y actuaciones jurídicas, cuya protección resulta vital para preservar la confianza institucional y el cumplimiento de su misión.

No obstante, el entorno tecnológico moderno expone a las entidades públicas a crecientes amenazas digitales como ransomware, accesos indebidos, fugas de información, entre otros riesgos que pueden afectar la disponibilidad, integridad y confidencialidad de los activos informacionales. A pesar de contar con algunas medidas de protección, la Personería no dispone actualmente de un diagnóstico integral ni de un marco estructurado que le permita gestionar los riesgos de manera sistemática, ni cumplir a cabalidad con estándares reconocidos de seguridad de la información.

Ante esta situación, el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 se plantea como una necesidad estratégica. Esta norma internacional proporciona una metodología robusta y probada que permitirá a la entidad identificar sus activos críticos, valorar riesgos, establecer políticas, controles y procedimientos, y promover una mejora continua en la gestión de la seguridad. A su vez, se integrarán los principios de gobernanza del marco COBIT, lo cual contribuirá a alinear las decisiones

tecnológicas con los objetivos estratégicos de la entidad, garantizando una gestión más transparente, efectiva y orientada a resultados.

Los beneficios tangibles de este proyecto incluyen el fortalecimiento de la infraestructura tecnológica, la prevención de incidentes de seguridad, la mejora en la continuidad del negocio, el cumplimiento de marcos normativos nacionales como la Ley 1581 de 2012 sobre protección de datos personales y los lineamientos del Ministerio TIC, así como el aumento de la resiliencia institucional frente a futuras amenazas. Estratégicamente, permitirá posicionar a la entidad como un referente de buenas prácticas en el manejo responsable y seguro de la información pública.

Desde una perspectiva académica y disciplinaria, el proyecto se justifica por la oportunidad de aplicar estándares internacionales y herramientas de análisis de riesgos en un entorno real, promoviendo el desarrollo de competencias técnicas avanzadas en seguridad de la información. Socialmente, se contribuye a salvaguardar los derechos fundamentales de la ciudadanía mediante la protección efectiva de sus datos. Y a nivel personal, representa un ejercicio formativo integral que fortalece habilidades críticas, analíticas y profesionales en el diseño de soluciones aplicadas al sector público.

Finalmente, el diseño de un SGSI para la Personería Municipal de Armenia no solo responde a una necesidad operativa, sino que representa una contribución relevante desde lo técnico, lo social y lo institucional, brindando a la entidad una herramienta estratégica para enfrentar los desafíos de la seguridad de la información.

Objetivos

Objetivo General

Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en las normas ISO/IEC 27001 para la Personería Municipal de Armenia, con el propósito de establecer las políticas, procedimientos y controles necesarios para proteger la confidencialidad, integridad y disponibilidad de la información.

Objetivos Específicos

Realizar un diagnóstico del estado actual de la seguridad de la información en la Personería Municipal de Armenia, mediante la identificación de los activos de información y el análisis de los procesos y sistemas existentes, con el fin de detectar riesgos y vulnerabilidades.

Aplicar una metodología de gestión de riesgos para identificar, valorar y clasificar los riesgos asociados a los activos de información, priorizando los más críticos y estableciendo un plan de tratamiento adecuado a la realidad tecnológica de la entidad.

Evaluar el nivel de madurez de los controles de seguridad de la información mediante un análisis GAP estructurado, con el propósito de identificar brechas y proponer mejoras en la implementación de controles de seguridad.

Formular las políticas de seguridad de la información, así como el alcance del SGSI, la identificación de los procesos críticos, los servicios involucrados y las partes interesadas, asegurando su alineación con los lineamientos de la norma ISO/IEC 27001.

Definir roles, responsabilidades y mecanismos de seguimiento del SGSI con base en principios de gobernanza de TI establecidos en COBIT, con el propósito de asegurar una gestión transparente y alineada con los objetivos institucionales.

Marco Referencial

El presente proyecto se fundamenta en una serie de marcos que brindan el sustento conceptual, normativo, contextual e histórico necesario para comprender y justificar el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Personería Municipal de Armenia.

Antecedentes

La seguridad de la información es esencial en las organizaciones, especialmente en las entidades gubernamentales que manejan datos sensibles. Diversas investigaciones destacan la importancia de un Sistema de Gestión de Seguridad de la Información (SGSI) para proteger los activos digitales y mitigar riesgos. En este contexto, la implementación de marcos como ISO/IEC 27001 y COBIT permite establecer un enfoque estructurado y alineado con las mejores prácticas internacionales para gestionar la seguridad de la información y la gobernanza de TI

En el caso de la Personería Municipal de Armenia, el diseño de un SGSI basado en estos estándares fortalecerá la protección de sus datos sensibles, asegurando su confidencialidad, integridad y disponibilidad, y alineando los procesos tecnológicos con los objetivos institucionales. La adopción de estas normativas no solo optimiza los controles de seguridad, sino que también promueve la mejora continua en la gestión de la información institucional.

En primer lugar, según (De León Camelo, 2019), planteó el desarrollo de un *Sistema de Gestión de Seguridad de la Información (SGSI) fundamentado en la norma ISO/IEC 27001*, específicamente dirigido a entidades del sector público. Como resultado, se elaboró una guía que recopila buenas prácticas y procedimientos estructurados, con el propósito de reducir riesgos y garantizar la protección de la información en organizaciones estatales.

El propósito central de esta propuesta fue asegurar la confidencialidad, integridad y disponibilidad de los datos, a través de una herramienta de gestión enfocada en la seguridad y la privacidad de la información. Con base en esta necesidad, se diseñó un SGSI tomando como modelo la metodología definida en la norma ISO/IEC 27001. Así mismo, la finalidad es brindar a las instituciones gubernamentales una guía práctica que facilite la definición de sus políticas de seguridad de la información, ofreciendo orientaciones esenciales para iniciar el diseño, delimitar el alcance e implementar un SGSI adecuado al contexto del sector público en Colombia.

Otro antecedente relevante de (Tonysé de la Rosa, 2021), en su artículo desarrollado Automatización de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001, resalta la importancia de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) y de automatizar el diagnóstico a través de una plantilla de control interno, enfocada en los tres pilares fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad. Esta metodología permite realizar un análisis de brechas ("Gap-Analysis") respecto a los requisitos del estándar ISO/IEC 27001:2013, utilizando representaciones gráficas como diagramas de radar para medir el nivel de madurez. El objetivo es facilitar la instauración de un SGSI o el proceso de certificación, minimizando riesgos y asegurando la protección de la información, considerada uno de los activos más importantes en cualquier organización. La pérdida, fuga o indisponibilidad de datos críticos puede comprometer seriamente la operación institucional, lo que justifica la adopción de prácticas estructuradas de gestión de seguridad.

Desde el punto de vista (Guacanes Castro & Vilatuña Morales, 2022), desarrolló una Propuesta de Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 para la empresa Ultralink, con el objetivo de apoyar la toma de

decisiones en materia de seguridad de la información. El modelo fue adaptado a la realidad y necesidades específicas de la organización, buscando prevenir o reducir los riesgos mediante procedimientos que facilitaran su tratamiento. Para fortalecer la gestión de los activos de información, se incorporaron nuevas tecnologías que mejoraron los procesos internos y la atención a los usuarios. En cuanto al tratamiento de riesgos, se realizó una comparativa entre diferentes metodologías, eligiéndose finalmente MAGERIT por su factibilidad y beneficios para la empresa. Como resultado del proyecto, se identificaron los activos críticos, las amenazas y vulnerabilidades asociadas, se definieron políticas alineadas con los dominios, controles y objetivos del Anexo A de la norma ISO/IEC 27001, y se elaboró un plan de tratamiento de riesgos que proporciona acciones recomendadas para minimizar los riesgos identificados.

Una experiencia relevante en el diseño e implementación de un SGSI conforme a la norma ISO/IEC 27001:2013 se encuentra en el modelo adoptado por el Registro de la Propiedad del Cantón Pedro Moncayo (PRPMC), en la provincia de Pichincha, Ecuador. Como menciona el autor (Tintin & Hidalgo , 2023), este modelo se ha consolidado como un referente nacional en buenas prácticas. La investigación que documenta esta experiencia utilizó una metodología cuantitativa para analizar el diseño del SGSI, integrando tanto los lineamientos de la norma ISO/IEC 27001:2013 como regulaciones nacionales. Entre sus logros destaca la preparación ante incidentes mediante planes de contingencia, así como la mejora continua basada en informes de hacking ético. Esta implementación demuestra que incluso instituciones del sector público pueden alcanzar altos niveles de seguridad, garantizando la fiabilidad y la continuidad operativa de los servicios vinculados a la gestión documental y registral.

Como menciona (Monev, 2024), un enfoque emergente en la gestión de la seguridad de la información es el "SGSI centrado en TI", el cual se aparta del modelo tradicional al dar mayor

protagonismo a la seguridad informática. A diferencia de los programas holísticos que requieren amplios recursos, este modelo es diseñado y gestionado directamente por la unidad de TI, lo que lo convierte en una opción viable para organizaciones con recursos limitados. Para su implementación, es fundamental que los especialistas en seguridad evalúen la idoneidad de los controles disponibles en los distintos marcos normativos, seleccionando aquellos que mejor se ajusten a los objetivos y capacidades de la organización. En este contexto, se propone un método para comparar controles de seguridad entre marcos, facilitando así su selección y adaptación.

De acuerdo con los autores, (Niemeläinen y otros, 2025), invertir en un Sistema de Gestión de Seguridad de la Información (SGSI) fortalece la competitividad organizacional y protege los activos de información, aunque su implementación puede implicar un consumo significativo de recursos. Un estudio de caso sobre la empresa finlandesa Kempower demuestra cómo el uso de inteligencia artificial generativa permitió optimizar la creación e implementación de un SGSI basado en ISO/IEC 27001, reduciendo considerablemente la carga operativa y documental, que incluye hasta 116 controles. Lo anterior, basada en entrevistas semiestructuradas a los involucrados en el proyecto, evidencia el potencial de la IA para agilizar procesos en ciberseguridad. Este antecedente resulta pertinente, ya que muestra cómo es posible optimizar la gestión de recursos en el diseño de un SGSI, lo cual es una consideración clave para la presente propuesta.

En el contexto actual de acelerado avance tecnológico, el autor (Moses & Sandkuhl, 2025), menciona la evaluación e implementación de Sistemas de Gestión de Seguridad de la Información (SGSI) se ha vuelto una prioridad para muchas entidades del sector público. A pesar de su importancia, la mayoría de estas organizaciones aún no cuentan con un SGSI formalmente establecido, debido a limitaciones como la escasez de personal, tiempo y recursos financieros. Un

estudio reciente propone un modelo de procedimiento diseñado específicamente para facilitar la adopción del SGSI en pequeñas entidades públicas, abordando las principales barreras identificadas. Este modelo fue evaluado mediante una estrategia basada en métodos reconocidos en la literatura, mostrando resultados promisorios. Este antecedente resulta relevante para el presente proyecto, ya que evidencia los retos y soluciones específicas para entidades públicas similares a la Personería Municipal de Armenia.

Los antecedentes revisados evidencian la creciente necesidad de diseñar Sistemas de Gestión de Seguridad de la Información (SGSI) en las organizaciones, especialmente en el sector público, donde los desafíos en cuanto a recursos humanos, técnicos y financieros son notorios. Diversos estudios y experiencias internacionales demuestran que es posible desarrollar modelos efectivos de SGSI alineados con la norma ISO/IEC 27001, adaptándolos al contexto y capacidades institucionales. Además, enfoques innovadores centrados en TI revelan nuevas formas de optimizar el diseño y la gestión de la seguridad de la información. En conjunto, estos antecedentes proporcionan una base sólida para proponer el diseño de un SGSI adaptado a las necesidades de la Personería Municipal de Armenia, orientado a salvaguardar los activos de información y asegurar la continuidad de los procesos institucionales.

Marco Conceptual

Control Objectives for Information and Related Technologies COBIT

Marco que facilita la gobernanza y administración integral de las Tecnologías de la Información en toda la organización, cubriendo de manera completa el negocio desde su inicio hasta su finalización, así como las áreas funcionales responsables de las TI. Se tienen en cuenta los intereses de las partes involucradas tanto dentro como fuera de la organización en relación con las TI. (ISACA, 2019). Esta estructura de trabajo resulta beneficiosa para compañías de

cualquier magnitud. El marco de trabajo de COBIT se compone de cinco principios y siete facilitadores. Los cinco principios se unen para ayudar a la organización a establecer un sólido sistema de gobierno y administración, fundamentado en siete habilitadores holísticos que mejoran la inversión en tecnología y su aplicación para beneficiar a todas las partes involucradas como satisfacer las necesidades de las partes interesadas, cubrir la empresa extrema a extremo, aplicar un marco de referencia único integrado, hacer posible holístico y separa el gobierno de la gestión.

Confidencialidad

Asegura que la información esté protegida contra accesos no autorizados, garantizando su privacidad y uso adecuado. Si la confidencialidad se ve comprometida, los datos pueden ser expuestos o utilizados indebidamente, lo que pone en riesgo la seguridad de la organización y puede afectar su operatividad y reputación.

Control de Seguridad

Las normas, directrices, metodologías y estructuras organizativas diseñadas para mantener los riesgos de seguridad de la información dentro de los niveles aceptables. El término "control" también se emplea como sinónimo de medida de protección o estrategia de mitigación, ya que ayuda a disminuir la probabilidad o el impacto de un incidente. (Funcion Publica, 2020).

Disponibilidad

La disponibilidad de la información garantiza que los datos y servicios estén accesibles en todo momento cuando sean requeridos, evitando interrupciones que puedan afectar la operatividad. Una gestión eficiente de la disponibilidad contribuye a la continuidad del negocio, optimizando la productividad y la toma de decisiones dentro de la organización. (ISO, 2018).

Infraestructura Tecnológica

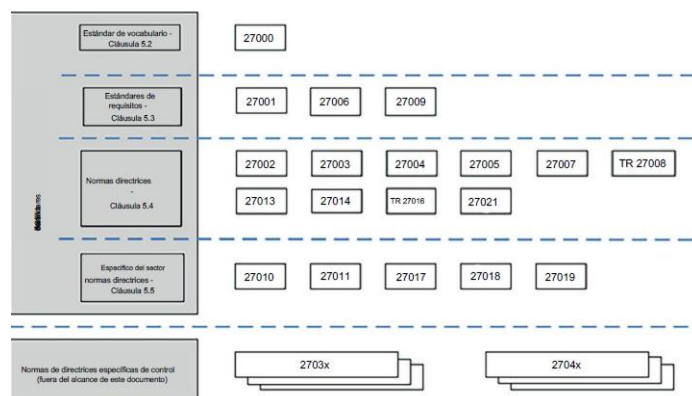
Son los elementos de hardware, software y comunicaciones que facilitan el funcionamiento de los diversos servicios de la organización. Estos incluyen computadoras de escritorio, equipos móviles, impresoras, escáneres, cámaras de vigilancia, redes inalámbricas, sistemas operativos, software de oficina y acceso a internet, entre otros. (Funcion Publica, 2020).

Integridad

Garantiza que la información se mantenga completa y precisa, evitando alteraciones, corrupción o pérdida. Cuando la integridad se ve comprometida, los datos pueden ser manipulados o incompletos, lo que afecta directamente el desempeño y la eficiencia de las funciones dentro de una organización. (Ministerio de Hacienda y Administraciones Públicas, 2014).

ISO/IEC 27000

Los estándares de la familia ISMS (Sistema de Gestión de Seguridad de la Información) proporcionan un conjunto de directrices y mejores prácticas para establecer, implementar, mantener y mejorar la seguridad de la información en una organización. Uno de los estándares más conocidos dentro de esta familia es ISO/IEC 27001:2013, que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI). Este estándar proporciona un marco para que las organizaciones identifiquen, evalúen y gestionen los riesgos de seguridad de la información, y establezcan controles para mitigar esos riesgos.

Figura 1*Estándares ISO 27000*

Nota. Estándares ISO 27000. Tomado de (ISO, 2018). <https://www.iso.org/standard/iso-iec-27000-family>

ISO/IEC 27001

Publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013 (segunda edición) y actualizada el 25 de octubre de 2022 (versión 3). Establece los requisitos para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI). Asimismo, ayuda a las organizaciones a gestionar de manera sistemática la seguridad de la información, identificando y mitigando los riesgos relacionados con los activos de información garantizando la confidencialidad, integridad y disponibilidad de la información crítica. Facilita un marco sólido y flexible que se puede adaptar a las necesidades específicas de cada organización. Así mismo, proporciona requisitos normativos para el desarrollo y operación de un SGSI, contribuye a mitigar los riesgos de seguridad de la información, estos controles se derivan de un análisis de riesgos realizado por la organización y se implementan para abordar los riesgos identificados de manera efectiva. Por otro lado,

establecer objetivos medibles para los procesos de Gestión de Seguridad de la Información y para los controles de seguridad.

ISO/IEC 27002

La ISO/IEC 27002 es una norma internacional que ofrece buenas prácticas para mejorar la seguridad de la información en las organizaciones. A diferencia de la ISO/IEC 27001, que establece los requisitos del sistema de gestión, esta norma guía sobre temas como el control de acceso, la criptografía y la respuesta a incidentes. Es muy importante porque ayuda a proteger los datos sensibles, prevenir riesgos y generar confianza entre clientes y socios. Adoptarla permite a las empresas enfrentar los desafíos de la ciberseguridad de forma proactiva. (ISO, 2022).

ISO/IEC 27005

La norma ISO/IEC 27005 es un estándar internacional que proporciona directrices específicas para la gestión de riesgos de seguridad de la información, en apoyo a la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001. Esta norma ofrece un enfoque estructurado y sistemático para identificar, evaluar y tratar los riesgos relacionados con la seguridad de la información en cualquier tipo de organización. Su propósito es facilitar la integración de la gestión de riesgos como parte esencial del SGSI, promoviendo una actitud proactiva frente a las amenazas. (ISO, 2022).

Magerit

Aplica este proceso dentro de un marco estructurado que permite a los órganos de gobierno tomar decisiones considerando los riesgos asociados al uso de tecnologías de la información, se enmarca en lo que se conoce como el “Proceso de Administración de Riesgos”. El objetivo es sensibilizar a los responsables sobre la existencia de riesgos y la importancia de su gestión, proporcionando un método estructurado para analizarlos en el uso de las TIC. Además,

busca facilitar la planificación de medidas para mantener los riesgos bajo control y preparar a la organización para evaluaciones, certificaciones o acreditaciones. (Ministerio de Hacienda y Administraciones Públicas, 2014).

NIST

El Marco de Ciberseguridad del NIST constituye una herramienta estratégica que orienta a las organizaciones en el fortalecimiento de sus capacidades frente a los riesgos cibernéticos. A través de un conjunto coherente de lineamientos, normas técnicas y prácticas recomendadas, este marco facilita la adopción de una cultura de seguridad adaptable a diferentes contextos organizacionales; puede integrarse en sistemas de gestión existentes, promoviendo una efectiva protección de activos de información. (IBM, 2020).

Política de la Seguridad de la Información

Garantizar la seguridad de la información, promoviendo una cultura de protección entre empleados y colaboradores, establecer normativas y procedimientos claros, minimizar riesgos en los procesos, mejorar continuamente la gestión de seguridad y aplicar controles tecnológicos que resguarden los activos y reduzcan las amenazas. (MinTIC, 2021).

Sistema de Gestión de Seguridad de la Información

El Sistema de Gestión de Seguridad de la Información (SGSI, por sus siglas en inglés: Information Security Management System) es un conjunto estructurado de principios, políticas, procedimientos y controles que se implementan para identificar, evaluar y gestionar los riesgos asociados a la seguridad de la información. Su objetivo principal es garantizar que las organizaciones adopten medidas sistemáticas y continuas para proteger sus activos de información. Un SGSI abarca todos los tipos de información, incluyendo datos sensibles de clientes, procesos internos, detalles de pago, entre otros. A través de su implementación, las

organizaciones buscan establecer un enfoque integral para mitigar los riesgos que podrían comprometer la confidencialidad, integridad y disponibilidad de los datos. (Soluciones de Software OTRS, 2025).

Marco Teórico

Gestión de la Información y su Importancia en las Organizaciones

Las organizaciones, independientemente de su tipo de actividad o tamaño, están involucradas en un proceso continuo de recopilación, procesamiento, almacenamiento y transmisión de información. Este proceso involucra la interacción de sistemas, redes y recursos humanos, tanto internos como externos, que permiten gestionar los activos de información clave para alcanzar los objetivos organizacionales. Según la (ISO, 2018), la información se ha convertido en uno de los activos más valiosos de cualquier entidad, y su protección es esencial para garantizar la operatividad y la confianza dentro de la organización.

En este sentido, reconocer la información como un activo crítico implica adoptar un enfoque de protección integral que considere su valor, sensibilidad y función dentro de los procesos institucionales. La clasificación y control de los activos de información permite priorizar su protección de acuerdo con su importancia estratégica, facilitando la toma de decisiones informadas en materia de seguridad y continuidad del negocio. (Whitman & Mattord, 2021).

Riesgos y Vulnerabilidades en la Gestión de la Información

Las organizaciones están expuestas a diversos riesgos que pueden afectar negativamente la integridad, confidencialidad y disponibilidad de estos activos. Estos riesgos varían según el contexto organizacional (tipo de industria, entorno de operación, etc.) y las circunstancias particulares del momento. La capacidad para identificar, evaluar y mitigar estos riesgos es crucial

para la supervivencia de las organizaciones, ya que el impacto de la pérdida o vulneración de los activos de información puede afectar no solo la seguridad de los datos, sino también el logro de los objetivos estratégicos.

Además, la presencia de amenazas y brechas de datos obliga a las organizaciones a adoptar metodologías de gestión de riesgos que incluyan tanto medidas preventivas como planes de contingencia.

La Gestión de Riesgos como Estrategia de Protección de la Información

Una gestión proactiva de los riesgos es esencial para garantizar la protección de los activos de información. Según (Kitsios y otros, 2023), el proceso de gestión de riesgos en una organización implica identificar, evaluar y mitigar las amenazas que afectan los sistemas de información. Para ello, la alta dirección debe implementar estrategias adecuadas para evitar, transferir o reducir el nivel de exposición al riesgo, con base en un análisis de coste-eficacia y los recursos disponibles. Estas estrategias deben partir de unos estándares mínimos de protección, establecidos por normativas internacionales, en particular en relación con la seguridad de la información.

En el contexto digital actual, la gestión de riesgos vinculada a la gestión de incidentes constituye una estrategia esencial para proteger la integridad y confidencialidad de la información. Evaluar la postura de seguridad, implementar tecnologías adecuadas y anticipar amenazas permite establecer sistemas de gestión eficaces. No obstante, su implementación enfrenta desafíos como la resistencia al cambio, la escasez de recursos y la complejidad normativa. Integrar la gestión de riesgos con la respuesta a incidentes fortalece la capacidad organizacional de adaptación frente a un entorno dinámico y en constante evolución. (Blerton, 2025).

El Sistema de Gestión de Seguridad de la Información (SGSI) y la ISO/IEC 27001

En este contexto, la norma ISO/IEC 27001 se presenta como un marco esencial para la creación de un Sistema de Gestión de Seguridad de la Información (SGSI). Esta norma proporciona directrices para identificar, evaluar y gestionar los riesgos relacionados con la seguridad de la información, garantizando la protección de los activos de información de la organización. Un SGSI basado en ISO 27001 permite a las organizaciones identificar los riesgos informáticos y establecer medidas necesarias para proteger sus datos y activos digitales, alineando la seguridad con los objetivos organizacionales (Aleman & Rodríguez, 2019).

El diseño de un SGSI bajo este estándar implica establecer un ciclo de mejora continua (PDCA: Planificar, Hacer, Verificar, Actuar), así como documentar políticas, procedimientos y controles orientados a la protección de la información. Esto permite construir una cultura organizacional basada en la seguridad, donde todos los actores conocen sus responsabilidades y se alinean con los objetivos estratégicos y normativos de la entidad. (ISO, 2018).

Metodología Magerit y su Aplicación en la Gestión de Riesgos

Una herramienta clave para la implementación de un SGSI es la metodología Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), proporciona un enfoque estructurado para identificar los activos de información, evaluar las amenazas y vulnerabilidades, y analizar los riesgos asociados.

El proceso comienza con el análisis de riesgo, donde se identifican y evalúan los activos esenciales para la organización (información, servicios, software, hardware, redes, personal). Se asigna un valor a estos activos en función de su importancia y el impacto de su posible pérdida. Posteriormente, en la evaluación de riesgo, una vez identificados y evaluados los riesgos, se establece un enfoque adecuado para su protección. Las organizaciones pueden optar por

estrategias como minimizar el impacto, modificar procesos para evitar la exposición, transferir el riesgo o asumirlo si su impacto es mínimo. Finalmente, en la selección de controles, la entidad implementa medidas de seguridad alineadas con los requisitos del Anexo A de ISO/IEC 27001.

Gobernanza de Tecnologías de la Información (TI) y su Relación con el SGSI

Para asegurar que el Sistema de Gestión de Seguridad de la Información (SGSI) esté alineado con los objetivos institucionales y cuente con una estructura clara de responsabilidades, resulta esencial incorporar principios de gobernanza de Tecnologías de la Información (TI). En este contexto, COBIT se presenta como un marco de referencia adecuado para definir los roles, responsabilidades y mecanismos de seguimiento del SGSI.

El marco de COBIT permite establecer una estructura organizacional clara, promoviendo la transparencia en la gestión del sistema y facilitando la toma de decisiones alineadas con los objetivos estratégicos de la entidad. Su enfoque en la asignación de responsabilidades y en el monitoreo del desempeño permite que el SGSI no solo se estructure correctamente, sino que también pueda ser gestionado de forma eficiente y con mecanismos claros de supervisión. Así, el uso de COBIT en este proyecto se circunscribe a proporcionar directrices prácticas para asegurar una gobernanza efectiva, sin que se utilice como marco principal para la gestión de la seguridad de la información.

Criterios para la Selección del Marco Normativo de Seguridad

Existen diversos marcos y estándares reconocidos internacionalmente para la gestión de la seguridad de la información, entre los cuales se destacan ISO/IEC 27001, el Marco de Ciberseguridad del NIST (National Institute of Standards and Technology) y COBIT (Control Objectives for Information and Related Technology). La elección del marco más adecuado

depende del tipo de organización, sus necesidades específicas, el entorno regulatorio y los objetivos institucionales.

ISO/IEC 27001 es una norma internacional que proporciona un modelo integral para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Su enfoque está centrado en la gestión de riesgos, la mejora continua y el cumplimiento de requisitos legales y contractuales. Una de sus principales fortalezas es su aplicabilidad a todo tipo de organizaciones, independientemente de su tamaño o sector, lo cual la hace especialmente adecuada para entidades públicas como la Personería Municipal de Armenia.

Por otro lado, el marco NIST, aunque ampliamente utilizado en entornos gubernamentales y tecnológicos, especialmente en los Estados Unidos, tiene un enfoque más técnico-operativo y menos orientado a la gestión organizacional integral. NIST proporciona guías detalladas de seguridad, pero no establece un sistema de gestión como tal, lo que puede dificultar su adopción en contextos donde se requiere una estructura organizacional y documental clara, como en el caso del diseño de un SGSI.

A diferencia de otras normas complementarias, como la ISO/IEC 27005, que se enfoca exclusivamente en la gestión de riesgos, la ISO/IEC 27001 proporciona un marco más amplio que abarca políticas, procedimientos, responsabilidades, recursos y mejora continua del sistema, lo que permite una alineación efectiva con los objetivos estratégicos institucionales. Además, al ser una norma certificable, ofrece un respaldo formal que facilita su adopción en contextos regulatorios y contractuales exigentes. Por lo tanto, aunque ISO/IEC 27005 resulta útil para guiar el análisis y tratamiento de riesgos, no sustituye la estructura organizativa y de gestión que proporciona ISO/IEC 27001, la cual se considera esencial para el diseño efectivo de un SGSI. (ISO, 2022).

En cuanto a COBIT, su fortaleza radica en la gobernanza y gestión de TI, proporcionando un marco para asegurar que la tecnología se utilice de manera alineada con los objetivos estratégicos de la organización. No obstante, COBIT no está diseñado específicamente para la gestión de la seguridad de la información, sino más bien para establecer controles generales de TI y mecanismos de gobernanza. Por ello, en este proyecto se lo incorpora como complemento a ISO/IEC 27001, específicamente para definir roles, responsabilidades y mecanismos de seguimiento del SGSI.

Así, la elección de ISO/IEC 27001 como norma base para el diseño del SGSI en la Personería Municipal de Armenia se justifica por su enfoque estructurado, su reconocimiento internacional, su compatibilidad con procesos de mejora continua y su capacidad para integrarse con otras normativas y marcos, como MAGERIT para la gestión de riesgos y COBIT para la gobernanza de TI. Esta combinación permite construir un sistema robusto, adaptable y alineado con los requerimientos institucionales y normativos de la entidad.

Marco Legal

Decreto 1008 de 2018: "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones". (MinTIC, 2018). Las organizaciones tienen un rol crucial al implementar recursos tecnológicos para alcanzar los objetivos de esta ley, gestionando los riesgos y amenazas que puedan surgir con la adopción de nuevas tecnologías para promover la competitividad, proactividad e innovación tanto en la ciudadanía como en el Estado.

Directiva presidencial No. 03 del 15 de marzo de 2021: Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos (Función Pública,

2021). Con el objetivo de cumplir con lo establecido en el artículo 147 de la Ley 1955 de 2019, la cual se refiere al Plan Nacional de Desarrollo 2018-2022 "Pacto por Colombia, Pacto por la Equidad", se buscan reducir los gastos operativos, fomentar la innovación, garantizar entornos digitales seguros para las entidades públicas.

Ley 338 de 2022: Mediante el presente decreto se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, reglamentario del sector de Tecnologías de la Información y las Comunicaciones, con el propósito de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, crear el Modelo e instancias de Gobernanza de Seguridad Digital y dictar otras disposiciones relacionadas.

Ley 527 de 1999: “Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos” El mensaje de datos es “La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos, Internet, el correo electrónico, el telegrama, el télex o el telefax”.

Ley 1226 de 2008: “Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países”. Se establecen normas para el control de la información que incluya "cualquier dato personal almacenado en una base de datos, ya sea operada por entidades públicas o privadas".

Ley 1273 de 2009: “Por medio de la cual se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones”. De los atentados

contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. (Función Pública, 2021).

Ley 1437 de 2011: por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. (Uso de medios electrónicos Procedimiento Administrativo Electrónico), Artículo 1 de la ley 1755 de 2015.

Ley 1581 de 2012: Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales. (Función Pública, 2021). Hace referencia, en particular, al artículo 15 de la Constitución Nacional, según el cual “todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De la misma manera, las personas tienen el derecho de acceder, modificar y corregir la información que haya sido recopilada sobre ellos en bases de datos y registros de instituciones tanto públicas como privadas.

Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública (Función Pública, 2022). Se refiere principalmente al artículo 74 de la Constitución Nacional que garantiza el acceso de todas las personas a los documentos públicos, excepto en los casos determinados por la ley. La ley tiene como objetivo regular cómo se accede a la información pública, y las situaciones en las que se puede restringir la divulgación de información.

Ley de derechos de autor: El Derecho de Autor protege todas las creaciones artísticas, literarias y científicas. Entre ellas se incluyen obras escritas, como libros y folletos; discursos y conferencias; composiciones musicales; representaciones teatrales y coreografías. También abarca producciones audiovisuales, expresiones de bellas artes como dibujos, pinturas, esculturas y fotografías, así como diseños arquitectónicos y software. Esta protección se extiende a diversas

formas de expresión creativa, garantizando los derechos de sus autores. (Robles Chaparro y otros, 2023).

Marco Contextual

Según lo establecido en el artículo 118 de la Constitución Política de Colombia y en la Ley 136 de 1994, las Personerías Municipales son organismos públicos de nivel municipal, con independencia administrativa y financiera, encargados de ejercer funciones de control y vigilancia como parte del Ministerio Público dentro de su jurisdicción.

La Personería Municipal de Armenia tiene la responsabilidad de velar por la promoción, protección y garantía de los derechos humanos, asegurando que se respeten dentro del ámbito municipal. Además, actúa como defensora del orden jurídico, salvaguardando el cumplimiento de las normativas y regulaciones vigentes para la correcta administración pública. Su labor también se enfoca en la protección del interés general y la preservación del patrimonio público, previniendo cualquier acción que pueda vulnerar los recursos y bienes de la comunidad.

Según (Personería Municipal de Armenia, 2023), en ejercicio de estas funciones, la Personería Municipal de Armenia presta los siguientes servicios a la comunidad:

Promoción y protección de los Derechos Humanos: Son los derechos y atribuciones inherentes a todas las personas por su condición humana, sin importar su nacionalidad, etnia, género, religión, idioma, pensamiento político o cualquier otra característica que pueda generar diferenciación.

Vigilancia de la gestión pública: Responsabilidad de recibir y gestionar quejas contra servidores públicos o particulares que desempeñan funciones estatales. Además, supervisar la correcta ejecución de las funciones administrativas en las entidades municipales, garantizando su eficiencia y transparencia. Así mismo, vela por la protección del patrimonio público, ejerciendo

control y tomando las medidas judiciales y administrativas necesarias para su resguardo.

Adicionalmente, monitorea el recaudo y uso de los recursos públicos, asegurando su adecuada inversión, y realiza seguimiento y control a los procesos electorales para garantizar su transparencia y legalidad.

Atención a las víctimas del conflicto armado: Brinda acompañamiento a la Alcaldía en la elaboración del censo de personas afectadas en sus derechos debido al conflicto armado. Además, gestionar la inscripción de organizaciones de víctimas y defensoras de derechos humanos para su participación en las mesas de víctimas. Supervisar el cumplimiento de las medidas de ayuda humanitaria inmediata por parte del municipio y facilita el trámite de inscripción en el Registro Único de Víctimas. Asimismo, ofrecer asesoría y apoyo jurídico a las víctimas, garantizando la protección de sus derechos.

Centros de Conciliaciones: Ofrecer un Centro de Conciliación donde las personas de bajos recursos pueden resolver sus conflictos de manera rápida, gratuita y definitiva con la ayuda de un conciliador. Este centro atiende casos en distintas áreas, como: familiar, abordando temas como fijación, aumento, reducción o exoneración de cuotas alimentarias; civil y comercial, resolviendo disputas sobre la dirección del hogar, patria potestad y responsabilidad contractual o extracontractual; y penal, en delitos que requieren denuncia, como lesiones personales, entre otros. (Personería Municipal de Armenia, 2023).

Misión: La Personería Municipal de Armenia es un órgano de control que ejerce funciones de Ministerio Público para la defensa y promoción de los derechos humanos, el orden jurídico, el interés general y el patrimonio público. Así mismo, vigila el ejercicio eficiente de las funciones administrativas y la conducta oficial de quienes desempeñan funciones públicas en el municipio de Armenia. (Personería Municipal de Armenia en Quindío, 2024).

Visión: Para el año 2028 la Personería Municipal de Armenia será reconocida a nivel local, regional y nacional por contribuir a la solución integral de problemáticas jurídicas, sociales, económicas, ambientales y culturales del municipio de Armenia; por promover la participación de los armenios en la defensa de sus derechos y en el ejercicio del control social y será referente en la vigilancia efectiva de la gestión administrativa y el patrimonio público, a través de un equipo de trabajo calificado, comprometido con la inclusión social, el mejoramiento continuo, la innovación y el uso de las tecnologías de la información y comunicación.

Figura 2

Organigrama Personería de Armenia



Nota. Organigrama Personería de Armenia (Personería Municipal de Armenia en Quindío, 2024).

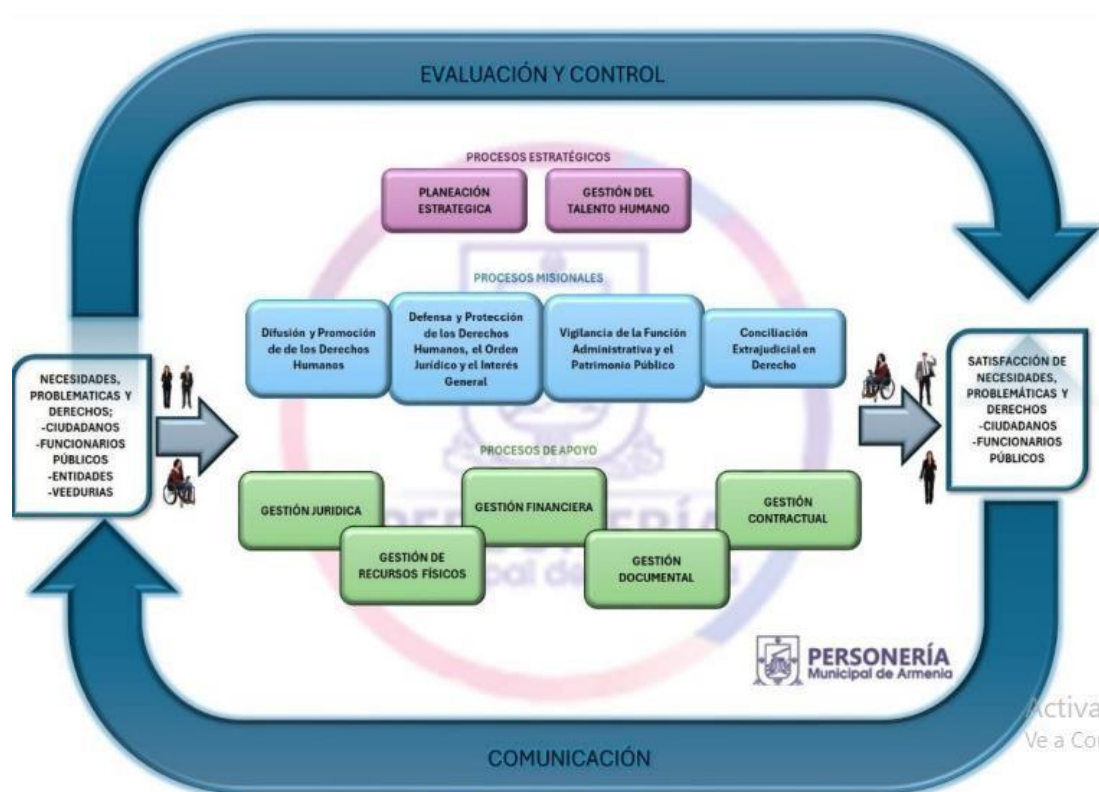
Tomada de <https://www.personeria-armenia.gov.co/>

Mapa de Procesos de la Personería Municipal de Armenia: El mapa de procesos de la Personería Municipal de Armenia representa la manera en que la entidad organiza y desarrolla sus funciones para garantizar la defensa de los derechos ciudadanos y el cumplimiento de sus responsabilidades.

Los procesos estratégicos son lo que proporcionan directrices y estrategias para la correcta gestión de la entidad; los procesos centrales que cumplen directamente con la misión de la Personería y finalmente los procesos de apoyo son aquellos que permiten el adecuado funcionamiento de los procesos misionales. Se estructura en tres grandes categorías de procesos:

Figura 3

Mapa de Procesos Personería Municipal de Armenia



Nota. Mapa de Procesos Personería Municipal de Armenia (Personería Municipal de Armenia en Quindío, 2024). Tomado de <https://www.personeria-armenia.gov.co/>

Líneas estratégicas, objetivos estratégicos, estrategias y responsables.

Tabla 1.*Líneas Estratégicas, Objetivos Estratégicos*

Líneas Estratégicas	Objetivos Estratégicos	Estrategias	Dependencias Responsables
Difusión y promoción de los Derechos Humanos.	Promover la participación de los armenios en la defensa de sus derechos y en el ejercicio del control social.	1. Implementar programas de capacitación sobre derechos humanos, obligaciones, y mecanismos legales y constitucionales para su protección, así como fomentar la participación ciudadana. 2. Apoyar la creación y operatividad de espacios de participación ciudadana. 3. Desarrollar una estrategia para el análisis de datos y la toma de decisiones.	Despacho, Personería delegada para los Derechos Humanos y Centro de conciliación.
Defensa y protección de los Derechos Humanos, el orden jurídico y el interés general.	Apoyar la solución de problemáticas en Armenia y garantizar los derechos humanos, el orden jurídico y el interés general.	1. Ofrecer asesoría y apoyo jurídico. 2. Implementar estrategias jurídicas de alto impacto. 3. Actuar como Ministerio Público para proteger los derechos humanos, el orden jurídico y el interés general. 4. Fomentar el empleo de métodos alternativos para la resolución de conflictos.	Despacho, Personería delegada para los Derechos Humanos y Centro de Conciliación

Tabla 1 (Continuación)*Líneas Estratégicas, Objetivos Estratégicos*

Líneas Estratégicas	Objetivos Estratégicos	Estrategias	Dependencias Responsables
Vigilancia efectiva de la gestión administrativa y defensa del patrimonio público.	Fortalecer la vigilancia de la conducta oficial de los servidores públicos y del manejo del patrimonio público.	1. Ejecutar acciones preventivas. 2. Realizar investigaciones de oficio y ejercer el poder preferente. 3. Implementar estrategias de litigio de gran impacto.	Despacho, Personería delegada para la Vigilancia Administrativa y Personería delegada para los Derechos Humanos.
	Fortalecer la capacidad institucional para mejorar continuamente la prestación de servicios.	1. Diseñar y ejecutar planes, programas y políticas conforme a la normativa vigente. 2. Modernizar la estructura y los procesos de la Personería Municipal.	Despacho, Dirección Administrativa y Financiera, Oficina asesora de control interno, Personería delegada para la Vigilancia Administrativa y Centro de Conciliación.
Modernización y posicionamiento de la Personería Municipal de Armenia.	Acercar los servicios de la Personería de Armenia a toda la población.	1. Fortalecer la imagen institucional mediante la difusión continua de servicios y logros.	

Nota. Líneas Estratégicas, Objetivos Estratégicos (Personería Municipal de Armenia en Quindío, 2024). Tomada de <https://www.personeria-armenia.gov.co/>

Marco Histórico

La transformación digital del sector público colombiano ha sido un proceso progresivo impulsado por políticas nacionales que buscan modernizar la gestión institucional mediante el uso estratégico de las Tecnologías de la Información y las Comunicaciones (TIC). El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ha liderado diversas iniciativas orientadas a fortalecer la seguridad digital, la protección de los datos y la confianza en el entorno digital, siendo uno de los pilares fundamentales del modelo de Gobierno Digital. (MinTIC, 2021).

A través de lineamientos como la Política de Seguridad Digital, se ha promovido la implementación de prácticas responsables para la gestión de riesgos relacionados con la información, especialmente en las entidades públicas que administran datos sensibles de los ciudadanos. Estas directrices reconocen que, ante el incremento de ciberamenazas y el uso masivo de sistemas de información, resulta imprescindible que las organizaciones públicas adopten marcos de seguridad basados en estándares internacionales, como la norma ISO/IEC 27001, que permita establecer políticas y controles adecuados para proteger sus activos digitales y garantizar la continuidad operativa.

En este contexto, entidades como la Personería Municipal de Armenia requieren diseñar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que les permita fortalecer sus capacidades institucionales, proteger la información que gestionan y responder de forma proactiva ante posibles incidentes de seguridad, todo ello en concordancia con las recomendaciones emitidas por el MinTIC.

Marco Científico

El marco científico y tecnológico del presente proyecto se basa en los avances y desarrollos clave en el campo de la gestión de la seguridad de la información (SGSI) y la gestión de riesgos tecnológicos, los cuales proporcionan una base sólida para el diseño e implementación de un sistema de seguridad de la información efectivo y alineado con estándares internacionales.

Uno de los pilares fundamentales es la norma ISO/IEC 27001, que establece los requisitos para implementar, mantener y mejorar un SGSI dentro de cualquier organización, proporcionando directrices sobre la identificación, evaluación y gestión de riesgos. A esta se le complementa la ISO/IEC 27005, que ofrece una guía específica para la gestión de riesgos de seguridad de la información, detallando metodologías para identificar y mitigar riesgos tecnológicos que puedan comprometer la seguridad de los activos de información (ISO, 2018)

Además, se considera la metodología MAGERIT, que proporciona un enfoque estructurado para el análisis y gestión de riesgos de los sistemas de información. Esta metodología integra la identificación de activos, la evaluación de amenazas y vulnerabilidades, y la asignación de medidas de protección basadas en una valoración precisa de los riesgos.

El NIST Cybersecurity Framework (CSF) también juega un papel crucial, ya que ofrece un conjunto de estándares, pautas y mejores prácticas para la gestión de la ciberseguridad, que puede ser integrado de manera flexible con los procesos existentes dentro de la organización. Este marco permite a las entidades implementar un enfoque sistemático para gestionar y reducir el riesgo cibernético (IBM, 2020).

Adicionalmente, el COBIT (Control Objectives for Information and Related Technologies) se incluye como un marco de gobernanza que apoya la alineación entre la tecnología de la información (TI) y los objetivos estratégicos de la organización. COBIT

proporciona directrices para gestionar los recursos de TI de manera eficiente y efectiva, garantizando la integridad y protección de la información (ISACA, 2019).

Este conjunto de marcos y metodologías garantiza un enfoque robusto y multidimensional para el diseño, implementación y evaluación continua de un SGSI, asegurando que los riesgos tecnológicos sean gestionados de manera proactiva, alineados con las mejores prácticas internacionales y con un enfoque en la continuidad operativa y la protección de los activos de información.

Diseño Metodológico

Para el logro de los objetivos propuestos, es necesario realizar un diseño metodológico apropiado que permita desarrollar el uso de técnicas e instrumentos para garantizar los resultados esperados. A continuación, se exponen el enfoque, el tipo de investigación, diseño de investigación, población y muestra.

Tipo de Investigación

Teniendo en cuenta los objetivos planteados, esta investigación busca analizar los riesgos, vulnerabilidades, amenazas y controles asociados a los activos de información de la Personería Municipal de Armenia, evaluando su impacto en la calidad de los servicios prestados a través de los programas que ofrece la entidad.

Para ello, se empleará un tipo de investigación no experimental de corte transversal. Según, (Hernandez Sampieri & Mendoza Torres, 2018, pág. 152), la investigación no experimental "se realiza sin manipular deliberadamente las variables; lo que se hace en este tipo de investigación es observar fenómenos tal y como se presentan en su contexto natural para, posteriormente, analizarlos". De esta forma, se recopilarán datos en un solo momento, permitiendo identificar el estado actual de la gestión de la información en la organización y establecer las bases para el diseño del Sistema de Gestión de Seguridad de la Información (SGSI).

La investigación desempeña un papel clave en la identificación del estado actual de la seguridad de la información, permitiendo un análisis detallado de los datos recopilados. Esto facilita el seguimiento necesario para comprender, gestionar y visualizar los riesgos, proporcionando una herramienta eficaz para la toma de decisiones oportunas por parte de la Personería Municipal de Armenia. En el contexto del diseño de un Sistema de Gestión de

Seguridad de la Información (SGSI) basado en las normas ISO/IEC 27001, este enfoque garantiza un análisis estructurado, alineado con estándares internacionales, que contribuye a fortalecer la gestión de la seguridad y el cumplimiento normativo. De acuerdo con (Hernandez Sampieri & Mendoza Torres, 2018), los diseños de investigación transeccional o transversal recopilan información en un único momento, con el propósito de describir variables y analizar su interrelación en un contexto determinado, lo cual resulta adecuado para este estudio.

Enfoque Investigativo

La investigación se desarrollará bajo un enfoque mixto, combinando métodos cuantitativos y cualitativos para aprovechar las fortalezas de ambos y minimizar sus debilidades potenciales, conforme a lo planteado por (Hernandez Sampieri & Mendoza Torres, 2018). Esta combinación agrega valor al estudio, permite una evaluación más integral, proporcionando no solo datos numéricos sobre el estado de la seguridad informática, sino un entendimiento más profundo de los factores organizacionales y humanos que influyen en la gestión de la seguridad de la Personería Municipal de Armenia.

Desde el enfoque cuantitativo, se recopilarán métricas relacionadas con el cumplimiento normativo, evaluación de riesgos, controles existentes y niveles de madurez, mediante herramientas como listas de verificación e indicadores de desempeño. Paralelamente, el enfoque cualitativo permitirá examinar aspectos organizacionales y humanos, como la percepción de los empleados sobre la cultura de ciberseguridad y el diagnóstico interno en gestión de seguridad, mediante entrevistas y análisis documental. Esta metodología permitirá diseñar un Sistema de Gestión de Seguridad de la Información ajustado a las necesidades reales de la organización y alineado con los estándares internacionales.

Población y Muestra

El objeto de estudio de esta investigación es la Personería Municipal de Armenia, una entidad del orden territorial que forma parte de la rama ejecutiva del Ministerio Público en Colombia, encargada de la defensa de los derechos humanos, la vigilancia de la conducta oficial y la protección del interés público. Se trata de una entidad pública de tamaño pequeño, con funciones administrativas, jurídicas y sociales, que presta atención directa a la ciudadanía del municipio de Armenia.

La población total de la entidad está compuesta por aproximadamente 48 funcionarios y contratistas activos, distribuidos en diferentes áreas: atención al ciudadano, representación judicial, vigilancia administrativa, gestión documental y tecnologías de la información, entre otros.

Según (Hernandez Sampieri & Mendoza Torres, 2018) , la muestra corresponde a un subgrupo representativo de la población de interés, definido y delimitado de manera precisa, sobre el cual se recolectarán los datos necesarios para el estudio. La selección de la muestra incluye únicamente a los colaboradores que accedan voluntariamente a participar, y que tengan un conocimiento o rol directo en los procesos estratégicos e informáticos. Esto garantiza que la información recolectada sea pertinente y relevante para el diagnóstico del estado actual de la seguridad de la información en la entidad. La muestra para el proyecto se centrará particularmente en:

- Funcionarios con responsabilidades en el tratamiento, gestión o custodia de información sensible, tanto física como digital.

- Personal del área de Tecnología de la Información, conformada por 1 técnico, encargados de la infraestructura tecnológica, la administración de redes, servidores, software institucional y soporte a usuarios.

Variables de la Investigación

Para el desarrollo del proyecto de diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Personería Municipal de Armenia, se consideran dos tipos de variables: cualitativas y cuantitativas, que permiten un análisis integral de los factores que influyen en la seguridad de la información dentro de la organización.

Variables de índole cualitativa: Estas se identificarán a partir de la observación, entrevistas y revisión documental. Se enfocan en aspectos como la percepción del personal frente a la seguridad de la información, la cultura organizacional y los procesos internos que afectan la confidencialidad, integridad y disponibilidad de la información. Su análisis permitirá comprender los elementos humanos y estructurales que inciden en la gestión de la seguridad.

Variables de índole cuantitativa: Son definidas con base en estándares como ISO/IEC 27001 y COBIT, y se centran en datos medibles como el número de controles existentes, niveles de cumplimiento normativo, madurez en la gestión de riesgos, y métricas de seguridad aplicables. Estas variables facilitarán la identificación de brechas y la toma de decisiones fundamentadas para estructurar el SGSI propuesto.

Técnicas e Instrumentos de Recolección de Información

Las técnicas de recopilación de datos ayudan a obtener la información necesaria para examinar y desarrollar correctamente los temas de estudio y su contexto. Se aplicarán las siguientes técnicas:

Fuentes Primarias

- Entrevistas dirigidas al personal clave del área de Tecnología de la Información.

Estos expertos, al estar directamente involucrados en la gestión de los sistemas y activos de información, proporcionarán información crítica sobre los procesos actuales, las prácticas de seguridad implementadas y las principales dificultades que enfrenta la entidad.

- Observación directa sobre los activos de información identificados, con el fin de analizar su estado, vulnerabilidades, niveles de exposición y prácticas asociadas a su gestión. Esta fuente de información permitirá complementar el análisis de riesgos y evaluar la efectividad de los controles existentes.

Fuentes Secundarias

- Documentos oficiales de la Personería Municipal de Armenia, informes estadísticos, información institucional y normativa disponible en páginas web oficiales y literatura especializada. Estas fuentes permitirán contextualizar el estado actual de la seguridad de la información y servirán como base técnica y normativa para el diseño del SGSI.

Metodología de Análisis de Riesgos

El análisis de riesgos se desarrollará utilizando la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), promovida por el Ministerio de Asuntos Económicos y Transformación Digital de España. Esta metodología permitirá identificar los activos, las amenazas que los afectan, las vulnerabilidades presentes y el impacto potencial sobre la misión institucional, estructurando un plan de tratamiento de riesgos que sirva de base para el SGSI.

Herramientas de Apoyo

Se emplearán herramientas tecnológicas de apoyo para facilitar el análisis de datos:

- SPSS (Statistical Package for the Social Sciences): para el procesamiento estadístico de los datos obtenidos en las encuestas aplicadas al personal, permitiendo generar medidas de tendencia central, tablas de frecuencia, cruces de variables y análisis inferencial.
- Microsoft Excel: para el registro, categorización y visualización preliminar de los datos recolectados.
- Google Forms: para la aplicación de encuestas digitales de forma ágil y centralizada a los funcionarios de planta y contratistas de la Personería Municipal de Armenia.
- Plantilla MAGERIT: como base para la estructuración del análisis de riesgos y elaboración del plan de tratamiento.

Variables Clave

En el desarrollo del proyecto de diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para la Personería Municipal de Armenia, es fundamental definir variables clave que permitan medir de manera objetiva el avance y cumplimiento de los objetivos planteados. Estas variables, tanto cualitativas como cuantitativas, servirán como base para diagnosticar el estado actual de la seguridad de la información, evaluar los riesgos, determinar el nivel de madurez de los controles existentes, y diseñar estrategias de mejora alineadas con los marcos ISO/IEC 27001 y COBIT. Cada variable ha sido seleccionada en función de su relevancia para el contexto del problema identificado y se operacionaliza mediante indicadores específicos que facilitan su medición y análisis durante el desarrollo de la investigación.

- Nivel de cumplimiento de controles de seguridad existentes: La definición operativa del proyecto se refiere a la proporción (%) de controles de seguridad implementados en los procesos de la Personería Municipal de Armenia respecto al total de controles exigidos por la norma ISO/IEC 27001, medido a través de una verificación documental y entrevistas a

responsables de áreas. Esta variable es relevante para establecer el grado real de protección de los activos de información frente a amenazas internas y externas. Medirla permite identificar brechas específicas que afectan la seguridad de los servicios prestados, y priorizar acciones correctivas que respalden el diseño de un SGSI eficaz.

- **Número y criticidad de riesgos identificados:** La definición operativa contempla el conteo total de riesgos de seguridad de la información detectados en los activos críticos de la entidad, clasificados por su nivel de impacto (alto, medio, bajo) según metodologías estandarizadas de gestión de riesgos como ISO 27005. Dado el contexto actual de amenazas cibernéticas y operativas, esta variable es crucial para enfocar los esfuerzos en los riesgos más significativos que pueden comprometer la misión institucional. Priorizar los riesgos facilita diseñar medidas de seguridad más efectivas y adecuadas a las necesidades reales de la organización.

- **Porcentaje de cumplimiento de requisitos ISO/IEC 27001:** La definición operativa establece la relación porcentual (%) entre los requisitos de la norma ISO/IEC 27001 cumplidos y los requisitos aplicables al entorno organizacional de la Personería Municipal de Armenia, verificados mediante un análisis GAP estructurado. Esta variable mide de forma concreta el nivel de alineación de la entidad con las mejores prácticas internacionales en seguridad de la información. Su análisis es esencial para diseñar un SGSI que no solo sea efectivo, sino también certificable en un futuro, aumentando la confianza de los ciudadanos en la gestión de sus datos.

- **Número de políticas y procedimientos diseñados:** La definición operativa corresponde a la cantidad de documentos normativos creados (políticas, procedimientos, instructivos) que aborden la gestión de la seguridad de la información, elaborados conforme a los requisitos de la norma ISO/IEC 27001 y adaptados al contexto de la Personería Municipal de

Armenia. La ausencia de documentación formal debilita la implementación y sostenibilidad de cualquier sistema de gestión. Esta variable es crítica para asegurar que los procesos de seguridad estén claramente definidos, sean comprensibles para todo el personal y faciliten la correcta ejecución y mantenimiento del Sistema de Gestión de Seguridad de la Información.

- Nivel de estructuración de roles, responsabilidades y mecanismos de seguimiento del SGSI: El grado de formalización y claridad en la asignación de roles, responsabilidades y mecanismos de seguimiento del SGSI será evaluado mediante la verificación documental y entrevistas, tomando como referencia los principios de gobernanza de TI definidos en COBIT. Esta variable permite medir el alineamiento del SGSI con una estructura de gobernanza efectiva, lo que garantiza una gestión transparente, responsable y coherente con los objetivos institucionales. Su análisis es esencial para fortalecer la toma de decisiones, la rendición de cuentas y la sostenibilidad del sistema de seguridad de la información.

Hipótesis

La aplicación de una metodología basada en los estándares ISO/IEC 27001 y el marco COBIT permitirá diseñar un Sistema de Gestión de Seguridad de la Información efectivo y aplicable a la Personería Municipal de Armenia, mejorando significativamente la protección de sus activos de información y alineando la seguridad con sus objetivos institucionales

Análisis crítico sobre la aplicabilidad y efectividad de la metodología: La metodología seleccionada para el diseño del SGSI combina un enfoque mixto de investigación (cualitativo y cuantitativo) apoyado en estándares reconocidos internacionalmente como la norma ISO/IEC 27001 y el marco COBIT. Esta elección es altamente aplicable al contexto de la Personería Municipal de Armenia, ya que proporciona un marco estructurado, sistemático y validado para abordar la seguridad de la información de manera integral.

Desde la perspectiva de la aplicabilidad, el uso de ISO/IEC 27001 asegura que el diseño del sistema se base en mejores prácticas aceptadas a nivel mundial, lo que facilita su alineación con los requerimientos legales, normativos y de buenas prácticas en el sector público. Por su parte, COBIT proporciona directrices claras para el gobierno y la gestión de TI, permitiendo que los objetivos de seguridad estén en sintonía con los objetivos estratégicos de la organización.

Respecto a la efectividad, esta metodología promueve una identificación sistemática de riesgos, vulnerabilidades y controles, permitiendo diseñar políticas y procedimientos que respondan a las necesidades reales de la entidad. La combinación de análisis cualitativos y cuantitativos fortalece la robustez del diagnóstico y del diseño propuesto, favoreciendo una toma de decisiones más informada.

No obstante, existen retos importantes que pueden afectar su efectividad. En primer lugar, la Personería Municipal puede enfrentar limitaciones de recursos humanos, financieros y tecnológicos que dificulten la implementación inmediata de todas las recomendaciones derivadas del diseño del SGSI. Además, el éxito dependerá en gran medida del compromiso de la alta dirección y de la cultura organizacional respecto a la gestión de la seguridad de la información.

Por último, la metodología seleccionada es adecuada y ofrece alta aplicabilidad y efectividad para diseñar un SGSI en la Personería Municipal de Armenia, siempre que se consideren las capacidades internas, se garantice el apoyo institucional y se realice una adaptación contextualizada de las buenas prácticas internacionales.

Desarrollo de los Objetivos

Realizar un Diagnóstico del Estado Actual de la Seguridad de la Información en la Personería Municipal de Armenia

El diagnóstico del estado actual de la seguridad de la información permitirá identificar riesgos, vulnerabilidades y debilidades en los procesos y sistemas de la Personería Municipal de Armenia. Esta evaluación servirá como base para diseñar un SGSI que responda a las necesidades reales de la entidad y fortalezca la protección de sus activos de información.

Análisis del Entorno

Para analizar los factores que afectan la seguridad y privacidad de la información, se utiliza un diagrama de Ishikawa o espina de pescado. Esta herramienta permite identificar, desde una perspectiva interna y externa, las posibles debilidades que podrían aumentar el riesgo de incidentes relacionados con la protección de la información.

Figura 4

Diagrama Análisis del Entorno



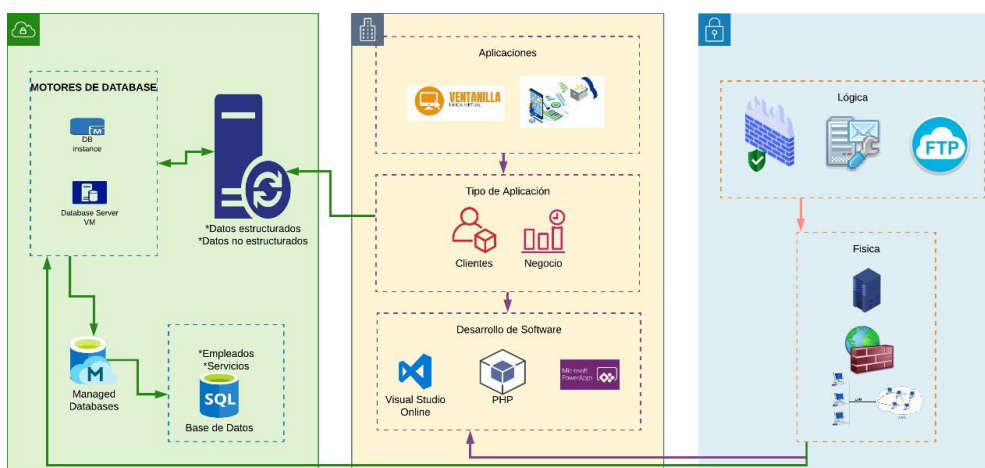
Nota. Diagrama Análisis del entorno (Personería Municipal de Armenia en Quindío, 2024).

Tomada de <https://www.personeria-armenia.gov.co/>

El Formulario Único Reporte de Avances de la Gestión (FURAG) es una herramienta que permite medir y evaluar el avance de las entidades en la implementación de las políticas del Modelo Integrado de Planeación y Gestión (MIPG). Dentro de esta evaluación, se analiza la política de Gobierno Digital, que incluye aspectos como arquitectura tecnológica, estado abierto, uso de datos y seguridad de la información. Su objetivo es mejorar la gestión institucional y los servicios a la ciudadanía. La Personería Municipal de Armenia obtuvo un 67,9% en esta política, ubicándose en un nivel intermedio, reflejando avances importantes, pero también áreas de mejora. En cuanto a seguridad y privacidad de la información, la entidad obtuvo una calificación de 57,5%, lo que indica que aún hay oportunidades para fortalecer este aspecto.

Por otra parte, el siguiente diagrama representa la arquitectura tecnológica de la Personería Municipal de Armenia, proporcionando una visión estructurada de los componentes que conforman su infraestructura de tecnologías de la información. Este esquema permite identificar las principales capas tecnológicas que soportan la operación institucional, así como los controles de seguridad implementados en cada nivel.

La siguiente figura identificará claramente los puntos donde existen controles activos, como firewalls, y también áreas con debilidades, por ejemplo, servidores sin respaldo automatizado o aplicaciones sin control de acceso. Este enfoque facilitará no solo la comprensión del estado actual de la seguridad, sino también la priorización de intervenciones para cerrar brechas y fortalecer la protección de los activos de información.

Figura 5.*Diagrama Arquitectura Tecnológica*

Nota. Diagrama Arquitectura Tecnológica (Autoría Propia)

La arquitectura se organiza en capas que incluyen:

- Infraestructura física y lógica (servidores, redes, equipos de comunicación).
- Sistemas de información y aplicaciones (plataformas internas y de atención al ciudadano).
- Gestión de seguridad de la información (firewalls, autenticación, respaldo de datos).

Diagnostico Organizacional

Después de comprender el entorno, se realiza una evaluación interna de la organización para identificar fortalezas y debilidades.

Procesamiento estadístico de datos: Se analizan los resultados obtenidos de la encuesta realizada a los funcionarios de la Personería Municipal de Armenia. Estos resultados permiten

evaluar la seguridad de la información en la entidad. Para ello, se tuvieron en cuenta dimensiones (preguntas) como elementos determinantes, los cuales se abordaron a través de la encuesta.

- Fase Recolección de la información: Se utiliza un instrumento para recopilar información y determinar los elementos clave de la seguridad de la información. Como técnica, se emplea una encuesta semiestructurada, aplicada al personal de la Personería Municipal de Armenia, toda vez que ellos poseen una visión integral de los procesos que se desarrollan. Asimismo, para contrastar los resultados, se encuesta al funcionario soporte del área TIC.
- Fase Tabulación y Análisis: Las encuestas se organizan y analizan para identificar el modelo de gestión del conocimiento utilizado por los grupos de investigación. Para este proceso, se utilizó el software SPSS, donde primero se realizó un análisis descriptivo para resumir los datos y encontrar las dimensiones más importantes que expliquen la mayor cantidad de información.

Análisis de confiabilidad y validez: Un instrumento de medición debe ser válido y confiable. La confiabilidad se refiere a la consistencia de los resultados, mientras que la validez indica qué tan bien mide realmente lo que se pretende evaluar. Para calcular estos aspectos, se pueden usar diferentes métodos, como el alfa de Cronbach, que ayuda a determinar la fiabilidad.

- Alfa de Cronbach: El coeficiente Alfa de Cronbach mide la consistencia interna de un conjunto de preguntas, basándose en el promedio de sus correlaciones. Sirve para evaluar si eliminar un ítem mejora o empeora la fiabilidad de la prueba. La tabla 2 muestra las recomendaciones para interpretar este coeficiente.

Tabla 2*Valores del Cálculo del Coeficiente de Alfa de Cronbach*

Rango	Magnitud
0.81 – 1.00	Muy alta
0.61 – 0.80	Alta
0.41 - 0.60	Moderada
0.21 – 0.40	Baja
0.001 – 0.20	Muy baja

Nota. Coeficiente de Alfa de Cronbach. Tomada de (SPSS datos del instrumento)

La tabla 3 muestra el resultado de Alfa de Cronbach, en donde se puede identificar que, a mayor valor de Alfa mayor fiabilidad. El mayor valor teórico de Alfa es 1.

Tabla 3*Índice de Confiabilidad de Alfa de Cronbach*

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
,909	19

Nota. Índice de Confiabilidad Tomada de (SPSS datos del instrumento)

El índice de confiabilidad de las variables es .909 se concluye que el instrumento tiene alta confiabilidad.

Análisis de factores: El análisis factorial es un método que ayuda a reducir datos agrupando variables relacionadas entre sí. Permite identificar conjuntos de variables con significados comunes, simplificando la información. Antes de aplicar este análisis, es necesario verificar si los datos son adecuados. Para esto, se realizan pruebas llamadas medidas de adecuación muestral, como el test de esfericidad de Bartlett y la prueba de adecuación de Kaiser-

Meyer-Olkin (KMO). (López Aguado & Gutiérrez Provecho, 2019). La prueba de esfericidad de Bartlett analiza si hay correlaciones significativas entre las variables.

Tabla 4

Prueba de Esfericidad de Bartlett y el Índice KMO

Prueba de KMO y Bartlett		
Medida Kaiser-Meyer-Olkin de adecuación de muestreo		,768
	Aprox. Chi-cuadrado	529,110
Prueba de esfericidad de Bartlett	Gl	120
	Sig.	<,001

Nota. Prueba de Esfericidad de Bartlett Tomada de (SPSS datos del instrumento)

En la tabla 4, el valor de KMO es 0.768, lo que indica que el análisis factorial sí puede realizarse. Además, la matriz de correlaciones muestra un valor cercano a cero, lo que sugiere una alta correlación entre las variables. Por último, el valor de significancia (Sig) en la prueba de esfericidad de Bartlett es 0.001, confirmando que el análisis factorial es válido.

Tabla 5

Comunalidades

Comunalidades		
	Inicial	Extracción
Cargo Entidad	1,000	,780
Vinculación Entidad	1,000	,832
Experiencia Entidad	1,000	,675
Uso Sistemas Informáticos	1,000	,849
Conocimiento Seguridad Informática	1,000	,725
Información Sensible	1,000	,868
Capacitación Seguridad Informática	1,000	,945
Efectividad Capacitación	1,000	,916
Capacitación Alineada Riesgos	1,000	,944

Comunalidades		
	Inicial	Extracción
Frecuencia Cambio Contraseñas	1,000	,921
Uso Diferentes Contraseñas	1,000	,899
Almacenamiento Contraseña	1,000	,937
Correo Sospechoso	1,000	,913
Seguridad Sistemas Internos	1,000	,917
Dispositivos Externos	1,000	,896
Efectividad Soporte TIC	1,000	,945
Compromiso Entidad Seguridad	1,000	,924
Reportar Incidente Seguridad	1,000	,913
Cultura Seguridad Informática	1,000	,924

Nota. Comunalidades Tomada de (SPSS datos del instrumento)

En la tabla 5 presenta las comunalidades con valores altos, lo que implica que todas las variables tienen una buena representación en el espacio de los factores (Método de extracción: análisis de componentes principales).

Análisis de Correlaciones: El análisis de correlación ayuda a medir la relación entre dos o más variables. Con este método, se pueden identificar conexiones y patrones en los datos. En este caso, se usa SPSS para calcular la correlación entre variables, aplicando coeficientes como Pearson. También se verifica si estas relaciones son significativas o si ocurren por casualidad.

Correlaciones

		Cargo Entidad	Vinculación Entidad	Experiencia Entidad	Uso Sistemas Informáticos	Conocimiento Seguridad I.	Información Sensible	Capacitación Seguridad informática	Efectividad Capacitación	Capacitación Alineada R.	Frecuencia Cambio Contraseñas	Uso Diferentes Contraseñas	Almacenamiento Contraseña	Correo Sospechoso	Seguridad Sistemas Internos	Dispositivos Externos	Efectividad Soporte TIC	Compromiso Entidad Seguridad	Reportar Incidente Seguridad	Cultura Seguridad Informática
Capacitación Alineada Riesgos	Correlación de Pearson Sig. (bilateral) N	-,388 ,082 21	,117 ,614 21	,296 ,193 21	,820** <,001 21	,762** <,001 21	,826** <,001 21	,968** <,001 21	,952** <,001 21	1 21	,927** <,001 21	,944** <,001 21	,905** <,001 21	,905** <,001 21	,917** <,001 21	,865** <,001 21	,931** <,001 21	,888** <,001 21	,799** <,001 21	,888** <,001 21
Frecuencia Cambio Contraseñas	Correlación de Pearson Sig. (bilateral) N	-,267 ,241 21	,117 ,614 21	,412 ,064 21	,820** <,001 21	,799** <,001 21	,826** <,001 21	,933** <,001 21	,913** <,001 21	,927** <,001 21	1 21	,983** <,001 21	,944** <,001 21	,905** <,001 21	,872** <,001 21	,865** <,001 21	,888** <,001 21	,888** <,001 21	,835** <,001 21	,888** <,001 21
Uso Diferentes Contraseñas	Correlación de Pearson Sig. (bilateral) N	-,269 ,238 21	,168 ,466 21	,361 ,107 21	,813** <,001 21	,813** <,001 21	,820** <,001 21	,918** <,001 21	,895** <,001 21	,944** <,001 21	,983** <,001 21	1 21	,922** <,001 21	,874** <,001 21	,877** <,001 21	,835** <,001 21	,890** <,001 21	,852** <,001 21	,809** <,001 21	,852** <,001 21
Almacenamiento Contraseña	Correlación de Pearson Sig. (bilateral) N	-,201 ,383 21	,180 ,435 21	,348 ,122 21	,790** <,001 21	,725** <,001 21	,791** <,001 21	,911** <,001 21	,922** <,001 21	,905** <,001 21	,944** <,001 21	,922** <,001 21	1 21	,960** <,001 21	,928** <,001 21	,875** <,001 21	,903** <,001 21	,909** <,001 21	,887** <,001 21	,909** <,001 21
Correo Sospechoso	Correlación de Pearson Sig. (bilateral) N	-,294 ,196 21	,076 ,742 21	,350 ,120 21	,789** <,001 21	,679** <,001 21	,793** <,001 21	,921** <,001 21	,933** <,001 21	,905** <,001 21	,905** <,001 21	,874** <,001 21	,960** <,001 21	1 21	,956** <,001 21	,865** <,001 21	,921** <,001 21	,930** <,001 21	,841** <,001 21	,930** <,001 21
Seguridad Sistemas Internos	Correlación de Pearson Sig. (bilateral) N	-,328 ,146 21	,114 ,623 21	,264 ,247 21	,797** <,001 21	,724** <,001 21	,806** <,001 21	,900** <,001 21	,911** <,001 21	,917** <,001 21	,872** <,001 21	,877** <,001 21	,928** <,001 21	,956** <,001 21	1 21	,866** <,001 21	,953** <,001 21	,917** <,001 21	,800** <,001 21	,917** <,001 21
Dispositivos Externos	Correlación de Pearson Sig. (bilateral) N	-,182 ,429 21	,039 ,867 21	,377 ,092 21	,801** <,001 21	,728** <,001 21	,806** <,001 21	,919** <,001 21	,892** <,001 21	,865** <,001 21	,865** <,001 21	,835** <,001 21	,875** <,001 21	,865** <,001 21	,866** <,001 21	1 21	,927** <,001 21	,931** <,001 21	,923** <,001 21	,931** <,001 21
Efectividad Soporte TIC	Correlación de Pearson Sig. (bilateral) N	-,263 ,249 21	,105 ,650 21	,241 ,292 21	,834** <,001 21	,791** <,001 21	,849** <,001 21	,922** <,001 21	,895** <,001 21	,931** <,001 21	,888** <,001 21	,890** <,001 21	,903** <,001 21	,921** <,001 21	,953** <,001 21	,927** <,001 21	1 21	,958** <,001 21	,856** <,001 21	,958** <,001 21

		Correlaciones																		
		Cargo Entidad	Vinculación Entidad	Experiencia Entidad	Uso Sistemas Informáticos	Conocimiento Seguridad I.	Información Sensible	Capacitación Seguridad informática	Efectividad Capacitación	Capacitación Alineada R.	Frecuencia Cambio Contraseñas	Uso Diferentes Contraseñas	Almacenamiento Contraseña	Correo Sospechoso	Seguridad Sistemas Internos	Dispositivos Externos	Efectividad Soporte TIC	Compromiso Entidad Seguridad	Reportar Incidente Seguridad	Cultura Seguridad Informática
Compromiso Entidad Seguridad	Correlación de Pearson	-	,096	,344	,761**	,683**	,774**	,917**	,899**	,888**	,888**	,852**	,909**	,930**	,917**	,931**	,958**	1	,899**	1,000**
	Sig. (bilateral)	,175	,679	,127	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001		<,001	<,001
	N	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21
Reportar Incidente Seguridad	Correlación de Pearson	,043	,193	,386	,696**	,599**	,700**	,848**	,823**	,799**	,835**	,809**	,887**	,841**	,800**	,923**	,856**	,899**	1	,899**
	Sig. (bilateral)	,852	,401	,084	<,001	,004	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001		<,001
	N	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21
Cultura Seguridad Informática	Correlación de Pearson	-	,096	,344	,761**	,683**	,774**	,917**	,899**	,888**	,888**	,852**	,909**	,930**	,917**	,931**	,958**	1,000**	,899**	1
	Sig. (bilateral)	,175	,447	,679	,127	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001	<,001
	N	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21

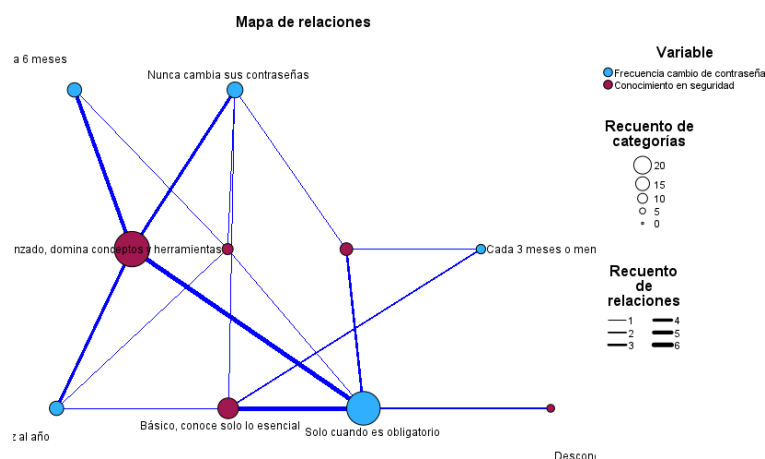
Nota. Correlaciones. Tomada de (SPSS datos del instrumento)

- Conocimiento en seguridad de la Información y frecuencia de cambio de contraseñas: El análisis realizado mediante un mapa de relaciones generado en SPSS, se evidenció una correlación directa entre el nivel de conocimiento en seguridad informática de los funcionarios y la frecuencia con la que cambian sus contraseñas. Los datos muestran que los funcionarios que dominan conceptos y herramientas de seguridad informática tienden a cambiar sus contraseñas cada tres meses o con mayor frecuencia, en línea con buenas prácticas reconocidas, aquellos con un conocimiento básico o limitado manifiestan cambiar sus contraseñas solo cuando es obligatorio o incluso nunca lo hacen.

Esta correlación sugiere que el grado de alfabetización digital en seguridad informática influye directamente en los hábitos de protección personal y organizacional. Si bien existe un grupo consciente y proactivo, la mayoría actúa de manera reactiva o por imposición, lo que pone en riesgo la confidencialidad y la integridad de la información institucional.

Figura 6

Mapa de Correlaciones Conocimiento de Seguridad y Cambio de Contraseñas

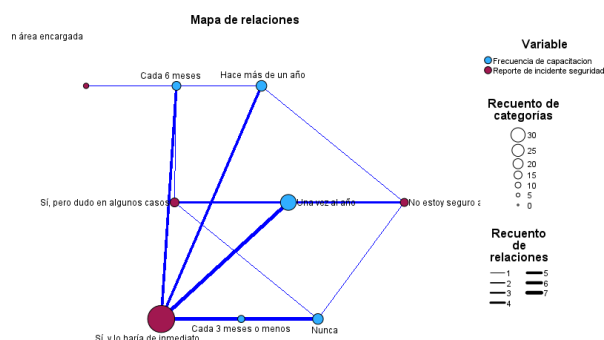


Nota. Mapa de Correlaciones. Tomada de (SPSS datos del instrumento)

- **Frecuencia de capacitaciones y reporte de incidentes de seguridad:** Los encuestados manifiestan haber recibido capacitación hace más de un año, o solo una vez al año, tendieron a manifestar dudas al momento de reportar incidentes o mostraron inseguridad respecto a cómo actuar ante un posible evento. Este comportamiento evidencia una menor claridad sobre los procedimientos establecidos, lo cual podría generar retrasos o incluso omisiones en la notificación de incidentes relevantes. Aún más preocupante es el caso de aquellos funcionarios que indicaron no recibir ningún tipo de capacitación en seguridad informática. En estos casos, las respuestas predominantes se vinculan a opciones como “no estoy seguro” o “nunca reportaría”, lo cual representa un riesgo considerable para la organización, ya que estos individuos podrían convertirse en eslabones débiles dentro de la cadena de protección de los activos de información. Este análisis demuestra que fortalecer la formación continua en seguridad no solo mejora la competencia técnica del recurso humano, sino que también constituye un pilar fundamental en la consolidación de un entorno organizacional más resiliente ante las amenazas de seguridad de la información.

Figura 7

Mapa de Correlaciones Frecuencia de Capacitaciones y Reporte de Incidentes

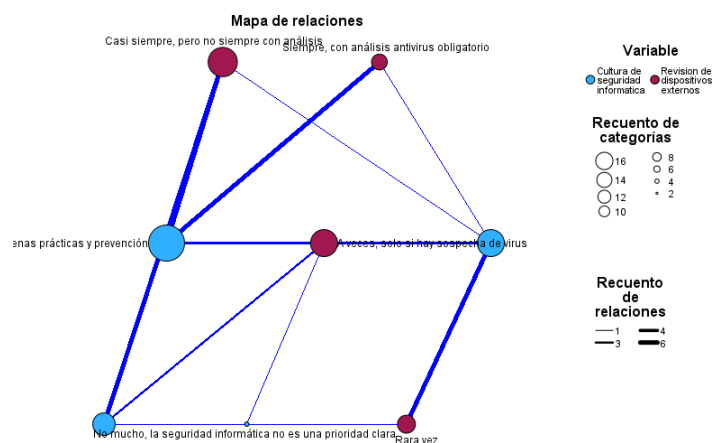


Nota. Mapa de Correlaciones. Tomada de (SPSS datos del instrumento)

- **Cultura de seguridad informática y revisión de dispositivos externos:** El análisis de la relación entre la cultura de seguridad informática en la organización y la frecuencia con la que se revisan los dispositivos externos, como memorias USB o discos portátiles, evidencia una correlación directa entre el nivel de concienciación del personal y la aplicación de prácticas preventivas. A partir del mapa de relaciones, se identificó que los funcionarios que manifestaron una cultura sólida de seguridad en donde las buenas prácticas son parte del comportamiento habitual también reportaron realizar revisiones constantes de los dispositivos externos, incluyendo el uso obligatorio de antivirus. En contraste, se observó que aquellos colaboradores que consideraron que la seguridad informática no es una prioridad clara o relevante dentro de sus funciones, tienden a revisar los dispositivos externos solo en caso de sospechas o, en el peor de los casos, rara vez lo hacen. La baja revisión de estos elementos puede derivar en la introducción inadvertida de software malicioso, generando riesgos para la integridad, disponibilidad y confidencialidad de la información institucional.

Figura 8

Mapa de Correlación Cultura Organizacional y Revisión de Dispositivos



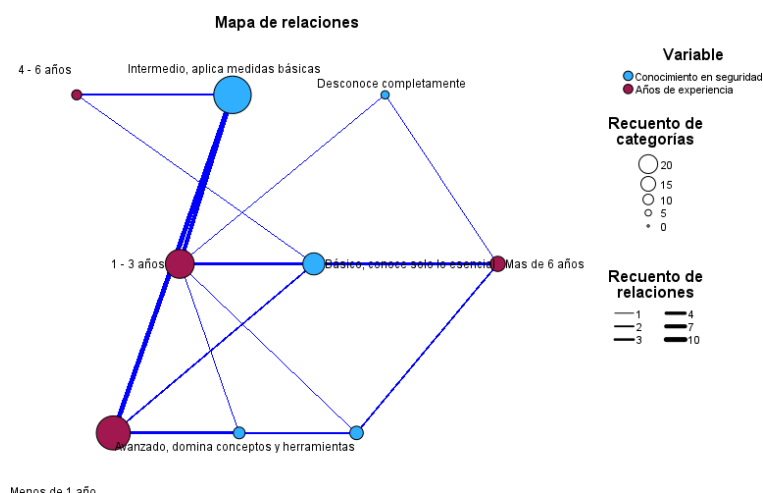
Nota. Mapa de correlación. Tomada de (SPSS datos del instrumento)

- Uso Diferentes Conocimiento en seguridad y años de experiencia en la entidad:

Los empleados con entre 1 y 3 años de experiencia muestran una fuerte vinculación con niveles de conocimiento variados, destacándose principalmente en el nivel intermedio, en el cual aplican medidas básicas de seguridad. Asimismo, se destaca que quienes cuentan con más de 6 años de experiencia tienden a ubicarse en el nivel de conocimiento “básico, conoce solo lo esencial”, lo cual podría interpretarse como una señal de estancamiento o falta de actualización en temas de seguridad informática, pese a su trayectoria profesional. Por otro lado, aquellos que manifiestan un conocimiento avanzado, es decir, dominio de conceptos y herramientas se concentran mayormente entre quienes tienen entre 4 y 6 años de experiencia. Finalmente, el grupo con menos de un año de experiencia o aquellos que “desconocen completamente” sobre seguridad informática, presentan relaciones menos marcadas o aisladas, lo cual pone de manifiesto la importancia de establecer programas de inducción sólidos para el nuevo personal, que incluyan temas de ciberseguridad desde el inicio de su vinculación institucional.

Figura 9

Mapa de Correlaciones Conocimiento en Seguridad y Años de Experiencia

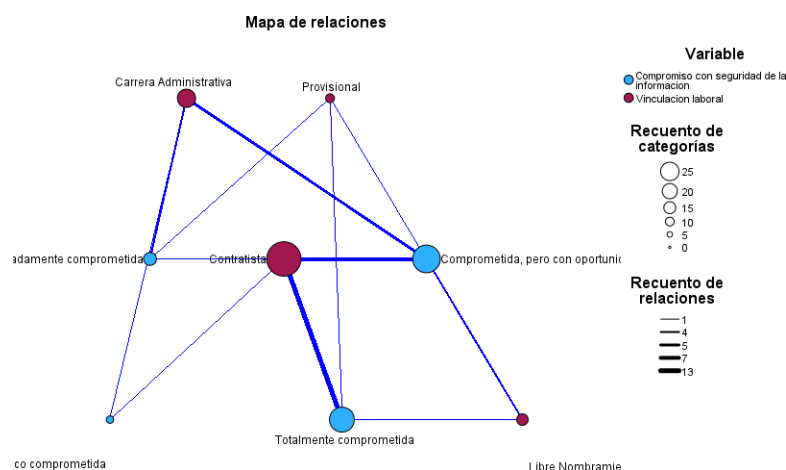


Nota. Mapa de correlación. Tomada de (SPSS datos del instrumento)

- **Cargo en la entidad y compromiso con la entidad con la seguridad informática:** El mapa de relaciones muestra una fuerte asociación entre los contratistas y un alto compromiso con la seguridad de la información, lo que sugiere una actitud proactiva, posiblemente motivada por el cumplimiento de obligaciones específicas en sus contratos. Este grupo destaca con la mayor frecuencia en la categoría "totalmente comprometida". En contraste, los funcionarios de carrera administrativa se relacionan principalmente con un compromiso intermedio, lo que podría reflejar una percepción de menor urgencia frente a las políticas de seguridad, aunque también presentan casos con bajo compromiso. Los trabajadores en condición provisional muestran relaciones dispersas con niveles bajos de compromiso, indicando una necesidad de refuerzo en cultura de seguridad. Por su parte, el grupo de libre nombramiento tiene menor representación, pero muestra cierta inclinación hacia el compromiso total. En general, el tipo de vinculación laboral influye en el compromiso con la seguridad de la información, lo que sugiere la importancia de aplicar estrategias de concienciación adaptadas a cada perfil contractual.

Figura 10

Mapa de Correlaciones Cargo de la Entidad y el Compromiso con la Entidad



Nota. Mapa de correlación. Tomada de (SPSS datos del instrumento)

Inventario de Activos

Se identifican los activos clave que soportan las operaciones de la Personería Municipal de Armenia, además de clasificar los activos de información para garantizar su protección según su importancia y características específicas. La clasificación de activos se basa en tres principios: confidencialidad, integridad y disponibilidad.

Tabla 7

Clasificación de Acuerdo con la Confidencialidad

	Nomenclatura	Categoría	Valoración
Confidencialidad	MA	Muy Alto	La pérdida de confidencialidad es extremadamente perjudicial para la entidad.
	A	Alto	La pérdida de confidencialidad es altamente perjudicial para la entidad.
	M	Medio	La pérdida de confidencialidad es medianamente perjudicial para la entidad.
	B	Bajo	La pérdida de confidencialidad es poco perjudicial para la entidad.
	MB	Muy Bajo	La pérdida de confidencialidad no es perjudicial para la entidad o no aplica para el activo.

Nota. Clasificación de acuerdo con la confidencialidad (Autoría Propia)

Tabla 8

Clasificación de Acuerdo con la Disponibilidad

	Nomenclatura	Categoría	Valoración
Disponibilidad	MA	Muy Alto	La pérdida de disponibilidad es extremadamente perjudicial para la entidad.
	A	Alto	La pérdida de disponibilidad es altamente perjudicial para la entidad.
	M	Medio	La pérdida de disponibilidad es medianamente perjudicial para la entidad.
	B	Bajo	La pérdida de disponibilidad es poco perjudicial para la entidad.
	MB	Muy Bajo	La pérdida de disponibilidad no es perjudicial para la entidad o no aplica para el activo.

Nota. Clasificación de acuerdo con la disponibilidad (Autoría Propia)

Tabla 9*Clasificación de Acuerdo con la Integridad*

	Nomenclatura	Categoría	Valoración
Integridad	MA	Muy Alto	La pérdida de integridad es extremadamente perjudicial para la entidad.
	A	Alto	La pérdida de integridad es altamente perjudicial para la entidad.
	M	Medio	La pérdida de integridad es medianamente perjudicial para la entidad.
	B	Bajo	La pérdida de integridad es poco perjudicial para la entidad.
	MB	Muy Bajo	La pérdida de integridad no es perjudicial para la entidad o no aplica para el activo.

Nota. Clasificación de acuerdo con la integridad (Autoría Propia)

Mediante las visitas, se llevó a cabo un inventario detallado de los activos de información en la Personería Municipal de Armenia, clasificándolos en activos físicos (servidores, estaciones de trabajo, redes de comunicación y dispositivos de almacenamiento), lógicos (sistemas de información, bases de datos y software de gestión), personal (funcionario encargado de la administración y protección de la información) y documentales (políticas de seguridad, procedimientos internos y normativas aplicables).

Posteriormente, se realizará un análisis de riesgos para identificar amenazas como accesos no autorizados y fallos en la infraestructura, evaluando su impacto en la disponibilidad, integridad y confidencialidad de la información.

Es fundamental identificar los activos del proceso para incorporarlos en la metodología y evaluar los riesgos y controles existentes o por aplicar. Para optimizar la identificación y gestión de los activos, se establece su organización en diferentes categorías. Este enfoque facilita la comprensión por parte de los líderes de proceso, permitiéndoles reconocer qué activos forman

parte de sus responsabilidades y cómo deben ser administrados. En el desarrollo de este trabajo, se han definido las siguientes categorías:

Datos [D]: Incluye todos los datos generados, almacenados, procesados, sin importar su formato. Esto abarca bases de datos, documentos administrativos y registros digitales.

Software [SW]: Comprende las aplicaciones utilizadas para gestionar y optimizar los procesos organizacionales.

Equipos Informáticos [HW]: Hace referencia al equipo físico esencial para el desarrollo de actividades diarias, como computadoras, dispositivos, servidores, impresoras, cableado.

Redes de comunicación [COM]: Engloba los dispositivos que garantizan la conectividad, tales como routers, switches y pasarelas de comunicación.

Soporte de Información [MEDIA]: Abarca los medios utilizados para almacenar, proteger y gestionar los datos de una organización.

Servicios [S]: Abarca los recursos y procesos que garantizan el funcionamiento eficiente de la infraestructura tecnológica y operativa. Estos incluyen servicios de TI, conectividad.

Personal [P]: Incluye a los empleados directos, contratistas y cualquier persona con acceso a información interna o confidencial de la empresa.

Instalaciones [I]: Comprenden los espacios físicos donde se encuentran los sistemas esenciales para el funcionamiento de la organización, como oficinas.

Equipamiento Auxiliar [AUX]: Incluye aquellos activos que brindan soporte a los sistemas de información, pero que no han sido clasificados dentro de las categorías mencionadas.

Tabla 10*Inventario de Activos*

Datos del activo de información			
No.	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo
1	Base de Datos de PQRS	Andrés Felipe Piedrahita A	SOFTWARE
2	Portal Web de la Personería	Andrés Felipe Piedrahita A	SERVICIOS
3	Sistema de Información financiero	Juliana Victoria Ríos Quintero	SOFTWARE
4	Sistema de Información Ventanilla Única	Juliana Victoria Ríos Quintero	SOFTWARE
5	Servidor Principal	Andrés Felipe Piedrahita A	HARDWARE
6	Servidor físico adicional	Andrés Felipe Piedrahita A	HARDWARE
7	Correo Electrónico Institucional	Juliana Victoria Ríos Quintero	SERVICIOS
8	Backup de Base de Datos	Andrés Felipe Piedrahita A	DATOS
9	Licencias de Microsoft Office	Andrés Felipe Piedrahita A	SOFTWARE
10	Licencias de Windows	Andrés Felipe Piedrahita A	SOFTWARE
11	Router principal	Andrés Felipe Piedrahita A	COMUNICACIONES
12	Switches de red	Andrés Felipe Piedrahita A	COMUNICACIONES
13	Access Point	Andrés Felipe Piedrahita A	COMUNICACIONES
14	Historias Laborales	Katheryn Tatiana Patiño O	DATOS
15	Licencia Windows Server	Andrés Felipe Piedrahita A	SOFTWARE
16	Oficinas	Juliana Victoria Ríos Quintero	INSTALACIONES
17	Técnico TIC	Juliana Victoria Ríos Quintero	PERSONAL
18	Personera	Juliana Victoria Ríos Quintero	PERSONAL
19	Personeros delegados	Juliana Victoria Ríos Quintero	PERSONAL
20	Directores Administrativos	Juliana Victoria Ríos Quintero	PERSONAL
21	Funcionarios	Juliana Victoria Ríos Quintero	PERSONAL
22	Contratistas	Juliana Victoria Ríos Quintero	PERSONAL

Tabla 10 (Continuación)*Inventario de Activos*

Datos del activo de información			
No.	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo
23	Actas de comité	Katheryn Tatiana Patiño O	DATOS
24	Actos administrativos	Katheryn Tatiana Patiño O	DATOS
25	Comunicaciones Oficiales	Katheryn Tatiana Patiño O	DATOS
26	Contratos estatales	Katheryn Tatiana Patiño O	DATOS
27	Informes Institucionales	Katheryn Tatiana Patiño O	DATOS
28	Planes, programas y proyectos	Katheryn Tatiana Patiño O	DATOS
29	Conciliaciones	Luz Elena Osorno Arias	DATOS
30	Equipo Personera	Juliana Victoria Ríos Quintero	HARDWARE
31	Equipo Personeros delegados	Juliana Victoria Ríos Quintero	HARDWARE
32	Equipos jefes Administrativos	Juliana Victoria Ríos Quintero	HARDWARE
33	Equipo Soporte TIC	Andrés Felipe Piedrahita A	HARDWARE
34	Equipos funcionarios	Andrés Felipe Piedrahita A	HARDWARE
35	Equipos Contratistas	Andrés Felipe Piedrahita A	HARDWARE
36	Internet	Juliana Victoria Ríos Quintero	SERVICIOS
37	Rack	Andrés Felipe Piedrahita A	SOPORTE
38	Disco duro externo	Andrés Felipe Piedrahita A	SOPORTE
39	UPS	Andrés Felipe Piedrahita A	AUXILIAR
40	Impresoras	Andrés Felipe Piedrahita A	HARDWARE

Nota. Inventario de activos (Autoría Propia)

En la Personería Municipal de Armenia, se han identificado los activos de información para el desarrollo de sus funciones y la prestación de sus servicios. Estos activos incluyen documentos, bases de datos, sistemas y otros recursos que respaldan la gestión institucional. Su

adecuada protección y administración son fundamentales para garantizar la transparencia, eficiencia y continuidad en la atención a la ciudadanía. se organizan los datos para su identificación, se siguen estos pasos:

- Determinar qué información se genera en cada proceso de la empresa.
- Identificar la información que cada proceso usa de otros procesos para conocer su interacción.
- Clasificar los activos identificados.
- Realizar una correcta identificación de cada activo.

En cuanto a la responsabilidad de los activos, la entidad ha determinado que el dueño del proceso en el que se genera la información será el encargado de decidir quién puede acceder a ella. Esto asegura que cada activo tenga un responsable visible y que la gestión de la información esté distribuida entre el personal autorizado, bajo la supervisión del dueño del proceso.

Así mismo, se identificaron 40 activos de información clave que son fundamentales para la operación de Estrategias organizacionales. Estos garantizan el correcto desarrollo de las actividades, por lo que cualquier afectación podría impedir que la entidad cumpla con sus servicios, tanto internamente como para sus usuarios.

Aplicar una Metodología de Gestión de Riesgos para Identificar, Valorar y Clasificar los Riesgos Asociados a los Activos de Información

El objetivo de aplicar una metodología de gestión de riesgos busca identificar, valorar y clasificar los riesgos asociados a los activos de información de la Personería Municipal de Armenia. La prioridad se dará a los riesgos más críticos para garantizar que los esfuerzos de mitigación se enfoquen en las áreas más vulnerables. Además, se establecerá un plan de

tratamiento adecuado a la realidad tecnológica de la entidad, con el fin de minimizar los riesgos y asegurar la protección de la información sin afectar la operatividad.

Valoración Cualitativa de los Activos

Se identificó que los activos de la entidad tienen diferentes niveles de importancia y que, ante un imprevisto, el impacto puede variar. Por ello, se realizó una evaluación cualitativa basada en la metodología Magerit, considerando las siguientes dimensiones de seguridad:

- Autenticidad
- Confiabilidad
- Integridad
- Disponibilidad
- Trazabilidad

Esta metodología plantea preguntas relacionadas con cada dimensión y brinda ejemplos de activos a los que pueden aplicarse. Las respuestas a estas preguntas permitieron valorar adecuadamente cada activo

Tabla 11*Identificación de Activos*

EMPRESA: Personería Municipal de Armenia																		
INFORMACIÓN DE LOS ACTIVOS																		
DATOS DEL ACTIVO DE INFORMACION			DIMENSION							ATRIBUTOS					UBICACIÓN			
No.	Nombre del activo de información	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes o corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:			Físico	Electrónico
														Leve	Importante	Grave		
1	Base de Datos de Peticiones y Solicitudes	SOFTWARE	A	A	MA	MA	MA	SI	SI	SI	SI	SI	SI			X		X
2	Portal Web de la Personería	SERVICIOS	M	B	B	M	M	SI	NO	NO	SI	NO	SI		X			X
3	Sistema de Información financiero	SOFTWARE	A	MA	MA	MA	A	SI	SI	SI	SI	NO	NO			X		X
4	Sistema de Información Ventanilla Única	SOFTWARE	A	A	MA	MA	A	SI	SI	SI	SI	SI	SI			X		X
5	Servidor Principal	HARDWARE	MA	A	MA	MA	MA	SI	SI	SI	SI	SI	SI			X	X	
6	Servidor físico adicional	HARDWARE	MA	A	MA	MA	A	SI	SI	SI	SI	SI	SI			X	X	
7	Correo Electrónico Institucional	SERVICIOS	B	B	M	M	B	SI	NO	SI	SI	NO	NO	X				X

Tabla 11 (Continuación)*Identificación de Activos*

EMPRESA:			Personería Municipal de Armenia															
INFORMACIÓN DE LOS ACTIVOS																		
DATOS DEL ACTIVO DE INFORMACION			DIMENSION					ATRIBUTOS						UBICACIÓN				
No.	Nombre del activo de información	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes o corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:			Físico	Electrónico
														Leve	Importante	Grave		
8	Backup de Base de Datos	DATOS	M	A	MA	A	MA	SI	SI	SI	SI	SI	SI					X
9	Licencias de Microsoft Office	SOFTWARE	B	MB	MB	B	B	NO	NO	NO	NO	NO	NO	X				X
10	Licencias de Windows	SOFTWARE	M	B	B	M	B	NO	NO	SI	NO	NO	NO	X				X
11	Router principal	COMUNICACIONES	A	M	A	MA	MA	NO	SI	SI	SI	SI	NO			X	X	
12	Switches de red	COMUNICACIONES	M	M	A	A	A	NO	SI	SI	SI	SI	NO		X		X	
13	Access Point	COMUNICACIONES	B	M	M	A	A	SI	SI	SI	SI	SI	NO		X		X	
14	Historias Laborales	DATOS	B	B	B	B	B	SI	SI	SI	NO	NO	NO	X				X
15	Licencia Windows Server	SOFTWARE	M	B	M	B	B	SI	SI	SI	SI	SI	NO	X				X
16	Oficinas	INSTALACIONES	B	B	B	B	B	NO	NO	NO	NO	NO	NO	X			X	
17	Técnico TIC	PERSONAL	A	A	MA	MA	MA	SI	NO	NO	SI	SI	SI		X		X	

EMPRESA: Personería Municipal de Armenia																		
INFORMACIÓN DE LOS ACTIVOS																		
DATOS DEL ACTIVO DE INFORMACION			DIMENSION					ATRIBUTOS							UBICACIÓN			
No.	Nombre del activo de información	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes o corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:			Físico	Electrónico
														Leve	Importante	Grave		
28	Planes, programas y proyectos institucionales	DATOS	B	B	B	B	B	NO	NO	NO	NO	NO	NO	X			X	
29	Conciliaciones	DATOS	A	M	A	A	A	NO	SI	SI	SI	SI	SI			X	X	
30	Equipo Personera	HARDWARE	M	M	A	A	A	NO	SI	SI	SI	SI	SI			X	X	
31	Equipo Personeros delegados	HARDWARE	M	M	A	A	A	NO	SI	SI	SI	SI	SI		X		X	
32	Equipos jefes Administrativos y/Financieros	HARDWARE	M	M	A	A	A	NO	SI	SI	SI	SI	NO		X		X	
33	Equipo Soporte TIC	HARDWARE	M	M	A	A	A	NO	SI	SI	SI	SI	NO		X		X	
34	Equipos funcionarios	HARDWARE	M	M	M	M	M	NO	SI	SI	SI	SI	NO		X		X	
35	Equipos Contratistas	HARDWARE	B	B	M	M	B	SI	SI	SI	SI	NO	NO	X			X	

EMPRESA: Personería Municipal de Armenia																		
INFORMACIÓN DE LOS ACTIVOS																		
DATOS DEL ACTIVO DE INFORMACION			DIMENSION					ATRIBUTOS						UBICACIÓN				
No.	Nombre del activo de información	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes o corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:			Físico	Electrónico
														Leve	Importante	Grave		
36	Internet	SERVICIOS	M	M	M	A	M	NO	NO	SI	NO	NO	NO		X			X
37	Rack	SOPORTE	B	B	B	B	B	NO	SI	SI	NO	SI	NO	X			X	
38	Disco duro externo	SOPORTE	B	B	M	B	M	NO	SI	SI	SI	NO	NO	X			X	
39	UPS	AUXILIAR	B	MB	MB	B	B	NO	NO	NO	NO	NO	NO	X			X	
40	Impresoras	HARDWARE	MB	MB	B	B	MB	NO	NO	SI	NO	NO	NO	X			X	

Nota. Identificación de activos (Autoría Propia)

A continuación, se presentan los activos identificados, resaltando su importancia y el impacto que tendrían en caso de ser afectados.

Tabla 12

Clasificación General y Números de Activos

Clasificación general y Número de activos	
Tipo de activo	Cantidad
Tipo Dato	9
Tipo Claves Criptográficas	0
Tipo Servicio	3
Tipo Software	6
Tipo Hardware	9
Tipo Comunicaciones	3
Tipo Soporte de Información	2
Tipo Equipamiento Auxiliar	1
Tipo Instalaciones	1
Tipo Personal	6
Total, de Activos	40

Nota. Clasificación general y Números de activos (Autoría Propia)

Tabla 13

Ubicación de los Activos de Información

Ubicación	
Física	29
Electrónica	11

Nota. Ubicación de los activos de información (Autoría Propia)

Tabla 14*Clasificación de Activos Según su Valor*

Clasificación de activos según su valor	
Número de activos de clientes o terceros que deben protegerse.	19
Activos de información que deben ser restringidos a un número limitado de empleados	26
Número de activos de información que deben ser restringidos a personas externas.	28
Activos de información que pueden ser alterados o comprometidos para fraudes o corrupción.	28
Número de activos de información que son muy críticos para las operaciones internas.	20
Número de activos de información que son muy críticos para el servicio hacia terceros	14

Nota. Clasificación de activos según su valor (Autoría Propia)

Tabla 15*Resumen de Nivel de Riesgos*

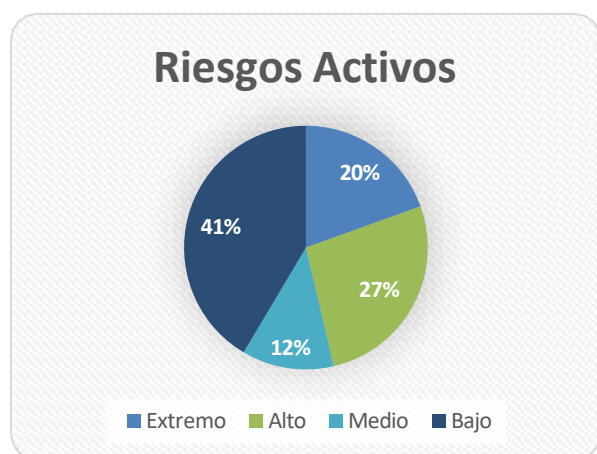
Resumen de nivel de riesgo en los activos	
Extremo	8
Alto	10
Medio	5
Bajo	17

Nota. Resumen de nivel de riesgo (Autoría Propia)

Tabla 16*Clasificación Según Impacto a la Seguridad*

Clasificación según impacto a la seguridad	
Leve	16
Importante	16
Grave	8

Nota. Clasificación según impacto a la seguridad (Autoría Propia)

Figura 12*Identificación de Activos*

Nota. Identificación de Activos (Autoría Propia)

La valoración de los activos de información en la escala C.C Eficiente permite identificar su nivel de criticidad y su impacto en la operación de la entidad. Este proceso facilita la toma de decisiones en materia de seguridad, garantizando la protección, disponibilidad y correcta gestión de los activos. A continuación, se presenta un resumen de la evaluación realizada, destacando los criterios aplicados y los resultados obtenidos.

Tabla 17*Valoración Cualitativa de los Activos*

Nombre	Riesgo	Confidencialidad	Integridad	Disponibilidad	Valor
Base de Datos de Peticiones y Solicitudes	EXTREMO	9	9	9	9
Portal Web de la Personería	BAJO	3	5	5	4
Sistema de Información financiero	EXTREMO	9	9	6	8
Sistema de Información Ventanilla Única	EXTREMO	9	9	6	8
Servidor Principal	EXTREMO	9	9	9	9
Servidor físico adicional	EXTREMO	9	9	6	8
Correo Electrónico Institucional	BAJO	5	5	3	4
Backup de Base de Datos	EXTREMO	9	6	9	8
Licencias de Microsoft Office	BAJO	3	3	3	3
Licencias de Windows	BAJO	3	3	3	3
Router principal	EXTREMO	6	9	9	8
Switches de red	ALTO	6	6	6	6
Access Point	ALTO	5	6	6	6
Historias Laborales	BAJO	3	3	3	3
Licencia Windows Server	BAJO	5	3	3	4
Oficinas	BAJO	3	3	3	3
Técnico TIC	EXTREMO	9	9	9	9
Personera	ALTO	6	6	5	6
Personeros delegados	ALTO	6	6	5	6
Directores Administrativos	ALTO	6	6	5	6
Funcionarios	MEDIO	5	6	5	5
Contratistas	MEDIO	5	6	5	5
Actas de comité	BAJO	3	3	3	3
Actos administrativos	BAJO	5	3	5	4
Comunicaciones Oficiales	BAJO	3	3	3	3
Contratos estatales	MEDIO	5	6	5	5
Informes Institucionales	BAJO	3	3	3	3
Planes, programas y proyectos institucionales	BAJO	3	3	3	3
Conciliaciones	ALTO	6	6	6	6
Equipo Personera	ALTO	6	6	6	6
Equipo Personeros delegados	ALTO	6	6	6	6

Tabla 17 (Continuación)*Valoración Cualitativa de los Activos*

Nombre	Riesgo	Confidencialidad	Integridad	Disponibilidad	Valor
Equipos jefes Administrativos y/o Financieros	ALTO	6	6	6	6
Equipos Soporte TIC	ALTO	6	6	6	6
Equipos funcionarios	MEDIO	5	5	5	5
Equipos Contratistas	BAJO	5	5	3	4
Internet	MEDIO	5	6	5	5
Rack	BAJO	3	3	3	3
Disco duro externo	BAJO	3	3	5	4
UPS	BAJO	3	3	3	3
Impresoras	BAJO	3	3	3	3

Nota. Valoración cualitativa de los activos (Autoría Propia)

Valoración Cuantitativa de los Activos

La valoración cuantitativa de los activos consiste en asignar un valor numérico que representa la importancia y el impacto de cada activo, de acuerdo con la evaluación cualitativa realizada previamente. Este proceso permite medir de manera más precisa los niveles de riesgo y priorizar la implementación de controles de seguridad. Para ello, se utilizó un cuadro adaptado de la tabla de MAGERIT, el cual establece una correspondencia entre las categorías cualitativas y su respectivo valor numérico, facilitando un análisis más estructurado y detallado.

Tabla 18*Valoración Cuantitativa de los Activos*

NOMBRE	RIESGO	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
Base de Datos de Peticiones y Solicitudes	CRITICO	20	20	25	25	25	23
Portal Web de la Personería	APRECIABLE	15	9	9	15	15	13
Sistema de Información financiero	CRITICO	20	25	25	25	20	23
Sistema de Información Ventanilla Única	CRITICO	20	20	25	25	20	22
Servidor Principal	CRITICO	25	20	25	25	25	24
Servidor físico adicional	CRITICO	25	20	25	25	20	23
Correo Electrónico Institucional	APRECIABLE	9	9	15	15	9	11
Backup de Base de Datos	CRITICO	15	20	25	20	25	21
Licencias de Microsoft Office	BAJO	9	4	4	9	9	7
Licencias de Windows	APRECIABLE	15	9	9	9	9	10
Router principal	CRITICO	20	15	20	25	25	21
Switches de red	IMPORTANTE	15	15	20	20	20	18
Access Point	IMPORTANTE	9	15	15	20	20	16
Historias Laborales	BAJO	9	9	9	9	9	9
Licencia Windows Server	APRECIABLE	15	9	15	9	9	11
Oficinas	BAJO	9	9	9	9	9	9
Técnico TIC	CRITICO	20	20	25	25	25	23
Personera	IMPORTANTE	15	9	20	20	15	16
Personeros delegados	IMPORTANTE	15	9	20	20	15	16
Directores Administrativos	IMPORTANTE	15	15	20	20	15	17
Funcionarios	APRECIABLE	9	15	15	20	15	15
Contratistas	APRECIABLE	9	9	15	20	15	14
Actas de comité	BAJO	9	9	9	9	9	9

Tabla 18*Valoración Cuantitativa de los Activos*

NOMBRE	RIESGO	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
Actos administrativos	APRECIABLE	9	9	15	9	15	11
Comunicaciones Oficiales	BAJO	9	9	9	9	9	9
Contratos estatales	APRECIABLE	9	9	15	20	15	14
Informes Institucionales	BAJO	9	9	9	9	9	9
Planes, programas y proyectos institucionales	BAJO	9	9	9	9	9	9
Conciliaciones	IMPORTANTE	20	15	20	20	20	19
Equipo Personera	IMPORTANTE	15	15	20	20	20	18
Equipo Personeros delegados	IMPORTANTE	15	15	20	20	20	18
Equipos jefes Administrativos y/o Financieros	IMPORTANTE	15	15	20	20	20	18
Equipos Soporte TIC	IMPORTANTE	15	15	20	20	20	18
Equipos funcionarios	APRECIABLE	15	15	15	15	15	15
Equipos Contratistas	APRECIABLE	9	9	15	15	9	11
Internet	IMPORTANTE	15	15	15	20	15	16
Rack	BAJO	9	9	9	9	9	9
Disco duro externo	APRECIABLE	9	9	9	9	15	10
UPS	BAJO	9	4	4	9	9	7
Impresoras	BAJO	4	4	9	9	4	6

Nota. Valoración cuantitativa de los activos (Autoría Propia)

Teniendo en cuenta lo anterior, se realiza la validación los activos cuyo valor resulta medio, alto y extremo, en entrevista con el contratista del área de tecnología, serán los prioritarios y recibirán los recursos necesarios a corto y mediano plazo. Se considera aceptable el riesgo en aquellos con calificación bajo o muy bajo.

La información es clave en cada proceso, ya que incluye datos de la entidad, usuarios y proveedores. En ella se encuentran datos sensibles como información personal, financiera y detalles de seguridad para acceder a herramientas corporativas y procesar información.

Uno de los activos más importantes es el personal clave, ya que tiene acceso a información restringida de la empresa. Por ello, se han establecido cláusulas especiales de confidencialidad con respaldo legal y económico en caso de incumplimiento.

La Ventanilla Única, es un activo extremo para la operación, toda vez que almacena todo el sistema de información sobre trámites relacionados con la difusión y promoción de los derechos humanos; la defensa y protección de los derechos humanos, el orden jurídico y el interés general y la vigilancia efectiva de la gestión administrativa y defensa del patrimonio público. El personal que lo maneja es clave para el proceso y requiere un alto nivel de control y monitoreo.

Así mismo, el Servidor Principal y el Servidor Físico Adicional son activos muy importantes porque son esenciales para el funcionamiento de los sistemas de la organización. Desde un punto de vista económico, estos servidores representan una gran inversión en equipos, programas y mantenimiento. Si dejan de funcionar, pueden generar altos costos de reparación, pérdida de datos y problemas en las operaciones diarias. Además, almacenan información clave y aplicaciones necesarias para el trabajo diario, por lo que su falla afectaría la productividad y la seguridad de la información. Si estos servidores no están disponibles, la organización podría

enfrentar dificultades para prestar servicios, pérdida de confianza y problemas legales. Por estas razones, su protección es una prioridad.

Se puede señalar, que el Router Principal es un activo muy importante porque controla y gestiona la conexión a la red de la entidad. es clave para la seguridad y estabilidad de la red, toda vez que, un mal uso o un ataque pueden permitir accesos no autorizados, robo de información o fallas en la conexión.

Se utilizan activos clave para la operación y seguridad de la información, como el switch, el router. Estos permiten controlar el acceso del personal a los sistemas de la empresa, aplicar controles y establecer restricciones definidas por el equipo de tecnología y aprobadas por la Personería Municipal.

Por último, se clasificó la disponibilidad e integridad como altas y la confidencialidad como restringida, ya que cada activo es clave para los procesos críticos de la empresa. Esto ayuda a que el personal tome conciencia sobre su importancia y la necesidad de protegerlos adecuadamente.

Amenazas y Vulnerabilidades

En la Personería Municipal de Armenia, las amenazas y vulnerabilidades pueden afectar la seguridad de los activos de información esenciales para el cumplimiento de sus funciones. Las amenazas incluyen riesgos como accesos no autorizados, pérdida de datos o ataques cibernéticos, mientras que las vulnerabilidades corresponden a debilidades en los sistemas, procesos o manejo de la información. Identificar estos factores es clave para proteger la integridad, disponibilidad y confidencialidad de la información, garantizando así una gestión eficiente y segura.

Tabla 19*Identificación de Amenazas y Vulnerabilidades*

NO. DE AMENAZAS Y VULNERABILIDADES	ACTIVOS DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACIÓN	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	AMENAZAS METODOLOGÍA MAGERIT	VULNERABILIDADES	RIESGO
1	SOFTWARE	Base de Datos de Peticiones y Solicitudes	23	[E20] Vulnerabilidades de los programas (software)	Inyección SQL	Carece de mecanismos efectivos y adecuados para validar y filtrar las entradas de datos.
2	SOFTWARE	Base de Datos de Peticiones y Solicitudes	23	[E2] Errores del administrador	Configuraciones Incorrectas de Seguridad	Configuración incorrecta de seguridad en la Base de Datos de peticiones y solicitudes generando fallos en los controles de acceso.
3	SOFTWARE	Base de Datos de Peticiones y Solicitudes	23	[E8] Difusión de software dañino	Exposición a Aplicaciones Web Vulnerables	Acceso no autorizado, modificación indebida o eliminación de información debido a la exposición a aplicaciones web.
4	SERVICIOS	Portal Web de la Personería	13	[E15] Alteración accidental de la información	Modificación malintencionada del portal web	Alteración malintencionada del Portal Web que compromete la integridad, disponibilidad y confiabilidad de la información institucional
5	SERVICIOS	Portal Web de la Personería	13	[A24] Denegación de servicio	Configuración de Seguridad Incorrecta	Exposición a ciberataques y accesos no autorizados debido a configuraciones de seguridad incorrectas en el Portal Web.
6	SOFTWARE	Sistema de Información financiero	23	[E10] Errores de secuencia	Falta de copias de seguridad (backup)	pérdida irreversible de datos financieros y afectación a la continuidad operativa.
7	SOFTWARE	Sistema de Información financiero	23	[A6] Abuso de privilegios de acceso	Privilegios de cuenta de administrador o superusuario	Acceso no autorizado, modificaciones indebidas de datos, eliminación de registros o instalación de software malicioso.
8	SOFTWARE	Sistema de Información financiero	23	[E21] Errores de mantenimiento / actualización de programas (software)	Software desactualizado	Falta de actualizaciones puede provocar fallos operativos, incompatibilidad con nuevos sistemas y pérdida de soporte técnico

NO. DE AMENAZAS Y VULNERABILIDADES	ACTIVOS DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACIÓN	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	AMENAZAS METODOLOGÍA MAGERIT	VULNERABILIDADES	RIESGO
9	SOFTWARE	Sistema de Información Ventanilla Única	22	[A5] Suplantación de la identidad del usuario	Programas ocultos de puerta trasera (Backdoor)	Manipulación, robo o eliminación de solicitudes, suplantación de identidad, filtración de datos sensibles.
10	SOFTWARE	Sistema de Información Ventanilla Única	22	[E1] Errores de los usuarios	Falta de autenticación multifactor (MFA)	Suplantación de identidad de usuarios, alteración o acceso indebido a información confidencial.
11	SOFTWARE	Sistema de Información Ventanilla Única	22	[A22] Manipulación de programas	Credenciales débiles o comprometidas	Acceso no autorizado y modificación indebida de registros.
12	HARDWARE	Servidor Principal	24	[E24] Caída del sistema por agotamiento de recursos	Sobrecarga de solicitudes o ataques de denegación de servicio	Indisponibilidad total del servidor, afectando los servicios y sistemas críticos.
13	HARDWARE	Servidor Principal	24	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Mala gestión de recursos del sistema	Degradación del rendimiento y posible falla total del servidor.
14	HARDWARE	Servidor Principal	24	[I5] Avería de origen físico o lógico	Insuficiente capacidad de hardware	Saturación del servidor e interrupción de servicios críticos.
15	HARDWARE	Servidor físico adicional	23	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de mantenimiento preventivo	Deterioro del hardware y falla inesperada del servidor.
16	HARDWARE	Servidor físico adicional	23	[E24] Caída del sistema por agotamiento de recursos	Fallas en la gestión del almacenamiento	Pérdida de datos o inaccesibilidad a la información almacenada.

NO. DE AMENAZAS Y VULNERABILIDADES	ACTIVOS DE INFORMACION		VALORACIÓN DEL RIESGO DE LOS ACTIVOS	AMENAZAS METODOLOGÍA MAGERIT		VULNERABILIDADES	RIESGO
		NOMBRE DEL ACTIVO DE INFORMACIÓN					
17	HARDWARE	Servidor físico adicional	23	[I7] Condiciones inadecuadas de temperatura o humedad		Desgaste de componentes físicos	Falla del servidor debido a la degradación de sus componentes físicos.
18	SERVICIOS	Correo Electrónico Institucional	11	[A6] Abuso de privilegios de acceso		Falta de control en los accesos y permisos	Acceso no autorizado a cuentas de correo electrónico institucional y exfiltración de información sensible
19	SERVICIOS	Correo Electrónico Institucional	11	[A7] Uso no previsto		Envío de información sensible a destinatarios no autorizados	Divulgación accidental de información confidencial a personas no autorizadas.
20	DATOS	Backup de Base de Datos	21	[E3] Errores de monitorización (log)		Falta de registros detallados en los logs de respaldo	Imposibilidad de rastrear o verificar el proceso de respaldo y recuperación de la base de datos.
21	DATOS	Backup de Base de Datos	21	[A4] Manipulación de la configuración		No detección de fallos en la ejecución del backup	Pérdida de datos importantes debido a la falta de verificación del proceso de respaldo.
22	DATOS	Backup de Base de Datos	21	[E2] Errores del administrador		No realizar auditorías periódicas a los registros de backup	Dificultad para detectar problemas en los backups, lo que podría resultar en la pérdida de datos importantes.
23	SOFTWARE	Licencias de Microsoft Office	7	[I5] Avería de origen físico o lógico		Uso de licencias no compatibles con la infraestructura TI	Disminución de la eficiencia operativa y vulnerabilidades de seguridad debido a la incompatibilidad de licencias.
24	SOFTWARE	Licencias de Microsoft Office	7	[E2] Errores del administrador		Fallo en los servidores de validación de Microsoft	Pérdida de acceso a las aplicaciones de Microsoft Office y afectación de la productividad de la organización

NO. DE AMENAZAS Y VULNERABILIDADES	ACTIVOS DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACIÓN	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	AMENAZAS METODOLOGÍA MAGERIT	VULNERABILIDADES	RIESGO
25	SOFTWARE	Licencias de Windows	10	[E20] Vulnerabilidades de los programas (software)	Fallas de seguridad en el sistema operativo	Compromiso de la seguridad de los sistemas TI debido a vulnerabilidades en el sistema operativo relacionadas con las licencias.
26	SOFTWARE	Licencias de Windows	10	[E21] Errores de mantenimiento / actualización de programas (software)	Uso de versiones obsoletas o sin soporte	Exposición a riesgos de seguridad y problemas operativos debido al uso de versiones no actualizadas o sin soporte.
27	COMUNICACIONES	Router principal	21	[A6] Abuso de privilegios de acceso	Acceso sin restricciones a la configuración del router	Alteración no autorizada de la configuración del router, afectando la seguridad y estabilidad de la red
28	COMUNICACIONES	Router principal	21	[A6] Abuso de privilegios de acceso	Configuración incorrecta de privilegios de usuario	Compromiso de la Seguridad y Estabilidad de la Red por Configuración Incorrecta de Privilegios de Usuario en el Router Principal
29	COMUNICACIONES	Router principal	21	[E10] Errores de secuencia	Modificación de reglas de tráfico y filtrado de contenido	Acceso indebido a la red, pérdida de control sobre el tráfico y exposición a amenazas cibernéticas
30	COMUNICACIONES	Switches de red	18	[E9] Errores de [re-]encaminamiento	Configuración incorrecta de VLANs	Pérdida de segmentación de la red, acceso no autorizado a datos y degradación del rendimiento de la red
31	COMUNICACIONES	Switches de red	18	[A10] Alteración de secuencia	Exposición a ataques de suplantación de direcciones MAC	Acceso no autorizado a la red, interceptación de tráfico y ataques de denegación de servicio.

NO. DE AMENAZAS Y VULNERABILIDADES	ACTIVOS DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACIÓN	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	AMENAZAS METODOLOGÍA MAGERIT	VULNERABILIDADES	RIESGO
32	COMUNICACIONES	Switches de red	18	[A15] Modificación deliberada de la información	Problemas en la asignación de direcciones IP o enrutamiento estático/dinámico	Fallos en la comunicación entre dispositivos, interrupción de servicios críticos y degradación del rendimiento de la red
33	COMUNICACIONES	Access Point	16	[A12] Análisis de tráfico	No uso de cifrado en la red inalámbrica o en el tráfico interno	Intercepción de datos, accesos no autorizados y compromiso de la confidencialidad de la información.
34	COMUNICACIONES	Access Point	16	[I8] Fallo de servicios de comunicaciones	Uso de protocolos de cifrado débiles o mal configurados	Acceso no autorizado, intercepción de datos y ataques de suplantación dentro de la red inalámbrica
35	DATOS	Historias Laborales	9	[A19] Divulgación de información	Falta de políticas de seguridad en el acceso a documentos	Divulgación no autorizada, manipulación indebida o pérdida de información sensible de empleados
36	SOFTWARE	Licencia Windows Server	11	[E21] Errores de mantenimiento / actualización de programas (software)	Incompatibilidad con otros programas o servicios	Fallos en la interoperabilidad, errores en sistemas críticos y pérdida de funcionalidad en servicios esenciales.
37	INSTALACIONES	Oficinas	9	[A11] Acceso no autorizado	Falta de controles de acceso físicos	Robo de información, manipulación de activos y acceso no autorizado a documentos sensibles.
38	PERSONAL	Técnico TIC	23	[E28] Indisponibilidad del personal	Dependencia excesiva de un solo empleado	Interrupción de Servicios y Pérdida de Conocimiento Crítico por Dependencia Excesiva de un Solo Empleado

NO. DE AMENAZAS Y VULNERABILIDADES	ACTIVOS DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACIÓN	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	AMENAZAS METODOLOGÍA MAGERIT	VULNERABILIDADES	RIESGO
39	PERSONAL	Personera	16	[A29] Extorsión	Ataques a través de medios digitales	Suplantación de Identidad y Exposición a Fraudes por Ataques a través de Medios Digitales
40	PERSONAL	Personera	16	[E19] Fugas de información	Acceso a información confidencial	Exposición, filtración o uso indebido de información sensible e impacto en la toma de decisiones
41	PERSONAL	Personeros delegados	16	[A30] Ingeniería social	Uso de dispositivos electrónicos personales para trabajo	Exposición a ciberataques, fuga de información y pérdida de control sobre datos sensibles
42	PERSONAL	Directores Administrativos	17	[E19] Fugas de información	Almacenamiento de información en dispositivos no protegidos	Exposición a Pérdida o Filtración de Información Sensible por Almacenamiento en Dispositivos No Protegidos
43	PERSONAL	Directores Administrativos	17	[E7] Deficiencias en la organización	Correos de phishing	Robo de credenciales, acceso no autorizado a sistemas y filtración de información sensible
44	PERSONAL	Funcionarios	15	[A30] Ingeniería social	Caer en correos fraudulentos o llamadas engañosas	Robo de credenciales, acceso no autorizado a sistemas y filtración de información sensible.
45	PERSONAL	Contratistas	14	[A28] Indisponibilidad del personal	Falta de planes de contingencia ante la ausencia de contratistas clave	Interrupción de la operación, pérdida de conocimiento crítico y retrasos en proyectos o servicios.
46	DATOS	Actas de comité	9	[A19] Divulgación de información	Almacenamiento sin controles de acceso adecuados	Exposición, modificación o eliminación no autorizada de información confidencial.

NO. DE AMENAZAS Y VULNERABILIDADES	ACTIVOS DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACIÓN	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	AMENAZAS METODOLOGÍA MAGERIT	VULNERABILIDADES	RIESGO
47	DATOS	Actos administrativos	11	[A11] Acceso no autorizado	Falta de controles de acceso adecuados	Acceso no autorizado, modificación o eliminación de actos administrativos críticos
48	DATOS	Comunicaciones Oficiales	9	[A15] Modificación deliberada de la información	Falta de trazabilidad en las modificaciones	Modificación no autorizada o eliminación de contenido sin registro ni control.
49	DATOS	Contratos estatales	14	[E19] Fugas de información	Falta de auditoría en el acceso a los documentos	Acceso, modificación o uso indebido de contratos sin registro ni supervisión.
50	DATOS	Informes Institucionales	9	[A18] Destrucción de información	Falta de políticas de recuperación de desastres	Pérdida o Inaccesibilidad de Informes Institucionales debido a la Falta de Políticas de Recuperación de Desastres
51	DATOS	Planes, programas y proyectos institucionales	9	[A15] Modificación deliberada de la información	Uso de formatos editables sin restricciones	Alteración no autorizada o pérdida de integridad de la información institucional
52	DATOS	Conciliaciones	19	[E15] Alteración accidental de la información	Uso de archivos no protegidos contra modificaciones accidentales	Pérdida de integridad y confiabilidad en la información de conciliaciones.
53	HARDWARE	Equipo Personera	18	[A26] Ataque destructivo	Protección inadecuada contra malware o ataques cibernéticos destructivos	Compromiso de la información institucional y paralización de las actividades de la Personera.
54	HARDWARE	Equipo Personeros delegados	18	[A23] Manipulación de los equipos	Modificación o eliminación de archivos sensibles	Compromiso de la integridad de la información y desorganización en la gestión de la institución.

NO. DE AMENAZAS Y VULNERABILIDADES	ACTIVOS DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACIÓN	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	AMENAZAS METODOLOGÍA MAGERIT	VULNERABILIDADES	RIESGO
55	HARDWARE	Equipos jefes Administrativos y/o Financieros	18	[A7] Uso no previsto	Uso de dispositivos USB o externos sin control	Exposición de la información sensible a amenazas de seguridad, como malware o pérdida de datos.
56	HARDWARE	Equipos Soporte TIC	18	[E2] Errores del administrador	Manejo incorrecto de permisos de acceso	Exposición, alteración o pérdida de datos críticos debido a permisos de acceso mal gestionados.
57	HARDWARE	Equipos Soporte TIC	18	[A26] Ataque destructivo	Respaldo insuficiente de configuraciones	Pérdida o corrupción de configuraciones críticas, lo que podría afectar la operatividad de los sistemas y procesos tecnológicos
58	HARDWARE	Equipos funcionarios	15	[A25] Robo	Falta de cifrado en los datos almacenados	Exposición, acceso no autorizado o robo de datos sensibles almacenados en los equipos de los funcionarios.
59	SERVICIOS	Equipos Contratistas	11	[A6] Abuso de privilegios de acceso	Uso compartido de credenciales o dispositivos	Acceso no autorizado, filtración o manipulación de información sensible almacenada en los equipos de los contratistas
60	SOPORTE	Internet	16	[A24] Denegación de servicio	Configuraciones de red inseguras	Exposición a ataques cibernéticos, acceso no autorizado o compromisos de seguridad debido a configuraciones inadecuadas en la infraestructura de red conectada a Internet
61	SOPORTE	Internet	16	[A7] Uso no previsto	Ancho de banda insuficiente para resistir ataques volumétricos	Interrupción del servicio y pérdida de disponibilidad debido a ataques de denegación de servicio distribuido

NO. DE AMENAZAS Y VULNERABILIDADES	ACTIVOS DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACIÓN	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	AMENAZAS METODOLOGÍA MAGERIT	VULNERABILIDADES	RIESGO
62	AUXILIAR	Rack	9	[I6] Corte del suministro eléctrico	Interrupción del funcionamiento de los equipos alojados	Pérdida de disponibilidad de servicios y datos debido a fallas en el sistema de alojamiento del rack
63	HARDWARE	Disco duro externo	10	[I10] Degradación de los soportes de almacenamiento de la información	Sobreescritura continua y uso intensivo	Pérdida o corrupción de datos almacenados debido al uso excesivo del disco duro externo.
64	HARDWARE	UPS	7	[I7] Condiciones inadecuadas de temperatura o humedad	Sobrecalentamiento de la UPS	Daño a la UPS y Pérdida de Energía de Respaldo por Sobrecalentamiento.
65	HARDWARE	Impresoras	6	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Obstrucción de los inyectores o rodillos de alimentación	Interrupción de la Producción de Documentos y Daño a las Impresoras por Obstrucción de Inyectores o Rodillos de Alimentación

Nota. Identificación de Amenazas y Vulnerabilidades (Autoría Propia)

En la Personería Municipal de Armenia, varios activos de información presentan vulnerabilidades significativas que pueden comprometer la seguridad, integridad y disponibilidad de los datos. A continuación, se describen los activos más críticos y las principales debilidades que enfrentan.

El sistema de peticiones, que gestiona solicitudes institucionales, es vulnerable a ataques como la inyección SQL, que podría permitir la manipulación de datos sensibles. Además, las configuraciones incorrectas de seguridad pueden facilitar accesos no autorizados, y la exposición a aplicaciones web vulnerables aumenta el riesgo de explotación por parte de atacantes.

Por su parte, el sistema de información financiero enfrenta riesgos asociados a la falta de copias de seguridad, lo que podría comprometer la recuperación de datos en caso de fallos. Además, el uso de privilegios excesivos en cuentas de administrador o superusuario puede generar accesos indebidos y modificaciones no autorizadas. A esto se suma el riesgo de software desactualizado, que expone al sistema a vulnerabilidades conocidas. El sistema de información Ventanilla Única, encargado de gestionar trámites y documentos, presenta riesgos como la presencia de programas ocultos de puerta trasera (Backdoor), que podrían permitir accesos remotos no autorizados. Asimismo, la falta de autenticación multifactor (MFA) deja el sistema expuesto a ataques de robo de credenciales, y el uso de credenciales débiles o comprometidas facilita accesos indebidos. Además, el servidor principal, al ser el núcleo de la infraestructura informática, enfrenta amenazas como la sobrecarga de solicitudes o ataques de denegación de servicio (DoS), los cuales pueden afectar la disponibilidad de los servicios. Además, la mala gestión de recursos del sistema podría degradar el rendimiento y generar fallos operativos, mientras que la insuficiente capacidad de hardware puede ocasionar interrupciones en el procesamiento de información.

La copia de seguridad de la base de datos, esencial para la recuperación de información en caso de incidentes, puede verse comprometido por la falta de registros detallados en los logs de respaldo, lo que dificulta el rastreo de fallos o accesos no autorizados. También, la no detección de fallos en la ejecución del backup podría resultar en copias de seguridad inservibles, y la ausencia de auditorías periódicas impide la identificación temprana de errores en los respaldos. Así mismo, el router principal, responsable de la conectividad de la entidad, presenta riesgos como el acceso sin restricciones a su configuración, lo que podría permitir modificaciones no autorizadas que afecten la seguridad de la red. También, una configuración incorrecta de privilegios de usuario podría otorgar permisos indebidos, y la modificación de reglas de tráfico y filtrado de contenido sin controles adecuados podría exponer la red a amenazas externas.

Finalmente, el recurso humano también representa un factor de riesgo. En particular, la dependencia excesiva del Técnico TIC es una vulnerabilidad significativa, ya que la falta de distribución del conocimiento y las responsabilidades podría afectar la continuidad de las operaciones en caso de ausencia de este contratista.

En la tabla 20 se evalúa la gestión de los controles existentes para mitigar los posibles riesgos asociados a las vulnerabilidades en los activos de información. La calificación de los controles se establece de la siguiente manera: 1 (control inexistente), 2 (existe, pero no es efectivo), 3 (efectivo, pero no documentado) y 4 (efectivo y documentado). Asimismo, se califica la probabilidad de vulneración, asignando valores de 1 (muy raro), 2 (poco probable), 3 (posible), 4 (probable) y 5 (prácticamente seguro). En los casos en que el control se calificó con 2, 3 o 4, se especificó el control aplicado.

Tabla 20

Matriz de APT

Nombre del activo de información	Valoración del riesgo de los activos	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
Base de Datos de Peticiones y Solicitudes	23	[E20] Vulnerabilidades de los programas (software)	Inyección SQL	I	4	92	C	1		92	C
Base de Datos de Peticiones y Solicitudes	23	[E2] Errores del administrador	Configuraciones Incorrectas de Seguridad	I	4	92	C	2	Uso de contraseñas robustas y autenticación segura para acceder a la base de datos	46	C
Base de Datos de Peticiones y Solicitudes	23	[E8] Difusión de software dañino	Exposición a Aplicaciones Web Vulnerables	I	5	115	C	2	Restricción de permisos innecesarios y desactivación de servicios no esenciales	58	C
Portal Web de la Personería	13	[E15] Alteración accidental de la información	Modificación malintencionada del portal web	I	4	52	C	3	Asignación de permisos mínimos a los usuarios administrativos para evitar modificaciones no autorizadas.	17	I
Portal Web de la Personería	13	[A24] Denegación de servicio	Configuración de Seguridad Incorrecta	M	3	39	I	4	El Ministerio TIC, como administrador del portal web del Estado, implementa medidas de seguridad esenciales para mitigar la vulnerabilidad	10	B
Sistema de Información financiero	23	[E10] Errores de secuencia	Falta de copias de seguridad (backup)	I	2	46	C	3	Se establecen backups manuales con una frecuencia diaria por la criticidad de la información.	15	A

Nombre del activo de información	Valoración del riesgo de los activos	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
Sistema de Información financiero	23	[A6] Abuso de privilegios de acceso	Privilegios de cuenta de administrador o superusuario	I	4	92	C	1		92	C
Sistema de Información financiero	23	[E21] Errores de mantenimiento / actualización de programas (software)	Software desactualizado	I	2	46	C	3	El proveedor del sistema realiza actualizaciones periódicas para corregir vulnerabilidades y mejorar el rendimiento del software.	15	A
Sistema de Información Ventanilla Única	22	[A5] Suplantación de la identidad del usuario	Programas ocultos de puerta trasera (Backdoor)	I	3	66	C	1		66	C
Sistema de Información Ventanilla Única	22	[E1] Errores de los usuarios	Falta de autenticación multifactor (MFA)	I	3	66	C	3	Se configura la autenticación multifactor como requisito obligatorio para todos los usuarios con acceso al sistema.	22	C
Sistema de Información Ventanilla Única	22	[A22] Manipulación de programas	Credenciales débiles o comprometidas	I	3	66	C	4	Se establece un periodo de expiración de contraseñas y la obligación de cambiarlas periódicamente.	17	I
Servidor Principal	24	[E24] Caída del sistema por agotamiento de recursos	Sobrecarga de solicitudes o ataques de denegación de servicio	I	5	120	C	1		120	C

Nombre del activo de información	Valoración del riesgo de los activos	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
Servidor Principal	24	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Mala gestión de recursos del sistema	I	4	96	C	1	Se establece un calendario de mantenimiento preventivo del hardware y software del servidor.	96	C
Servidor Principal	24	[I5] Avería de origen físico o lógico	Insuficiente capacidad de hardware	I	3	72	C	1		72	C
Servidor físico adicional	23	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de mantenimiento preventivo	I	2	46	C	2		23	C
Servidor físico adicional	23	[E24] Caída del sistema por agotamiento de recursos	Fallas en la gestión del almacenamiento	I	4	92	C	1		92	C
Servidor físico adicional	23	[I7] Condiciones inadecuadas de temperatura o humedad	Desgaste de componentes físicos	I	3	69	C	1		69	C
Correo Electrónico Institucional	11	[A6] Abuso de privilegios de acceso	Falta de control en los accesos y permisos	I	4	44	I	3	Se configura el correo para permitir el acceso únicamente a cuentas institucionales asignadas a funcionarios de planta activos.	15	A

Nombre del activo de información	Valoración del riesgo de los activos	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
Correo Electrónico Institucional	11	[A7] Uso no previsto	Envío de información sensible a destinatarios no autorizados	I	4	44	I	3	Se envían recordatorios sobre la importancia de verificar los destinatarios antes de enviar información sensible.	15	A
Backup de Base de Datos	21	[E3] Errores de monitorización (log)	Falta de registros detallados en los logs de respaldo	I	3	63	C	1		63	C
Backup de Base de Datos	21	[A4] Manipulación de la configuración	No detección de fallos en la ejecución del backup	I	4	84	C	2	Se establece una estrategia de almacenamiento en ubicaciones local y almacenamiento externo para mayor seguridad.	42	C
Backup de Base de Datos	21	[E2] Errores del administrador	No realizar auditorías periódicas a los registros de backup	I	3	63	C	1		63	C
Licencias de Microsoft Office	7	[I5] Avería de origen físico o lógico	Uso de licencias no compatibles con la infraestructura TI	M	2	14	A	3	Se adquieren únicamente licencias legítimas y compatibles con los sistemas operativos y hardware disponibles.	5	B
Licencias de Microsoft Office	7	[E2] Errores del administrador	Fallo en los servidores de validación de Microsoft	A	1	7	B	3	Se almacena de forma segura la información de claves de producto y configuraciones de activación para facilitar la recuperación ante fallos.	2	D

Nombre del activo de información	Valoración del riesgo de los activos	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
Licencias de Windows	10	[E20] Vulnerabilidades de los programas (software)	Fallas de seguridad en el sistema operativo	A	1	10	B	3	Se configura la actualización automática de Windows para recibir parches de seguridad por Microsoft.	3	D
Licencias de Windows	10	[E21] Errores de mantenimiento / actualización de programas (software)	Uso de versiones obsoletas o sin soporte	A	1	10	B	3	Se mantiene un registro actualizado de las versiones de Windows utilizadas en la entidad.	3	D
Router principal	21	[A6] Abuso de privilegios de acceso	Acceso sin restricciones a la configuración del router	I	3	63	C	2	Se modifica el usuario y contraseña por defecto del router, estableciendo credenciales seguras y únicas.	32	C
Router principal	21	[A6] Abuso de privilegios de acceso	Configuración incorrecta de privilegios de usuario	I	4	84	C	2	Se deshabilita el acceso remoto a la configuración del router, salvo en casos específicos con medidas de seguridad.	42	C
Router principal	21	[E10] Errores de secuencia	Modificación de reglas de tráfico y filtrado de contenido	M	2	42	I	3	Se limita el acceso a la configuración del router únicamente al personal autorizado mediante credenciales seguras.	14	A
Switches de red	18	[E9] Errores de [re-]encaminamiento	Configuración incorrecta de VLANs	I	4	72	C	1		72	C

Nombre del activo de información	Valoración del riesgo de los activos	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
Switches de red	18	[A10] Alteración de secuencia	Exposición a ataques de suplantación de direcciones MAC	I	3	54	C	1		54	C
Switches de red	18	[A15] Modificación deliberada de la información	Problemas en la asignación de direcciones IP o enrutamiento estático/dinámico	I	4	72	C	3	Se configuran rutas estáticas y se limita el rango de IPs asignadas para reducir posibles brechas de seguridad.	24	C
Access Point	16	[A12] Análisis de tráfico	No uso de cifrado en la red inalámbrica o en el tráfico interno	I	3	48	C	3	Se implementan herramientas de monitoreo (FING) para detectar intentos de acceso no autorizado.	16	I
Access Point	16	[I8] Fallo de servicios de comunicaciones	Uso de protocolos de cifrado débiles o mal configurados	I	3	48	C	3	Se implementa un firewall para bloquear conexiones que utilicen protocolos inseguros, garantizando así una comunicación segura dentro de la red.	16	I
Historias Laborales	9	[A19] Divulgación de información	Falta de políticas de seguridad en el acceso a documentos	I	4	36	I	1		36	C
Licencia Windows Server	11	[E21] Errores de mantenimiento / actualización de programas (software)	Incompatibilidad con otros programas o servicios	M	3	33	I	4	Se implementan versiones de Windows Server que cuenten con soporte oficial y sean compatibles con los programas.	8	B

Nombre del activo de información	Valoración del riesgo de los activos	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
Oficinas	9	[A11] Acceso no autorizado	Falta de controles de acceso físicos	M	4	36	I	3	Se instalan cámaras de seguridad en puntos estratégicos para supervisar accesos y detectar incidentes.	12	A
Técnico TIC	23	[E28] Indisponibilidad del personal	Dependencia excesiva de un solo empleado	I	2	46	C	2	Se establecen roles para garantizar la continuidad del servicio en ausencia del funcionario principal.	23	C
Personera	16	[A29] Extorsión	Ataques a través de medios digitales	I	3	48	C	3	Se instalan y mantienen actualizados antivirus y firewalls en los dispositivos de las diferentes áreas de la entidad.	16	I
Personera	16	[E19] Fugas de información	Acceso a información confidencial	I	3	48	C	3	Se establecen políticas de contraseñas seguras y cambios periódicos de credenciales.	16	I
Personeros delegados	16	[A30] Ingeniería social	Uso de dispositivos electrónicos personales para trabajo	I	2	32	I	2	Se restringe el uso de dispositivos personales no autorizados para el manejo de información oficial.	16	I
Directores Administrativos	17	[E19] Fugas de información	Almacenamiento de información en dispositivos no protegidos	I	5	85	C	1		85	C
Directores Administrativos	17	[E7] Deficiencias en la organización	Correos de phishing	I	4	68	C	1		68	C

Nombre del activo de información	Valoración del riesgo de los activos	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
Funcionarios	15	[A30] Ingeniería social	Caer en correos fraudulentos o llamadas engañosas	I	4	60	C	1		60	C
Contratistas	14	[A28] Indisponibilidad del personal	Falta de planes de contingencia ante la ausencia de contratistas clave	I	4	56	C	3	Se designan empleados o contratistas suplentes que puedan asumir funciones clave en caso de ausencia.	19	I
Actas de comité	9	[A19] Divulgación de información	Almacenamiento sin controles de acceso adecuados	M	3	27	I	3	Se establecen copias de seguridad periódicas en entornos seguros.	9	B
Actos administrativos	11	[A11] Acceso no autorizado	Falta de controles de acceso adecuados	I	4	44	I	1		44	C
Comunicaciones Oficiales	9	[A15] Modificación deliberada de la información	Falta de trazabilidad en las modificaciones	M	3	27	I	4	Se implementa un sistema de gestión documental que registre automáticamente cada modificación realizada en las comunicaciones oficiales.	7	B
Contratos estatales	14	[E19] Fugas de información	Falta de auditoría en el acceso a los documentos	I	4	56	C	1		56	C

Nombre del activo de información	Valoración del riesgo de los activos	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
Informes Institucionales	9	[A18] Destrucción de información	Falta de políticas de recuperación de desastres	M	3	27	I	2	Se implementa un sistema de backup manual con copias almacenadas en ubicación segura (local)	14	A
Planes, programas y proyectos institucionales	9	[A15] Modificación deliberada de la información	Uso de formatos editables sin restricciones	M	3	27	I	3	Se gestiona un historial de versiones para rastrear cualquier modificación y restaurar versiones previas si es necesario.	9	B
Conciliaciones	19	[E15] Alteración accidental de la información	Uso de archivos no protegidos contra modificaciones accidentales	M	2	38	I	3	Se implementa un control de versiones en los documentos, permitiendo revertir cambios accidentales.	13	A
Equipo Personera	18	[A26] Ataque destructivo	Protección inadecuada contra malware o ataques cibernéticos destructivos	I	4	72	C	1		72	C
Equipo Personeros delegados	18	[A23] Manipulación de los equipos	Modificación o eliminación de archivos sensibles	I	4	72	C	1		72	C
Equipos jefes Administrativos y/o Financieros	18	[A7] Uso no previsto	Uso de dispositivos USB o externos sin control	I	5	90	C	1		90	C
Equipos Soporte TIC	18	[E2] Errores del administrador	Manejo incorrecto de permisos de acceso	I	3	54	C	3	Se aplica el principio de mínimo privilegio, evitando accesos innecesarios a recursos sensibles.	18	I

Nombre del activo de información	Valoración del riesgo de los activos	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
Equipos Soporte TIC	18	[A26] Ataque destructivo	Respaldo insuficiente de configuraciones	I	4	72	C	2	Se realizan copias de seguridad manuales en intervalos regulares.	36	C
Equipos funcionarios	15	[A25] Robo	Falta de cifrado en los datos almacenados	I	3	45	I	3	Se establecen permisos de acceso para evitar que usuarios sin autorización manipulen información.	15	A
Equipos Contratistas	11	[A6] Abuso de privilegios de acceso	Uso compartido de credenciales o dispositivos	I	3	33	I	2	Se establece que cada contratista debe contar con credenciales únicas e intransferibles.	17	I
Internet	16	[A24] Denegación de servicio	Configuraciones de red inseguras	M	2	32	I	3	Se establecen reglas de firewall para bloquear accesos no autorizados.	11	A
Internet	16	[A7] Uso no previsto	Ancho de banda insuficiente para resistir ataques volumétricos	I	3	48	C	3	Se implementan herramienta de monitoreo en tiempo real para identificar picos de tráfico inusuales	16	I
Rack	9	[I6] Corte del suministro eléctrico	Interrupción del funcionamiento de los equipos alojados	M	4	36	I	4	Se instala un UPS para mantener el suministro eléctrico en caso de cortes.	9	B
Disco duro externo	10	[I10] Degradación de los soportes de almacenamiento de la información	Sobreescritura continua y uso intensivo	I	4	40	I	1		40	C

Nombre del activo de información	Valoración del riesgo de los activos	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
UPS	7	[I7] Condiciones inadecuadas de temperatura o humedad	Sobrecalentamiento de la UPS	M	3	21	I	3	Se instala la UPS en un espacio bien ventilado, alejado de fuentes de calor.	7	B
Impresoras	6	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Obstrucción de los inyectores o rodillos de alimentación	M	3	18	I	4	Se establece un mantenimiento preventivo, realizado por un tercero contratado a través de un contrato de soporte	5	B

Nota. Matriz de Activos y Amenazas (Autoría Propia)

La inyección SQL en la base de datos de peticiones y solicitudes es una vulnerabilidad crítica. Permite a los atacantes ejecutar comandos maliciosos que pueden alterar o robar datos importantes. Si no se controlan adecuadamente, pueden afectar la integridad y seguridad de la información, lo que podría generar problemas legales y dañar la confianza en la entidad. Adicionalmente en el Sistema de Información Financiero, los privilegios de administrador o superusuario pueden ser un riesgo si no se gestionan correctamente. Esto puede permitir el acceso a datos financieros sensibles por personas no autorizadas, lo que incrementa el riesgo de fraudes o manipulación de información financiera, afectando la transparencia y confiabilidad de los registros contables. Así mismo, los programas ocultos de puerta trasera (backdoors) en el sistema de ventanilla única permiten a los atacantes acceder sin ser detectados. Esto puede llevar al robo o modificación de información importante, o incluso al control total del sistema. Sin protección, los backdoors facilitan ataques cibernéticos peligrosos.

El servidor principal enfrenta vulnerabilidades como sobrecarga de solicitudes o ataques, mala gestión de recursos e insuficiente capacidad de hardware. Estas debilidades pueden generar interrupciones en los servicios, afectando la disponibilidad de sistemas cruciales para el funcionamiento de la entidad. Las fallas pueden llevar a pérdidas económicas y afectar la productividad. Así mismo, en el servidor físico adicional, el desgaste de componentes físicos y los problemas en la gestión del almacenamiento son riesgos importantes. Si no se hace un mantenimiento adecuado, los datos pueden perderse o volverse inaccesibles, afectando la disponibilidad y recuperación de la información.

La falta de registros detallados en los logs de respaldo y la ausencia de auditorías periódicas en el backup de la base de datos son riesgos graves. Sin estos controles, no se puede garantizar la integridad de los respaldos, lo que aumenta el riesgo de pérdida de datos en caso de

fallos en el sistema. Del mismo modo, el switch de red enfrenta vulnerabilidades como configuración incorrecta de VLANs y suplantación de direcciones MAC. Esto permite a los atacantes acceder a la red interna y obtener información confidencial. Si no se protegen adecuadamente, estos ataques pueden comprometer la seguridad de la infraestructura de la red. Además, el almacenamiento de información en dispositivos no protegidos, junto con el phishing y el riesgo de caer en correos fraudulentos en los directores y funcionarios, es otro riesgo importante. Estos ataques pueden dar acceso a sistemas internos, comprometiendo la seguridad de la información y exponiendo a la organización a filtraciones de datos.

La falta de auditoría en el acceso a documentos en los actos administrativos también es una vulnerabilidad. Sin auditorías, es difícil detectar accesos no autorizados o manipulaciones de documentos importantes, lo que puede afectar la integridad de los procesos organizacionales. Los equipos de cómputo de directivos y jefes administrativos enfrentan vulnerabilidades como protección inadecuada contra malware y modificación de archivos sensibles. Además, el uso de dispositivos USB sin control puede propagar software maligno y robar información, lo que aumenta el riesgo de pérdida de datos.

Finalmente, el disco duro externo enfrenta el riesgo de sobreescritura continua y uso intensivo, lo que puede llevar a la pérdida o corrupción de datos almacenados. Si no se gestionan adecuadamente, los recursos de almacenamiento pueden comprometer la integridad y disponibilidad de la información.

Por lo anterior, la falta de controles adecuados en estos activos de información puede poner en riesgo la confidencialidad, integridad y disponibilidad de los datos. Esto afectaría directamente las operaciones de la entidad.

Mapa de Riesgos

En la Personería Municipal de Armenia, la seguridad de la información es un aspecto crítico debido a la gestión de datos sensibles y procesos administrativos esenciales. Para garantizar la protección de estos activos, se elabora un mapa de riesgos, el cual permite identificar y analizar las amenazas que pueden comprometer la confidencialidad, integridad y disponibilidad de la información.

Esta herramienta facilita la visualización de los activos más vulnerables, evalúa la efectividad de los controles existentes y orienta la toma de decisiones para implementar medidas de mitigación adecuadas, asegurando una gestión proactiva de la seguridad de la información.

Tabla 21

Apetito por el riesgo y zonas de Admisibilidad

		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
IMPACTO	MUY ALTA		, R41, R18, R11, R9	, R59, R43, R42, R37, R36, R34, R30, R25, R23, R20, R17, R14, R13, R12	, R57, R56, R52, R48, R47, R35, R33, R31, R24, R19, R16, R10, R7, R5, R4	, Riesgo58, Riesgo45, Riesgo15, Riesgo6
	ALTA		, R63, R55, R44, R32	, R68, R67, R62, R61, R54, R53, R51, R49, R39, R8	, R66, R65, R50, R40, R38, R22, R21	
	MEDIA		, R26			
	BAJA					
	MUY BAJA					
	RIESGO	MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
		PROBABILIDAD				

Nota. Matriz de Riesgo (Autoría Propia)

Los riesgos de nivel catastrófico en estos casos pueden tener un impacto grave en la organización, como si se presenta acceso no autorizado, cambios indebidos o eliminación de información en la base de datos debido a fallas en la seguridad de las aplicaciones web, los datos importantes pueden ser alterados o robados. Esto puede afectar la privacidad, causar problemas legales y hacer que las personas pierdan confianza en la entidad. Por otro lado, si el servidor principal deja de funcionar por completo, los sistemas y servicios esenciales no estarán disponibles. Esto puede interrumpir el trabajo, generar pérdidas económicas y dificultar la prestación de servicios, afectando la productividad y el funcionamiento de la organización.

Se identifican varios riesgos mayores que afectan la seguridad de la información. Uno de los principales problemas es el almacenamiento inadecuado de documentos, lo cual puede causar pérdida o filtración de información. También se detectó el uso de contraseñas débiles o compartidas, lo que facilita el acceso no autorizado a los sistemas. Otro riesgo es la falta de capacitación del personal en temas de seguridad informática, lo que aumenta la posibilidad de caer en engaños como correos de phishing. En la parte técnica, se encontraron fallas en la configuración de la red, como errores en las VLANs, en la asignación de direcciones IP y en el enrutamiento, lo cual puede causar interrupciones o accesos indebidos. Además, hay debilidades en el uso de cifrado, ya sea por falta de protección en la red inalámbrica o por el uso de protocolos inseguros. Otros riesgos incluyen el uso de dispositivos personales sin protección para el trabajo, el almacenamiento de información en equipos no seguros y el acceso sin control a datos confidenciales.

Todos estos problemas muestran la necesidad de tomar medidas para mejorar la seguridad y proteger mejor la información de la Personería Municipal de Armenia.

Plan de Tratamiento de Riesgos

El plan de tratamiento del riesgo busca manejar los riesgos que afectan a los activos de la entidad, para que, si ocurre un incidente, no cause daños o pérdidas importantes. Para tratar los riesgos se pueden tomar distintas acciones: evitar lo que los pueda causar, reducir la probabilidad de que ocurran, limitar sus consecuencias, compartirlos con otra organización.

En este paso se dio prioridad a reducir los riesgos que necesitan atención inmediata, porque son los que pueden causar mayor daño si llegan a presentarse. Estos riesgos podrían afectar los activos de la entidad de forma total o parcial. En el plan de tratamiento de riesgos de la Personería Municipal de Armenia se incluyeron los riesgos clasificados como Crítico (MA), Importante (A) y Apreciable (M), ya que son los que requieren mayor atención y respuesta rápida.

A continuación, se presenta el cuadro que contiene el plan de tratamiento de riesgos correspondiente a los activos de la Personería Municipal de Armenia.

Tabla 22

Plan de Tratamiento

Activos de información	Nombre del activo de información	VALORACIÓN RIESGO	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO							
					Transferir	Aceptar	Eliminar	Mitigar	Control por aplicar a partir de la norma ISO 27001:2013			
									DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
SOFTWARE	Base de Datos de Peticiones y Solicitudes	23	[E20] Vulnerabilidades de los programas (software)	Inyección SQL			X	DOMINIO_A9	OBJETIVO_A9_4	A9.4.1 Restricción de acceso a la información --Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Definir perfiles de usuario según roles o funciones (principio de mínimo privilegio).	
SOFTWARE	Base de Datos de Peticiones y Solicitudes	23	[E2] Errores del administrador	Configuraciones Incorrectas de Seguridad			X	DOMINIO_A12	OBJETIVO_A12_6	A12.6.2 Restricciones sobre la instalación de software --Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	La organización debe implementar medidas de protección contra software malicioso, incluyendo virus, ransomware, troyanos, spyware, etc., mediante soluciones tecnológicas y prácticas de gestión adecuadas.	
SOFTWARE	Base de Datos de Peticiones y Solicitudes	23	[E8] Difusión de software dañino	Exposición a Aplicaciones Web Vulnerables			X	DOMINIO_A12	OBJETIVO_A12_6	A12.6.1 Gestión de las vulnerabilidades técnicas --Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	La organización debe implementar un proceso sistemático para identificar, evaluar, priorizar y mitigar las vulnerabilidades técnicas que puedan afectar la seguridad de los sistemas de información.	

Activos de información	Nombre del activo de información	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO							
				Control por aplicar a partir de la norma ISO 27001:2013							
				Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
SERVICIOS	Portal Web de la Personería	13	[E15] Alteración accidental de la información	Modificación malintencionada del portal web	X		DOMINIO_A12	OBJETIVO_A12_4	A12.4.1 Registro de eventos -- Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Garantizar que los eventos relevantes de seguridad sean registrados, monitoreados y revisados periódicamente, con el fin de detectar accesos no autorizados, comportamientos anómalos, incidentes potenciales y cumplir requisitos legales o de auditoría.	
SERVICIOS	Portal Web de la Personería	13	[A24] Denegación de servicio	Configuración de Seguridad Incorrecta	X		DOMINIO_A18	OBJETIVO_A18_1	A18.1.4 Privacidad y protección de información de datos personales -- Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	Utilizar herramientas de escaneo de vulnerabilidades (por ejemplo, Nessus, OpenVAS, Qualys) para detectar vulnerabilidades conocidas en sistemas, aplicaciones y dispositivos.	
SOFTWARE	Sistema de información financiero	23	[E10] Errores de secuencia	Falta de copias de seguridad (backup)		X	DOMINIO_A14	OBJETIVO_A14_2	A.14.2.7 Desarrollo contratado externamente --Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	Usar copias de seguridad en la nube o almacenamiento externo para proteger los datos de fallas físicas, además de pruebas regulares de restauración para asegurar la integridad de los backups	

Tabla 22 (Continuación)

Plan de Tratamiento

Activos de información	Nombre del activo de información	VALORACIÓN RIESGO	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO							
					Transferir	Aceptar	Eliminar	Mitigar	Control por aplicar a partir de la norma ISO 27001:2013			
									DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
SOFTWARE	Sistema de información financiero	23	[A6] Abuso de privilegios de acceso	Privilegios de cuenta de administrador o superusuario			X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Implementar MFA (autenticación multifactor) en todas las cuentas con acceso elevado es una de las medidas más efectivas para prevenir accesos no autorizados, incluso si las credenciales son comprometidas.	
SOFTWARE	Sistema de información financiero	23	[E21] Errores de mantenimiento / actualización de programas (software)	Software desactualizado			X	DOMINIO_A12	OBJETIVO_A12_6	A12.6.1 Gestión de las vulnerabilidades técnicas --Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Realizar revisión periódica de versiones instaladas, así como implementar una política de parches y actualizaciones	
SOFTWARE	Sistema de información Ventanilla Única	22	[A5] Suplantación de la identidad del usuario	Programas ocultos de puerta trasera (Backdoor)			X	DOMINIO_A12	OBJETIVO_A12_2	A12.2.1 Controles contra códigos maliciosos --Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Usar antivirus o EDR actualizados que detecten amenazas. También es importante dividir la red en partes (segmentación) para limitar el acceso. Además, se deben revisar los equipos y la red constantemente.	

Activos de información	Nombre del activo de información	VALORACIÓN RIESGO	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO							
					Transferir	Aceptar	Eliminar	Mitigar	Control por aplicar a partir de la norma ISO 27001:2013			
									DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
SOFTWARE	Sistema de información Ventanilla Única	22	[E1] Errores de los usuarios	Falta de autenticación multifactor (MFA)				X	DOMINIO_A9	OBJETIVO_A9_4	A9.4.2 Procedimiento de ingreso seguro --Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	Aplicar la autenticación multifactor (MFA) en servicios clave como el correo electrónico, implementar VPN para proteger el acceso contra el robo de contraseñas. Además, se debe capacitar a los usuarios para que comprendan cómo usar MFA. Reforzar las políticas de contraseñas para asegurar que los usuarios elijan contraseñas seguras y las cambien con regularidad. Además, se debe forzar el cambio de credenciales para evitar que personas no autorizadas accedan a aplicaciones.
SOFTWARE	Sistema de información Ventanilla Única	22	[A22] Manipulación de programas	Credenciales débiles o comprometidas				X	DOMINIO_A9	OBJETIVO_A9_4	A9.4.1 Restricción de acceso a la información --Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Implementar medidas como sistemas de protección anti-DDoS, equilibradores de carga que distribuyan el tráfico y firewalls que puedan filtrar las solicitudes sospechosas.
HARDWARE	Servidor Principal	24	[E24] Caída del sistema por agotamiento de recursos	Sobrecarga de solicitudes o ataques de denegación de servicio				X	DOMINIO_A13	OBJETIVO_A13_1	A13.1.1 Controles de redes --Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	

Activos de información	Nombre del activo de información	VALORACIÓN RIESGO	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO					Control por aplicar a partir de la norma ISO 27001:2013		
					Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
HARDWARE	Servidor Principal	24	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Mala gestión de recursos del sistema				X	DOMINIO_A12	OBJETIVO_A12_1	A12.1.3 Gestión de capacidad -- Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	Monitorear el servidor para saber si está usando bien sus recursos, si se detecta que algo consume mucho, se deben tomar acciones como optimizar procesos, borrar archivos innecesarios o mejorar el equipo, para que no se caigan los servicios.
HARDWARE	Servidor Principal	24	[I5] Avería de origen físico o lógico	Insuficiente capacidad de hardware				X	DOMINIO_A12	OBJETIVO_A12_1	A12.1.3 Gestión de capacidad -- Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	Revisar periódicamente si tiene suficientes recursos como memoria, almacenamiento y procesador. Si se nota que está al límite, es necesario ampliar el hardware o mejorar la infraestructura antes de que afecte los servicios.
HARDWARE	Servidor físico adicional	23	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de mantenimiento preventivo				X	DOMINIO_A12	OBJETIVO_A12_6	A12.6.1 Gestión de las vulnerabilidades técnicas --Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Hacer mantenimiento al servidor con frecuencia, como borrar archivos innecesarios, actualizar programas y revisar el estado del hardware. Esto ayuda a que el servidor funcione bien y no falle de forma inesperada.

Activos de información	Nombre del activo de información	VALORACIÓN RIESGO	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO					Control por aplicar a partir de la norma ISO 27001:2013		
					Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
HARDWARE	Servidor físico adicional	23	[E24] Caída del sistema por agotamiento de recursos	Fallas en la gestión del almacenamiento				X	DOMINIO_A12	OBJETIVO_A12_1	A12.1.3 Gestión de capacidad -- Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	Revisar regularmente cuánto espacio en disco tiene el servidor. Si se está llenando, es importante borrar archivos que no se necesitan o moverlos a otro lugar, también se pueden usar herramientas que informen cuando queda poco espacio.
HARDWARE	Servidor físico adicional	23	[I7] Condiciones inadecuadas de temperatura o humedad	Desgaste de componentes físicos				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Revisar el hardware del servidor cada cierto tiempo. Si se detecta que algún componente está viejo o funcionando mal, se debe cambiar antes de que falle. Esto ayuda a evitar interrupciones y pérdidas de datos.
SERVICIOS	Correo Electrónico Institucional	11	[A6] Abuso de privilegios de acceso	Falta de control en los accesos y permisos				X	DOMINIO_A13	OBJETIVO_A13_2	A13.2.3 Mensajería Electrónica -- Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	Controlar quién tiene acceso al correo institucional y verificar los permisos asignados. Las cuentas que ya no se utilizan deben eliminarse, se debe activar la autenticación en dos pasos y evitar reenvíos automáticos sin autorización.

Activos de información	Nombre del activo de información	VALORACIÓN RIESGO	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO							
					Transferir	Aceptar	Eliminar	Mitigar	Control por aplicar a partir de la norma ISO 27001:2013			
									DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
SERVICIOS	Correo Electrónico Institucional	11	[A7] Uso no previsto	Envío de información sensible a destinatarios no autorizados			X	DOMINIO_ A13	OBJETIVO _A13_2	A13.2.3 Mensajería Electrónica -- Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	Capacitar al personal a tener cuidado con lo que envía por correo, especialmente si la información es sensible. así como, clasificar los archivos según su nivel de confidencialidad y usar cifrado cuando se comparten. Activar los registros (logs) del sistema de respaldo para guardar detalles como fecha, hora y si el respaldo fue exitoso. Estos registros deben revisarse regularmente para asegurar que todo funcione bien y que los datos estén protegidos en caso de una falla.	
DATOS	Backup de Base de Datos	21	[E3] Errores de monitorización (log)	Falta de registros detallados en los logs de respaldo			X	DOMINIO_ A12	OBJETIVO _A12_4	A12.4.1 Registro de eventos -- Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Configurar el sistema para que nos avise automáticamente si un respaldo falla. Esto garantiza que podamos actuar rápidamente si algo sale mal, evitando la pérdida de datos valiosos y asegurando la continuidad del negocio.	
DATOS	Backup de Base de Datos	21	[A4] Manipulación de la configuración	No detección de fallos en la ejecución del backup			X	DOMINIO_ A12	OBJETIVO _A12_3	A12.3.1 Respaldo de la información -- Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.		

Activos de información	Nombre del activo de información	VALORACIÓN RIESGO	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO					Control por aplicar a partir de la norma ISO 27001:2013		
					Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
DATOS	Backup de Base de Datos	21	[E2] Errores del administrador	No realizar auditorías periódicas a los registros de backup				X	DOMINIO_A12	OBJETIVO_A12_4	A12.4.1 Registro de eventos -- Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Realizar revisiones periódicas de los registros para asegurarse de que los datos se están respaldando correctamente y sin fallos, las auditorías pueden hacerse de forma manual o automática y deben llevarse a cabo con regularidad para garantizar que siempre haya un respaldo confiable.
SOFTWARE	Licencias de Microsoft Office	7	[I5] Avería de origen físico o lógico	Uso de licencias no compatibles con la infraestructura TI				X	DOMINIO_A8	OBJETIVO_A8_1	A8.1.1 Inventario de activos -- Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Verificar si la licencia es compatible con el sistema donde se va a usar. También es importante tener un control de todas las licencias que tiene la empresa y asegurarse de que se usan correctamente para evitar fallos o problemas legales.
SOFTWARE	Licencias de Microsoft Office	7	[E2] Errores del administrador	Fallo en los servidores de validación de Microsoft				X	DOMINIO_A12	OBJETIVO_A12_1	A12.1.2 Gestión de cambios -- Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Verificar el estado de los servidores de validación antes de aplicar cambios, así como tener copias de respaldo de claves y activadores válidos

Activos de Información	Nombre del activo de información	VALORACIÓN RIESGO	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO					Control por aplicar a partir de la norma ISO 27001:2013		
					Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
SOFTWARE	Licencias de Windows	10	[E20] Vulnerabilidades de los programas (software)	Fallas de seguridad en el sistema operativo				X	DOMINIO_A12	OBJETIVO_A12_6	A12.6.1 Gestión de las vulnerabilidades técnicas --Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Usar sistemas operativos con licencia legal, verificar que sean compatibles y mantenerlos siempre actualizados.
SOFTWARE	Licencias de Windows	10	[E21] Errores de mantenimiento / actualización de programas (software)	Uso de versiones obsoletas o sin soporte				X	DOMINIO_A12	OBJETIVO_A12_1	A12.1.2 Gestión de cambios --Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	No se debe usar software o sistemas operativos antiguos que ya no reciben actualizaciones. Es importante hacer un inventario, saber qué versión está instalada y cambiarla por una que todavía tenga soporte para evitar riesgos de seguridad.
COMUNICACIONES	Router principal	21	[A6] Abuso de privilegios de acceso	Acceso sin restricciones a la configuración del router				X	DOMINIO_A13	OBJETIVO_A13_1	A13.1.1 Controles de redes --Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	El router debe tener contraseña fuerte y no usar la que viene por defecto. Solo personas autorizadas deben poder entrar a su configuración. Si no es necesario el acceso remoto, se debe desactivar. También es útil tener registros de quién accede.

Activos de Información	Nombre del activo de información	VALORACIÓN RIESGO	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO							
					Transferir	Aceptar	Eliminar	Mitigar	Control por aplicar a partir de la norma ISO 27001:2013			
									DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
COMUNICACIONES	Router principal	21	[A6] Abuso de privilegios de acceso	Configuración incorrecta de privilegios de usuario			X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Crear niveles de permiso según el rol de cada persona. Solo los administradores deben poder hacer cambios importantes. También es clave revisar las cuentas y eliminar las que no se usan.	
COMUNICACIONES	Router principal	21	[E10] Errores de secuencia	Modificación de reglas de tráfico y filtrado de contenido			X	DOMINIO_A13	OBJETIVO_A13_1	A13.1.1 Controles de redes --Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Solo personal autorizado debe cambiar las reglas del router. Se deben registrar todos los cambios y revisar que las reglas protejan la red, no la expongan. También es importante tener un control de quién accede al router	
COMUNICACIONES	Switches de red	18	[E9] Errores de [re-]encaminamiento	Configuración incorrecta de VLANs			X	DOMINIO_A13	OBJETIVO_A13_1	A13.1.3 Separación en las redes --Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	Las VLAN deben configurarse correctamente para que cada grupo de dispositivos esté en su red correspondiente. Se deben revisar los puertos y troncales del switch para evitar errores. Configurar el switch para aceptar solo ciertas direcciones por cada puerto. También es útil limitar cuántos dispositivos se pueden conectar y revisar si hay cambios inesperados en la red.	
COMUNICACIONES	Switches de red	18	[A10] Alteración de secuencia	Exposición a ataques de suplantación de direcciones MAC			X	DOMINIO_A13	OBJETIVO_A13_1	A13.1.1 Controles de redes --Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Así se bloquea el acceso de equipos no autorizados.	

Activos de Información	Nombre del activo de información	VALORACIÓN RIESGO	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO							
					Transferir	Aceptar	Eliminar	Mitigar	Control por aplicar a partir de la norma ISO 27001:2013			
									DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
COMUNICACIONES	Switches de red	18	[A15] Modificación deliberada de la información	Problemas en la asignación de direcciones IP o enrutamiento estático /dinámico			X	DOMINIO_A13	OBJETIVO_A13_1	A13.1.1 Controles de redes --Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Controlar las IP que entrega el router y cómo están configuradas las rutas para que el tráfico llegue al lugar correcto. Esto incluye evitar errores como IPs duplicadas y asegurarse de que cada red tenga su ruta definida.	
COMUNICACIONES	Access Point	16	[A12] Análisis de tráfico	No uso de cifrado en la red inalámbrica o en el tráfico interno			X	DOMINIO_A10	OBJETIVO_A10_1	A10.1.1 Política sobre el uso de controles criptográficos --Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	El Access point debe estar configurado con cifrado WPA2 o WPA3. Así, nadie podrá ver la información que se transmite por la red Wi-Fi. También es recomendable cifrar las conexiones internas con protocolos como HTTPS o VPN para proteger los datos.	
COMUNICACIONES	Access Point	16	[I8] Fallo de servicios de comunicaciones	Uso de protocolos de cifrado débiles o mal configurados			X	DOMINIO_A13	OBJETIVO_A13_1	A13.1.1 Controles de redes --Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Configurar el punto de acceso para usar cifrado WPA2 o WPA3, y evitar protocolos antiguos como WEP o WPA. También hay que revisar que la contraseña sea segura y actualizar la configuración regularmente para que la red esté bien protegida.	

Activos de Información	Nombre del activo de información	VALORACIÓN RIESGO	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO							
					Transferir	Aceptar	Eliminar	Mitigar	Control por aplicar a partir de la norma ISO 27001:2013			
									DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
DATOS	Historias Laborales	9	[A19] Divulgación de información	Falta de políticas de seguridad en el acceso a documentos			X	DOMINIO_A8	OBJETIVO_A8_2	A8.2.2 Etiquetado de la información - -Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Establecer reglas claras para saber quién puede acceder a qué documentos. Solo el personal autorizado debe ver o editar archivos importantes. También es útil clasificar los documentos por nivel de sensibilidad y revisar los permisos con frecuencia.	
SOFTWARE	Licencia Windows Server	11	[E21] Errores de mantenimiento / actualización de programas (software)	Incompatibilidad con otros programas o servicios			X	DOMINIO_A18	OBJETIVO_A18_1	A18.1.1 Identificación de la legislación aplicable. --Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	Antes de instalar un programa en el servidor, se debe revisar si la licencia del sistema lo permite y si es compatible. Así se evitan errores de funcionamiento o problemas legales. También es útil hacer pruebas antes de aplicarlo en producción.	
INSTALACIONES	Oficinas	9	[A11] Acceso no autorizado	Falta de controles de acceso físicos			X	DOMINIO_A11	OBJETIVO_A11_1	A11.1.2 Controles de acceso físicos --Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	Usar cerraduras, tarjetas de acceso o lectores biométricos para controlar quién entra a las áreas importantes. También es necesario registrar las entradas, instalar cámaras y asegurarse de que solo el personal autorizado tenga acceso físico a los equipos.	

Activos de Información	Nombre del activo de información	VALORACIÓN RIESGO	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO					Control por aplicar a partir de la norma ISO 27001:2013		
					Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
PERSONAL	Técnico TIC	23	[E28] Indisponibilidad del personal	Dependencia excesiva de un solo empleado				X	DOMINIO_A7	OBJETIVO_A7_2	A7.2.1 Responsabilidades de la dirección --Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	Es importante que el conocimiento y las tareas críticas no dependan solo de una persona. Se deben compartir conocimientos, capacitar a otros compañeros y tener instrucciones para que cualquiera pueda continuar con el trabajo si alguien se ausenta.
PERSONAL	Personera	16	[A29] Extorsión	Ataques a través de medios digitales				X	DOMINIO_A7	OBJETIVO_A7_2	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información. --Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	Proteger los equipos usando antivirus y filtros en el correo. También es clave enseñar a los usuarios a no abrir archivos o enlaces desconocidos, y controlar el uso de memorias USB que no sean confiables.
PERSONAL	Personera	16	[E19] Fugas de información	Acceso a información confidencial				X	DOMINIO_A12	OBJETIVO_A12_4	A12.4.2 Protección de la información de registro --Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	La información importante debe tener control de acceso y estar cifrada. Se debe enseñar a los empleados a manejarla con cuidado y usar herramientas para evitar que salga sin autorización.

Activos de Información	Nombre del activo de información	VALORACIÓN RIESGO	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO					Control por aplicar a partir de la norma ISO 27001:2013		
					Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
PERSONAL	Personeros delegados	16	[A30] Ingeniería social	Uso de dispositivos electrónicos personales para trabajo				X	DOMINIO_ A6	OBJETIVO _A6_2	A6.2.1 Política para dispositivos móviles --Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Si los empleados usan sus propios equipos, deben seguir reglas claras. Es importante asegurar esos dispositivos con claves, cifrado y permisos limitados, y enseñar a los usuarios cómo usarlos de forma segura para proteger los datos de la organización.
PERSONAL	Directores Administrativos	17	[E19] Fugas de información	Almacenamiento o de información en dispositivos no protegidos				X	DOMINIO_ A8	OBJETIVO _A8_3	A8.3.1 Gestión de medio removibles --Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Aplicar políticas de uso seguro de dispositivos, no se debe guardar información importante en USB o computadoras sin proteger. Es necesario usar cifrado y contraseñas, y evitar llevar datos si no es indispensable
PERSONAL	Directores Administrativos	17	[E7] Deficiencias en la organización	Correos de phishing				X	DOMINIO_ A12	OBJETIVO _A12_2	A12.2.1 Controles contra códigos maliciosos --Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Usar filtros que bloqueen correos falsos y educar a los usuarios para que no abran enlaces ni archivos sospechosos. También se recomienda usar verificación en dos pasos para proteger las cuentas.

Activos de Información	Nombre del activo de información	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO							
				Transferir	Aceptar	Eliminar	Mitigar	Control por aplicar a partir de la norma ISO 27001:2013			
								DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
PERSONAL	Funcionarios	15	[A30] Ingeniería social	Caer en correos fraudulentos o llamadas enganosas			X	DOMINIO_A7	OBJETIVO_A7_2	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información. --Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	Capacitar a los empleados a reconocer correos o llamadas sospechosas y no dar información sin verificar. También se deben seguir protocolos para confirmar identidades y usar medidas como la autenticación en dos pasos.
PERSONAL	Contratistas	14	[A28] Indisponibilidad del personal	Falta de planes de contingencia ante la ausencia de contratistas clave			X	DOMINIO_A15	OBJETIVO_A15_1	A15.1.1 Política de seguridad de la información para las relaciones con proveedores --Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	Tener un plan en caso de que un contratista importante no esté disponible. Esto incluye capacitar a personal interno, tener documentación técnica al día y contar con proveedores de respaldo si es necesario.
DATOS	Actas de comité	9	[A19] Divulgación de información	Almacenamiento o sin controles de acceso adecuados			X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Establecer permisos para que solo las personas autorizadas accedan a la información. También se recomienda usar contraseñas fuertes, revisar quién tiene acceso y proteger los datos sensibles con controles adicionales.

Activos de Información	Nombre del activo de información	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO							
				Transferir	Aceptar	Eliminar	Mitigar	Control por aplicar a partir de la norma ISO 27001:2013			
								DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
DATOS	Actos administrativos	11	[A11] Acceso no autorizado	Falta de controles de acceso adecuados			X	DOMINIO_A9	OBJETIVO_A9_1	A9.1.1 Política de control de acceso -- Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Limitar el acceso a la información solo a las personas que lo necesiten para trabajar. Además, usar contraseñas fuertes, activar verificación en dos pasos y revisar los permisos de forma regular.
DATOS	Comunicaciones Oficiales	9	[A15] Modificación deliberada de la información	Falta de trazabilidad en las modificaciones			X	DOMINIO_A12	OBJETIVO_A12_4	A12.4.1 Registro de eventos -- Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Registrar quién hace cambios en los sistemas o archivos importantes. Así se puede llevar un control, detectar errores o malas prácticas, y tener evidencias si ocurre algún incidente.
DATOS	Contratos estatales	14	[E19] Fugas de información	Falta de auditoría en el acceso a los documentos			X	DOMINIO_A18	OBJETIVO_A18_1	A18.1.3 Protección de registros -- Control: Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Registrar todos los accesos a documentos importantes para saber quién los abre o modifica, esto ayuda a detectar accesos no autorizados y mantener la seguridad de la información.

Activos de Información	Nombre del activo de información	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO							
				Control por aplicar a partir de la norma ISO 27001:2013							
				Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
DATOS	Informes Institucionales	9	[A18] Destrucción de información	Falta de políticas de recuperación de desastres			X	DOMINIO_A17	OBJETIVO_A17_1	A17.1.1 Planificación de la continuidad de la seguridad de la información --Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis.	Tener un plan que diga qué hacer si ocurre un desastre. El plan debe incluir respaldos, pasos para recuperar sistemas y datos, y responsables de ejecutar cada acción. También se debe probar el plan con frecuencia.
DATOS	Planes, programas y proyectos institucionales	9	[A15] Modificación deliberada de la información	Uso de formatos editables sin restricciones			X	DOMINIO_A9	OBJETIVO_A9_4	A9.4.1 Restricción de acceso a la información --Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Proteger los documentos que se comparten, usando formatos no editables, contraseñas o permisos de solo lectura. Esto evita que se modifiquen sin autorización o se filtre información.
DATOS	Conciliaciones	19	[E15] Alteración accidental de la información	Uso de archivos no protegidos contra modificaciones accidentales			X	DOMINIO_A8	OBJETIVO_A8_2	A8.2.2 Etiquetado de la información - -Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Conservar los archivos importantes para que no se puedan editar por accidente. También se pueden dar permisos de solo lectura o usar funciones de respaldo y control de versiones.

Activos de Información	Nombre del activo de información	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO							
				Control por aplicar a partir de la norma ISO 27001:2013							
				Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
HARDWARE	Equipo Personera	18	[A26] Ataque destructivo				X	DOMINIO_A18	OBJETIVO_A18_2	A18.2.3 Revisión del cumplimiento técnico --Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	Proteger todos los equipos con un buen antivirus, mantenerlos actualizados y evitar instalar programas desconocidos. También es importante educar a los usuarios para no abrir archivos sospechosos o entrar a sitios peligrosos. Los archivos sensibles deben tener permisos que limiten quién puede ver o cambiar su contenido. También se deben hacer copias de seguridad frecuentes para evitar perder la información por errores.
HARDWARE	Equipo Personeros delegados	18	[A23] Manipulación de los equipos				X	DOMINIO_A9	OBJETIVO_A9_1	A9.1.2 Acceso a redes y a servicios en red --Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	
HARDWARE	Equipos jefes Administrativos y/o Financieros	18	[A7] Uso no previsto				X	DOMINIO_A13	OBJETIVO_A13_2	A13.2.1 Políticas y procedimientos de transferencia de información --Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	Para evitar virus o robo de datos, se deben bloquear los USB no autorizados y permitir solo los que han sido revisados. También es importante enseñar a los usuarios sobre estos riesgos.

Activos de Información	Nombre del activo de información	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO							
				Transferir	Aceptar	Eliminar	Mitigar	Control por aplicar a partir de la norma ISO 27001:2013			
								DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
HARDWARE	Equipos Soporte TIC	18	[E2] Errores del administrador				X	DOMINIO_A9	OBJETIVO_A9_1	A9.1.2 Acceso a redes y a servicios en red --Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Asignar permisos según el rol de cada persona y revisar con frecuencia quién tiene acceso a los equipos de tecnología. Solo los encargados deben tener permisos especiales, y es importante eliminar accesos que ya no se usan.
HARDWARE	Equipos Soporte TIC	18	[A26] Ataque destructivo				X	DOMINIO_A12	OBJETIVO_A12_1	A12.1.2 Gestión de cambios --Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Guardar copias actualizadas de las configuraciones de los equipos TIC, en un lugar seguro, para poder restaurarlas rápidamente si ocurre un problema o falla del sistema.
HARDWARE	Equipos funcionarios	15	[A25] Robo				X	DOMINIO_A10	OBJETIVO_A10_1	A10.1.1 Política sobre el uso de controles criptográficos --Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Conservar los datos importantes se deben cifrar los discos y bases de datos. Así, si alguien accede sin permiso, no podrá leer la información sin la clave de seguridad.

Activos de Información	Nombre del activo de información	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO							
				Control por aplicar a partir de la norma ISO 27001:2013							
				Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
SERVICIOS	Equipos Contratistas	11	[A6] Abuso de privilegios de acceso	Uso compartido de credenciales o dispositivos			X	DOMINIO_A9	OBJETIVO_A9_3	A9.3.1 Uso de información de autenticación secreta --Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Cada persona debe tener su propia cuenta y contraseña. No se deben compartir usuarios ni contraseñas, ni dejar que varios usen el mismo equipo sin control, para saber siempre quién hace qué.
SOPORTE	Internet	16	[A24] Denegación de servicio	Configuraciones de red inseguras			X	DOMINIO_A13	OBJETIVO_A13_1	A13.1.2 Seguridad de los servicios de red --Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Asegurar que todos los dispositivos de red estén configurados de forma correcta y segura, utilizando contraseñas fuertes y desactivando servicios innecesarios. Además, se debe controlar y monitorear el tráfico de red para detectar posibles incidentes.
SOPORTE	Internet	16	[A7] Uso no previsto	Ancho de banda insuficiente para resistir ataques volumétricos			X	DOMINIO_A13	OBJETIVO_A13_1	A13.1.2 Seguridad de los servicios de red --Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Prevenir la caída de servicios durante un ataque a través del aseguramiento de la red tenga para que suficiente capacidad de ancho de banda, implementar soluciones de mitigación DDoS y monitorear el tráfico de red constantemente para detectar cualquier ataque.

Activos de Información	Nombre del activo de información	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO							
				Control por aplicar a partir de la norma ISO 27001:2013							
				Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
AUXILIAR	Rack	9	[I6] Corte del suministro eléctrico				X	DOMINIO_A12	OBJETIVO_A12_3	A12.3.1 Respaldo de la información -- Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Garantizar un suministro eléctrico confiable con sistemas de respaldo, realizar mantenimientos regulares de los equipos y tener planes de recuperación para asegurar la rápida restauración de los servicios en caso de fallos.
HARDWARE	Disco duro externo	10	[I10] Degradación de los soportes de almacenamiento de la información				X	DOMINIO_A12	OBJETIVO_A12_6	A12.6.1 Gestión de las vulnerabilidades técnicas --Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Para evitar la sobrecarga del disco duro, se debe gestionar adecuadamente el almacenamiento, evitar sobrescribir datos continuamente. Además, realizar copias de seguridad periódicas asegura la protección de los datos ante fallos.
HARDWARE	UPS	7	[I7] Condiciones inadecuadas de temperatura o humedad				X	DOMINIO_A12	OBJETIVO_A12_3	A12.3.1 Respaldo de la información -- Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Garantizar su adecuada ventilación, monitorear la temperatura y asegurarse de que no se sobrecargue con equipos que excedan su capacidad. Además, realizar mantenimiento preventivo regularmente ayuda a mantener su funcionamiento óptimo.

Activos de Información	Nombre del activo de información	Amenazas metodología Magerit	Vulnerabilidad	PLAN DE TRATAMIENTO						
				Transferir	Aceptar	Eliminar	Mitigar	Control por aplicar a partir de la norma ISO 27001:2013		
								DOMINIO	OBJETIVO	Descripción de la aplicación del control
HARDWARE	Impresoras	6	[E23] Errores de mantenimiento / actualización de equipos (hardware)				X	DOMINIO_A12	OBJETIVO_A12_1	A12.1.2 Gestión de cambios -- Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información. Limpiar periódicamente los inyectores y rodillos, usar insumos adecuados y seguir un plan de mantenimiento. Así se garantiza el buen funcionamiento de la impresora y se evitan interrupciones.

Nota. Plan de tratamiento (Autoría Propia)

Evaluar el Nivel de Madurez de los Controles de Seguridad de la Información Mediante un Análisis GAP Estructurado

Se evalúa de forma integral el nivel de madurez de los controles de seguridad de la información implementados en la organización, utilizando como referencia los marcos normativos y de buenas prácticas internacionalmente reconocidos, específicamente ISO/IEC 27001 y COBIT. Esta evaluación se realizará a través de un enfoque cuantitativo, que permita asignar puntuaciones objetivas a cada control evaluado, y mediante un análisis GAP estructurado.

Por consiguiente, evaluar el nivel de madurez de los controles de seguridad de la información mediante el modelo COBIT permite a la Personería Municipal de Armenia obtener una visión estructurada y objetiva del estado actual de sus procesos de seguridad. COBIT, como marco de referencia para el gobierno y la gestión de las tecnologías de la información, proporciona un enfoque basado en procesos y niveles de capacidad que facilita medir, comparar y mejorar los controles existentes.

Aunque la organización no cuente con un Sistema de Gestión de Seguridad de la Información (SGSI) formalmente establecido, esta evaluación se convierte en una herramienta fundamental para identificar fortalezas, debilidades y oportunidades de mejora en la protección de los activos de información. El uso de COBIT permite realizar este análisis de manera ordenada, asignando niveles de madurez incluso a controles que aún no han sido formalizados. Esto proporciona una base clara y realista del estado actual de la seguridad, y sirve como punto de partida para priorizar acciones, justificar inversiones y, a largo plazo, orientar la implementación de un SGSI sólido y alineado con los objetivos institucionales.

Tabla 23*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
A5 Controles Organizacionales										
1	A.5.1 Políticas para la seguridad de la información				x			Documentado, estandarizado y comunicado	Se evidencia que la entidad cuenta con una política de seguridad de la información documentada, aprobada por la alta dirección. Sin embargo, su actualización aún no se realiza con base en métricas de desempeño, y no existe un proceso formalizado para evaluar su eficacia	Institucionalizar un proceso de revisión periódica basado en indicadores de cumplimiento y riesgo, integrando mejoras continuas y asegurando que la política refleje los cambios en el entorno tecnológico, normativo y organizacional.
	A.5.2 Roles y responsabilidades en la seguridad de la información	x						Incompleto	No se han definido ni asignado formalmente roles y responsabilidades relacionados con la seguridad de la información dentro de la organización. No existe documentación que establezca quién es responsable de implementar, monitorear o hacer cumplir las medidas de seguridad de la información, lo que genera una falta de control, coordinación y rendición.	Iniciar el proceso de identificación y asignación formal de roles y responsabilidades específicas para la seguridad de la información, documentarlas claramente en políticas u organigramas, y comunicar esta información a todo el personal involucrado para garantizar una gestión estructurada y efectiva de la seguridad.
3	A.5.3 Segregación de tareas	x						Incompleto	No existen prácticas ni controles implementados para garantizar la separación de funciones críticas dentro de los procesos de la organización. Las personas pueden tener acceso o control sobre etapas de un proceso, lo que incrementa el riesgo de errores o abusos sin posibilidad de detección oportuna.	Identificar las funciones que requieren separación de deberes para reducir riesgos, establecer controles que impidan la concentración de responsabilidades incompatibles en una sola persona, y documentar dichas medidas en los procedimientos internos.
4	A.5.4 Responsabilidades de gestión		x					Control existe de manera informal	No existen roles y responsabilidades claramente definidos ni formalizados en lo referente a la seguridad de la información. Las funciones de gestión se desempeñan de forma reactiva, sin una asignación oficial o una supervisión estructurada.	Establecer y documentar formalmente las responsabilidades específicas para la gestión de la seguridad de la información, asignándolas a personal calificado, y asegurando su revisión periódica para facilitar el cumplimiento de los objetivos de seguridad

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
5	A.5.5 Contacto con las autoridades		x					Control existe de manera informal	La entidad reconoce la necesidad de mantener comunicación con autoridades competentes, pero esta práctica se realiza de manera informal y sin procedimientos establecidos, lo que puede generar demoras.	Formalizar el proceso de contacto con las autoridades mediante la elaboración de procedimientos, asignar roles específicos para esta función, asegurando una respuesta coordinada y oportuna.
6	A.5.6 Contacto con grupos de interés especial	x						Incompleto	La organización no ha establecido ningún tipo de contacto formal ni participa en grupos de interés relacionados con la seguridad de la información. No se reconoce la importancia para el fortalecimiento de la seguridad, lo que limita el acceso a información sobre riesgos emergentes y mejores prácticas.	Determinar los grupos de interés relevantes para su sector y área de seguridad, establecer canales de comunicación con estos grupos, y fomentar la participación en actividades o eventos relacionados, lo que permitirá mejorar la colaboración y reforzar la estrategia de ciberseguridad.
7	A.5.7 Inteligencia de amenazas		x					Control existe de manera informal	la entidad reconoce la importancia de conocer las amenazas, pero aún no ha establecido un proceso formal para recopilar, analizar o actuar sobre información de amenazas.	implementar un mecanismo de monitoreo de fuentes confiables de ciberinteligencia, así como designar responsables que analicen dicha información y generen alertas que permitan reaccionar ante riesgos emergentes.
8	A.5.8 Seguridad de la información en la gestión de proyectos		x					Control existe de manera informal	la organización tiene una conciencia básica de la importancia de la seguridad de la información en los proyectos, pero no ha integrado prácticas formales de seguridad en la gestión de proyectos. Las consideraciones de seguridad se abordan sin una planificación ni asignación de responsabilidades durante todo el ciclo de vida del proyecto.	Incorporar la seguridad de la información desde las primeras fases de la gestión de proyectos, asegurando que se realicen evaluaciones de riesgos de seguridad, se asignen responsabilidades claras para la protección de la información y se establezcan controles de seguridad a lo largo de las distintas etapas del proyecto.

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
9	A.5.9 Inventario de activos de información y otros asociados a la misma					x		Monitoreado y medido	La organización mantiene un inventario de activos completo, actualizado, que incluye clasificaciones, propietarios asignados y niveles de criticidad. Sin embargo, debe estar integrado con otros procesos de seguridad de la información y gestión de TI	Hacer uso de herramientas de gestión de activos, incorporando análisis predictivos o métricas avanzadas para anticipar riesgos asociados a los activos críticos, y asegurando su alineación con los objetivos de negocio y seguridad.
10	A.5.10 Uso aceptable de activos de información y otros asociados a la misma				x			Documentado, estandarizado y comunicado	la organización cuenta con directrices formales sobre el uso aceptable de los activos, las cuales son comunicadas al personal y aplicadas de manera general. Sin embargo, aún pueden existir brechas en su monitoreo y la concienciación del personal.	Implementar controles de supervisión y auditoría, asegurando que todo el personal reciba formación continua sobre el uso aceptable de los activos, e definir métricas que permitan evaluar el grado de cumplimiento.
11	A.5.11 Devolución de activos					x		Monitoreado y medido	La organización tiene un proceso formal, documentado para la devolución de activos al finalizar la relación laboral. Este proceso está coordinado entre las áreas de TI y recursos humanos, asegurando la recuperación oportuna de equipos, credenciales y otros recursos.	Optimizar el análisis de datos históricos para detectar posibles riesgos o demoras en la devolución, y reforzar la retroalimentación entre áreas para seguir mejorando la eficiencia del proceso.
12	A.5.12 Clasificación de la información				x			Documentado, estandarizado y comunicado	la organización cuenta con procesos definidos para la clasificación de la información, los cuales se aplican en la mayoría de las áreas. La información se clasifica en función de criticidad. Sin embargo, no existen lineamientos para su protección.	Reforzar la capacitación sobre clasificación de la información, mejorar los mecanismos de control para asegurar una aplicación en la organización y considerar herramientas que faciliten la identificación de datos según su nivel de sensibilidad.
13	A.5.13 Etiquetado de la información				x			Documentado, estandarizado y comunicado	El etiquetado aún depende en gran medida de acciones manuales y del criterio del personal, lo que puede generar inconsistencias o errores en la identificación de datos sensibles.	Reforzar la capacitación del personal en esta práctica, ampliar el uso de herramientas que faciliten el etiquetado automático y establecer controles de verificación para asegurar una aplicación eficaz.

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
14	A.5.14 Intercambio de la información			x				Planificado y ejecutado, sin medición formal	Existen prácticas informales para compartir información, pero no se cuenta con lineamientos documentados que garanticen la protección de los datos durante el intercambio.	Formalizar políticas y procedimientos de intercambio seguro, incluyendo acuerdos de confidencialidad y mecanismos de cifrado, para fortalecer la protección de la información transmitida internamente y con terceros.
15	A.5.15 Control de Acceso			x				Planificado y ejecutado, sin medición formal	Existe una política de control de acceso, la cual establece principios de asignación y uso de credenciales. Aunque, carece de mecanismos de verificación y seguimiento que aseguren su cumplimiento, no está actualizada ni alineada con los cambios tecnológicos o de riesgo.	Revisar y formalizar la política de control de acceso, ampliando su cobertura y especificidad, así como implementar controles técnicos y auditorías periódicas para reforzar su cumplimiento y efectividad en toda la entidad.
16	A.5.16 Gestión de la identidad			x				Planificado y ejecutado, sin medición formal	Se utiliza mecanismos básicos de autenticación, como contraseñas, y ha implementado algunas prácticas para su protección, como requisitos mínimos de complejidad. Sin embargo, estas medidas no están estandarizadas ni se aplican en todos los sistemas. Además, no se cuenta con una política formal para la gestión segura de la información	Establecer una política clara sobre la gestión de credenciales secretas, definir requisitos técnicos y operativos para su creación, almacenamiento y renovación, e implementar mecanismos de autenticación más robustos, como autenticación multifactor, para mejorar la seguridad de los accesos.
17	A.5.17 Información de autenticación			x				Planificado y ejecutado, sin medición formal	Se promueve el uso de contraseñas y directrices de uso como longitud mínima y complejidad. Sin embargo, estas prácticas no están completamente formalizadas y no se brinda suficiente capacitación a los usuarios sobre el manejo seguro.	Establecer una política clara sobre el uso seguro de credenciales secretas, reforzar la concientización del personal en buenas prácticas de autenticación, y evaluar la implementación de controles como la autenticación multifactor.
18	A.5.18 Derechos de acceso				x			Documentado, estandarizado y comunicado	Se cuenta con procedimientos establecidos y aplicados para retirar o ajustar los derechos de acceso cuando un usuario finaliza su relación laboral y están coordinados con áreas como Recursos Humanos y TI.	Optimizar la eficiencia mediante herramientas de gestión de identidades y accesos que automaticen el ajuste de privilegios, asegurando un mayor control y reducción de riesgos por accesos.

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
19	A.5.19 Seguridad de la información en la relación con proveedores				x			Documentado, estandarizado y comunicado	Existen acuerdos formales que incluyen cláusulas de seguridad de la información, aunque su monitoreo y evaluación no son sistemáticos	Fortalecer los procesos de supervisión continua, estableciendo revisiones periódicas y evaluaciones de cumplimiento para asegurar que los proveedores mantengan los estándares de seguridad requeridos.
20	A.5.20 Requisitos de seguridad de la información en contratos con terceros				x			Documentado, estandarizado y comunicado	Los contratos con terceros incluyen cláusulas de seguridad de la información alineadas a los riesgos identificados. No obstante, se observa que podría mejorarse la supervisión continua del cumplimiento de estos requisitos.	Implementar mecanismos de monitoreo y auditoría para asegurar que los terceros mantengan los niveles de seguridad acordados durante toda la vigencia de los contratos.
21	A.5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC (Tecnologías de Información y Comunicación)			x				Planificado y ejecutado, sin medición formal	La organización tiene identificados algunos riesgos relacionados con la cadena de suministro de TIC. Se observa una falta de políticas específicas y controles formales para proteger la información que se comparte o se gestiona a través de terceros	Desarrollar e implementar un enfoque estructurado de gestión de riesgos para la cadena de suministro de TIC, estableciendo requisitos de seguridad claros, evaluaciones periódicas de proveedores y acuerdos de cumplimiento documentados.
22	A.5.22 Gestión del cambio, revisión y monitoreo de los servicios del proveedor o suministrador			x				Planificado y ejecutado, sin medición formal	Existen prácticas para gestionar cambios en los servicios de los proveedores, pero estas no están documentadas, lo que genera riesgos en la seguridad de la información. Se observa además una limitada supervisión y evaluación continua de los servicios contratados.	Establecer procedimientos de gestión de cambios aplicables a los proveedores, realizar revisiones periódicas de desempeño y cumplimiento de seguridad, e implementar métricas de monitoreo que permitan anticipar y mitigar posibles vulnerabilidades.

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
23	A.5.23 Seguridad de la información para el uso de servicios en la nube (cloud)	x						Incompleto	Actualmente la entidad no utiliza servicios en la nube, por lo que no existen políticas o controles asociados a este entorno. Sin embargo, la ausencia de un marco preparado para la eventual adopción de servicios cloud representa un riesgo si se llegaran a incorporar sin una adecuada gestión de seguridad.	Establecer lineamientos preventivos que definan requisitos de seguridad para el uso de servicios en la nube, de modo que, ante una necesidad de adopción, la entidad cuente con una base para proteger la información y cumplir con los estándares de seguridad.
24	A.5.24 Planeamiento y preparación de la gestión de incidentes de seguridad de la información			x				Planificado y ejecutado, sin medición formal	La organización cuenta con una estrategia de gestión de incidentes de seguridad, pero aún no tiene un plan completamente formalizado y documentado para la preparación y respuesta ante incidentes. La falta de procedimientos bien definidos puede generar retrasos o ineficiencias en la resolución de incidentes	Fortalecer la preparación mediante la formalización de un plan de gestión de incidentes, estableciendo roles y responsabilidades claras, así como procedimientos de respuesta que incluyan capacitación para mejorar la capacidad de respuesta ante incidentes de seguridad.
25	A.5.25 Evaluación y decisión en los eventos de seguridad de la información		x					Control existe de manera informal	No se ha implementado un proceso formal para la evaluación y toma de decisiones en relación con los eventos de seguridad de la información. Actualmente, las decisiones sobre la gestión de eventos se toman de manera ad hoc, sin un procedimiento claro.	Establecer un proceso formalizado para la evaluación y priorización de eventos de seguridad, definiendo criterios de impacto y capacitando a los equipos para tomar decisiones basadas en un marco estándar.
26	A.5.26 Respuesta a los incidentes de seguridad de la información		x					Control existe de manera informal	No se cuenta con un procedimiento documentado ni estructurado para responder a los incidentes de seguridad de la información. Actualmente, las respuestas se realizan sin coordinación adecuada, lo que incrementa el tiempo de resolución y el riesgo de impacto.	Diseñar, documentar e implementar un plan de respuesta a incidentes que defina roles, responsabilidades, tiempos de respuesta, y pasos a seguir ante distintos tipos de incidentes. Esto permitirá actuar oportuna, eficiente a los incidentes de seguridad.

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
27	A.5.27 Aprendizaje sobre los incidentes de seguridad de la información		x					Control existe de manera informal	No existe un proceso formal de análisis posterior a los incidentes para identificar causas o lecciones aprendidas. La entidad actúa únicamente para resolver el incidente inmediato, sin aprovechar la oportunidad de mejorar su postura de seguridad.	Establecer un procedimiento de revisión posterior a incidentes que permita documentar los hallazgos, extraer aprendizajes clave y actualizar políticas, controles y planes de respuesta, fortaleciendo la entidad frente a eventos de seguridad.
28	A.5.28 Recolección de evidencia		x					Control existe de manera informal	La organización no cuenta con procedimientos formales ni herramientas adecuadas para la recolección, preservación y manejo de evidencia digital en caso de incidentes de seguridad. Esto puede comprometer investigaciones internas o acciones legales.	Implementar políticas y procedimientos específicos para la gestión de evidencia digital, capacitar al personal relevante en técnicas de preservación forense y asegurar que toda la recolección cumpla con requisitos legales y de integridad de la información.
29	A.5.29 Seguridad de la información durante interrupciones			x				Planificado y ejecutado, sin medición formal	Existen algunas medidas básicas para proteger la información en situaciones de interrupciones operativas, pero carece de planes documentados y pruebas de continuidad que garanticen la protección efectiva de los datos críticos.	Formalizar un plan de continuidad de la seguridad de la información, integrarlo con el plan de continuidad del negocio y realizar simulaciones para validar su eficacia y mejorar la respuesta ante incidentes.
30	A.5.30 Preparación de las TIC para la continuidad de negocio			x				Planificado y ejecutado, sin medición formal	La entidad cuenta con acciones básicas para asegurar la continuidad de los servicios TIC, pero estas no están completamente formalizadas ni alineadas con un plan de continuidad de negocio integral.	Desarrollar, documentar y mantener actualizado un plan formal de continuidad de las TIC, con la finalidad de garantizar que los sistemas críticos puedan recuperarse eficazmente en caso de una interrupción.
31	A.5.31 Requisitos legales, estatutarios, regulatorios y contractuales					x		Monitoreado y medido	Se tiene establecido procedimientos para identificar y cumplir con los requisitos legales y contractuales en materia de seguridad de la información, y estos son aplicados de manera consistente en las operaciones.	Fortalecer el proceso de actualización mediante mecanismos de vigilancia normativa y auditorías internas, para asegurar que todos los cambios relevantes sean incorporados y se mantenga el cumplimiento.

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
32	A.5.32 Derechos de propiedad intelectual						x	Mejora Continua	La entidad tiene implementadas prácticas maduras para proteger los derechos de propiedad intelectual, incluyendo controles y una cultura organizacional que promueve el respeto y la protección de estos derechos.	Mantener la vigilancia sobre cambios legislativos y continuar con programas de capacitación para asegurar que el personal se comprometa con la protección de la propiedad intelectual en las operaciones.
33	A.5.33 Protección de registros			x				Planificado y ejecutado, sin medición formal	La entidad cuenta con acciones básicas para proteger los registros, como controles de acceso limitados y respaldos manuales; sin embargo, estos mecanismos son informales y no están plenamente documentados ni estandarizados.	Formalizar procedimientos de protección de registros, definir responsabilidades claras, establecer políticas de retención y destrucción segura, y asegurar que estos procesos sean comunicados y aplicados de manera consistente en toda la entidad.
34	A.5.34 Privacidad y protección de la PII (Información Identificable Personal)				x			Documentado, estandarizado y comunicado	Se ha implementado medidas adecuadas para proteger la información personal identificable (PII), con controles básicos de acceso. No obstante, las prácticas aún son parcialmente formales y no están completamente integradas en todos los procesos organizacionales.	Fortalecer la integración de estas prácticas mediante la implementación de controles más robustos, como auditorías, formación continua al personal, y la actualización constante de la política de privacidad y Seguridad de la Información.
35	A.5.35 Revisión independiente de la seguridad de la información	x						Incompleto	La entidad no cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI) formalmente establecido y, además, no realiza revisiones independientes de seguridad, o estas se llevan a cabo de manera informal y sin criterios definidos.	Desarrollar e implementar un SGSI basado en un marco reconocido como ISO 27001 y establecer un proceso formal de revisiones, utilizando personal idóneo, para identificar deficiencias y oportunidades de mejora en la gestión de la seguridad de la información.
36	A.5.36 Cumplimiento con las políticas, reglas y normas de la seguridad		x					Control existe de manera informal	No existen mecanismos formales para asegurar que el personal cumpla de manera consistente con las políticas y normas de seguridad establecidas.	Establecer un programa de concienciación, supervisión y auditoría interna que permita asegurar el cumplimiento de las políticas de seguridad de la información, incluyendo acciones correctivas ante incumplimientos.

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
37	A.5.37 Procedimientos operacionales documentados		x					Control existe de manera informal	No existen procedimientos formales ni documentados que guíen las operaciones relacionadas con la seguridad de la información. Las actividades críticas se realizan de manera informal y dependen del conocimiento individual del personal, lo que genera riesgos.	Desarrollar, aprobar y mantener actualizados los procedimientos operacionales documentados, asegurando que sean accesibles al personal relevante y que se revisen periódicamente para garantizar su eficacia.
A6 Controles Orientados a las Personas										
38	A.6.1. Revisión de antecedentes						x	Mejora Continua	Se cuenta con un proceso de selección bien estructurado, documentado y alineado con la gestión de riesgos. Las verificaciones previas incluyen validaciones legales y contractuales. No obstante, aún existe oportunidad de mejora en la automatización de controles o el uso de métricas para anticipar riesgos de seguridad de la información.	Incluir herramientas analíticas para predecir comportamientos de riesgo, reforzar la retroalimentación con otras áreas como recursos humanos y ciberseguridad, y consolidar indicadores clave de desempeño que permitan afinar el proceso de selección como parte integral del sistema de gestión de seguridad de la información.
39	A.6.2. Términos y condiciones de empleo.						x	Mejora Continua	La organización incluye cláusulas de seguridad en los contratos laborales, como deberes de confidencialidad y cumplimiento de políticas. Sin embargo, se puede optimizar el seguimiento a su cumplimiento.	Automatizar el control de estas cláusulas e integrarlas con procesos de recursos humanos y programas de concienciación para reforzar la cultura de seguridad.
40	A.6.3. Concientización, educación y capacitación sobre seguridad de la información.			x				Planificado y ejecutado, sin medición formal	la organización ha iniciado acciones básicas de concienciación y formación en seguridad, como charlas puntuales o distribución de material informativo. Sin embargo, estas actividades no son sistemáticas ni se aplican de forma regular a todos los empleados, y no existe un programa formal que evalúe su efectividad	Desarrollar e implementar un programa estructurado y continuo de capacitación en seguridad, adaptado a los diferentes roles dentro de la organización, con mecanismos de seguimiento y evaluación que permitan medir el nivel de conocimiento adquirido y su impacto en la cultura organizacional.

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
41	A.6.4. Proceso disciplinario				x			Documentado, estandarizado y comunicado	La organización tiene un proceso disciplinario para gestionar los incumplimientos relacionados con la seguridad de la información, pero su aplicación puede ser inconsistente o no completamente formalizada	Estandarizar el proceso disciplinario, asegurando su alineación con la política de seguridad de la Información, comunicarla a todos los niveles y establecer un seguimiento para garantizar su aplicación efectiva.
42	A.6.5. Responsabilidades después de la terminación o cambio de empleo					x		Monitoreado y medido	La organización gestiona de forma eficaz los procesos de terminación o cambio de funciones, asegurando la revocación o ajuste oportuno de accesos. Estos procedimientos están documentados y se aplican.	Fortalecer el uso de indicadores y análisis de datos para anticipar posibles fallos o retrasos en el proceso, y continuar promoviendo la mejora continua mediante revisiones periódicas.
43	A.6.6. Acuerdos de confidencialidad o no divulgación						x	Mejora Continua	La Personería Municipal de Armenia ha implementado de forma óptima acuerdos de confidencialidad y no divulgación, abarcando a todos los funcionarios, contratistas y partes externas que acceden a información sensible. La organización ha definido ciertas directrices de seguridad para el teletrabajo, como el uso de acceso remoto controlado, pero estas medidas aún no están integradas ni normalizadas en todos los procesos. La aplicación de controles varía entre áreas o usuarios, y no existe una supervisión sistemática del cumplimiento.	Mantener este nivel mediante revisiones periódicas del proceso y promoviendo una cultura organizacional basada en la confidencialidad y protección de la información como principio del SGSI.
44	A.6.7. Trabajo remoto				x			Documentado, estandarizado y comunicado	La organización ha definido ciertas directrices de seguridad para el teletrabajo, como el uso de acceso remoto controlado, pero estas medidas aún no están integradas ni normalizadas en todos los procesos. La aplicación de controles varía entre áreas o usuarios, y no existe una supervisión sistemática del cumplimiento.	Consolidar una política formal de teletrabajo que contemple aspectos como control de accesos, protección de datos, uso de redes seguras, seguridad física en ubicaciones remotas. Además, de asegurar la aplicación en toda la entidad, acompañada de capacitación y monitoreo.
45	A.6.8. Reportes de eventos de seguridad de la información			x				Planificado y ejecutado, sin medición formal	Existen iniciativas aisladas para reportar eventos de seguridad de la información, pero no se cuenta con un proceso formal ni con lineamientos documentados que estandaricen dicha actividad. La falta de procedimientos definidos y de herramientas adecuadas limita la capacidad de respuesta ante incidentes.	Desarrollar y formalizar un procedimiento institucional para el reporte de eventos de seguridad, socializarlo con todos los funcionarios, e incorporar mecanismos accesibles que faciliten su uso, como formularios digitales o canales específicos de comunicación.

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
A7 Controles Físicos										
46	A.7.1. Perímetros de seguridad física.					x		Monitoreado y medido	La organización ha implementado un control robusto del perímetro de seguridad física, utilizando múltiples capas de protección controles de videovigilancia 24/7 y patrullajes.	Seguir realizando monitoreos para identificar nuevas amenazas y mantener la actualización de las tecnologías de seguridad física para garantizar que el perímetro sea seguro.
47	A.7.2. Entrada física.				x			Documentado, estandarizado y comunicado	la organización ha implementado controles de acceso físicos mínimos, como puertas con cerraduras tradicionales, pero no existen medidas de seguridad más avanzadas ni un control sistemático de los accesos.	Establecer un sistema de control de acceso más robusto, como el uso de tarjetas electrónicas o autenticación biométrica para mejorar la seguridad física del área de Tecnologías de Información.
48	A.7.3. Protección de oficinas, habitaciones e instalaciones			x				Planificado y ejecutado, sin medición formal	La entidad ha implementado medidas de seguridad adecuadas, como el uso de sistemas de videovigilancia, controles de acceso restringidos. Sin embargo, se observa que algunas áreas no cuentan con medidas de seguridad rigurosas o sin revisiones periódicas.	Realizar una evaluación continua de las instalaciones para identificar puntos vulnerables, fortalecer las medidas de seguridad en áreas críticas y garantizar una revisión periódica de los controles implementados, asegurando su efectividad.
49	A.7.4. Monitoreo de seguridad física.			x				Planificado y ejecutado, sin medición formal	Se han establecido políticas y procedimientos básicos para el monitoreo de la seguridad física, incluyendo controles de acceso y vigilancia en las instalaciones más críticas. Sin embargo, se evidencian limitaciones en la cobertura y actualización de los sistemas de monitoreo.	Fortalecer la infraestructura de monitoreo mediante la actualización de equipos, ampliar la cobertura a todas las áreas sensibles, y establecer un registro sistemático de incidentes para facilitar la mejora continua.
50	A.7.5. Protección contra amenazas físicas y ambientales			x				Planificado y ejecutado, sin medición formal	La entidad ha implementado algunas medidas de protección contra amenazas externas y ambientales, como sistemas básicos de control contra incendios y acceso restringido a áreas críticas. Sin embargo, los controles no están completamente documentados.	Mejorar la documentación y auditoría de las medidas de protección, así como realizar una evaluación periódica de riesgos ambientales para asegurar que los controles sean adecuados frente a nuevas amenazas y posibles vulnerabilidades.

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
51	A.7.6. Trabajar en áreas seguras			x				Planificado y ejecutado, sin medición formal	Se ha definido áreas seguras para el trabajo con información sensible, pero las medidas de seguridad implementadas en estas áreas no están completamente estandarizadas ni monitoreadas de manera continua.	Formalizar un protocolo de seguridad para el trabajo en áreas seguras, incluyendo la implementación de monitoreo continuo y auditorías para asegurar que las medidas de protección sean consistentes y eficaces.
52	A.7.7. Escritorio y pantalla limpios		x					Control existe de manera informal	La entidad no tiene una política definida, además no se han establecido prácticas uniformes para asegurar que los usuarios mantengan sus escritorios y pantallas libres de información.	Mejorar la concientización mediante campañas de sensibilización y capacitar al personal sobre la realización de controles periódicos para asegurar la información.
53	A.7.8. Emplazamiento y protección de equipos				x			Documentado, estandarizado y comunicado	Los equipos están ubicados en sitios apropiados y protegidos contra riesgos físicos y ambientales. Sin embargo, se observa que no todos los controles están documentados formalmente ni se revisan de forma regular.	Establecer políticas más robustas y documentadas para la protección física de los equipos, además de implementar revisiones periódicas que aseguren el cumplimiento y la efectividad de estas medidas.
54	A.7.9. Seguridad de los activos fuera de las instalaciones			x				Planificado y ejecutado, sin medición formal	Existen lineamientos sobre el uso de equipos fuera de la organización, pero no se supervisan adecuadamente. Se observa una falta de controles específicos para proteger los datos en portátiles utilizados externamente	Establecer políticas claras y mecanismos de control que aseguren la protección de los activos fuera de las instalaciones, incluyendo cifrado, autenticación y monitoreo del uso.
55	A.7.10. Medios de almacenamiento		x					Control existe de manera informal	La organización ha comenzado a reconocer la necesidad de controlar el uso de medios removibles como USB, discos duros externos o CDs, pero no cuenta aún con políticas formales ni controles técnicos consistentes para su gestión.	Establecer una política sobre el uso de medios removibles, implementar controles técnicos y la restricción de acceso, y capacitar al personal sobre los riesgos asociados, promoviendo una gestión segura y controlada.
56	A.7.11. Utilidades de soporte				x			Documentado, estandarizado y comunicado	Se han definido políticas y procedimientos para la gestión de utilidades de soporte como energía, climatización y conectividad, los cuales están documentados y parcialmente implementados. Sin embargo, aún se evidencian debilidades en el monitoreo proactivo que podría afectar.	Fortalecer la implementación de estos procedimientos, integrar herramientas de monitoreo en tiempo real y establecer pruebas periódicas de resiliencia, con el fin de asegurar que las utilidades críticas respalden de forma efectiva los sistemas de información.

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
57	A.7.12. Seguridad del cableado.			x				Planificado y ejecutado, sin medición formal	Se ha implementado medidas físicas para proteger el cableado contra accesos no autorizados o daños accidentales. No obstante, se identifican oportunidades para mejorar la documentación y la supervisión del cableado.	Establecer controles de monitoreo periódico y reforzar la segregación del cableado de datos sensibles, garantizando su trazabilidad y protección frente a riesgos físicos.
58	A.7.13. Mantenimiento del equipo			X				Planificado y ejecutado, sin medición formal	Existen prácticas básicas de mantenimiento, pero no están formalizadas ni se aplican de manera consistente. No se cuenta con un plan documentado ni con registros sistemáticos de los mantenimientos realizados.	Establecer procedimientos formales de mantenimiento preventivo y correctivo, así como llevar un registro detallado que permita asegurar la disponibilidad y funcionamiento adecuado de los equipos.
59	A.7.14. Eliminación segura o reutilización del equipo					x		Documentado, estandarizado y comunicado	Existen procedimientos parciales para la eliminación segura o reutilización del equipo, sin una estandarización completa ni documentación formal que garantice el borrado seguro de datos antes de desechar o reutilizar dispositivos.	Establecer políticas formales que incluyan métodos seguros de eliminación de información, trazabilidad de los equipos retirados, con el fin de reducir riesgos de filtración de datos y cumplir ISO/IEC 27001
A8 Controles Tecnológicos										
60	A.8.1. Dispositivos terminales de usuario		x					Control existe de manera informal	la organización ha reconocido la necesidad de gestionar la seguridad de los dispositivos móviles, pero la implementación de una política formal es incipiente o parcial. La política existente, es básica y no cubre todos los aspectos relevantes, como la configuración de seguridad, el cifrado, el control de acceso.	Formalizar una política integral para dispositivos móviles que cubra todos los aspectos de seguridad, asegurando que se realicen controles de acceso, gestión de riesgos. Además, promover la concientización y garantizar el cumplimiento a través de la capacitación.
61	A.8.2. Derechos de acceso privilegiado			X				Planificado y ejecutado, sin medición formal	Existe cuentas con privilegios elevados, pero no cuenta con una política definida ni controles para su gestión. El otorgamiento de estos accesos se realiza sin un proceso formal de seguimiento, lo que aumenta el riesgo de uso indebido, acceso no autorizado o alteraciones no controladas en los sistemas críticos.	Establecer una política específica para la gestión de accesos privilegiados, implementar procedimientos de aprobación documentados, registrar las actividades realizadas con dichos privilegios y revisar periódicamente su necesidad y uso, con el fin de fortalecer la seguridad.

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
62	A.8.3. Restricción de acceso a la información		x					Control existe de manera informal	Existen esfuerzos para restringir el acceso a la información, generalmente configurados por el área de TI según criterios operativos, pero sin una política formal definida basada en el principio de mínimo privilegio. Esta falta de estandarización puede dar lugar a accesos no autorizados a información sensible.	Establecer una política de control de acceso alineada con los roles y responsabilidades dentro de la entidad, implementar controles técnicos adecuados, y asegurar que los accesos se otorguen en función de la necesidad operativa, revisándolos periódicamente para garantizar su vigencia.
63	A.8.4. Acceso al código fuente					x		Monitoreado y medido	la organización ha implementado un control para la gestión de accesos al código fuente de los programas. Los accesos están restringidos mediante control de acceso basados en roles, asegurando que solo el personal autorizado pueda modificar o consultar el código fuente.	Continuar mejorando la seguridad mediante la implementación de políticas de revisión periódica de accesos y considerar la adopción de herramientas de protección de código, como cifrado o sistemas de protección contra el robo de propiedad intelectual.
64	A.8.5. Autenticación segura		x					Control existe de manera informal	La entidad ha implementado algunas medidas para proteger el acceso a sus sistemas. Sin embargo, no están respaldadas por una política formal ni se aplican en todos los entornos. Faltan mecanismos como bloqueo de cuentas tras múltiples intentos fallidos, autenticación multifactor	Formalizar un procedimiento de ingreso seguro que incluya controles técnicos y administrativos, asegurar su aplicación en todos los sistemas críticos, y fomentar la capacitación del personal en prácticas seguras de acceso.
65	A.8.6. Gestión de capacidad			x				Planificado y ejecutado, sin medición formal	La organización ha comenzado a implementar prácticas básicas para gestionar la capacidad de sus sistemas, pero aún no existen procesos formales ni documentados. La evaluación de la capacidad no se realizan análisis proactivos para anticipar necesidades futuras.	Desarrollar e implementar procesos más estructurados y documentados para la gestión de la capacidad, incorporando una planificación que permita anticipar las demandas futuras de los sistemas. Además, es crucial establecer un sistema de monitoreo.

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
66	A.8.7. Protección contra malware.		x					Control existe de manera informal	Se tiene medidas básicas de protección contra malware, pero éstas son limitadas y no están formalmente implementadas o monitoreadas. No existe un enfoque integral ni políticas claras sobre la detección y respuesta ante amenazas de malware.	Desarrollar e implementar políticas y procedimientos formales de protección contra malware, que incluyan soluciones de antivirus actualizadas, sistemas de detección de intrusiones, y medidas preventivas en todos los puntos críticos de la infraestructura. Implementar un proceso formal de gestión de vulnerabilidades que incluya la identificación, evaluación y priorización de vulnerabilidades técnicas, así como la aplicación de parches y actualizaciones de seguridad de manera oportuna. Además, se debe establecer un ciclo regular de auditorías.
67	A.8.8. Gestión de vulnerabilidades técnicas		x					Control existe de manera informal	No existen procesos formales establecidos para identificar, evaluar o mitigar las vulnerabilidades técnicas de forma sistemática. Las acciones correctivas se toman de manera reactiva y no se realizan evaluaciones periódicas.	Formalizar y documentar los procesos de gestión de configuración, asegurando su aplicación en toda la infraestructura tecnológica. Además, establecer un control más riguroso sobre los cambios de configuración, incluyendo su revisión.
68	A.8.9. Gestión de configuración			x				Planificado y ejecutado, sin medición formal	Se ha implementado algunos controles básicos para la gestión de configuraciones. Sin embargo, los procesos son parcialmente formales y no siempre se aplican de manera consistente en todos los entornos o sistemas.	Desarrollar e implementar una política formal de eliminación de información que incluya procedimientos claros y seguros para la destrucción de datos en todos los entornos, asegurando su cumplimiento mediante auditorías periódicas.
69	A.8.10. Borrado de información			x				Planificado y ejecutado, sin medición formal	Se ha implementado prácticas para la eliminación de información, como el uso de métodos de borrado. Sin embargo, no existe una política formalizada ni un proceso para garantizar que la eliminación de datos se realice de manera segura en todos los sistemas.	

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
70	A.8.11. Enmascaramiento de datos		x					Control existe de manera informal	No se ha implementado medidas de enmascaramiento de datos en sus procesos. La protección de datos sensibles no está suficientemente controlada, y no existen procedimientos claros ni herramientas implementadas para garantizar que los datos sean enmascarados en entornos no productivos.	Implementar soluciones de enmascaramiento de datos para proteger la información sensible. Además, es crucial desarrollar políticas y procedimientos que regulen el enmascaramiento de datos asegurando que los datos sean adecuadamente protegidos y que se cumpla con las regulaciones de privacidad.
71	A.8.12. Prevención de filtración de datos		x					Control existe de manera informal	No se ha implementado mecanismos específicos para prevenir la fuga de datos. No existen políticas formalizadas ni herramientas adecuadas para monitorear ni restringir el acceso o la transferencia no autorizada de información sensible.	Establecer políticas de prevención de fuga de datos que incluyan el monitoreo de los canales de comunicación y la implementación de controles técnicos que restrinjan la transferencia de datos sensibles. Además, de realizar capacitaciones periódicas al personal sobre las mejores prácticas de seguridad. Formalizar y documentar los procedimientos de copia de seguridad, asegurando que se realicen de manera consistente en todos los sistemas críticos. Además, es fundamental implementar pruebas de restauración para garantizar la fiabilidad de los respaldos.
72	A.8.13. Respaldo de información			x				Planificado y ejecutado, sin medición formal	Se ha implementado procesos básicos de copia de seguridad, como la realización periódica de respaldos. Sin embargo, estos procesos no están completamente documentados ni formalizados, y no se realiza una verificación regular de la integridad y recuperación de los datos.	
73	A.8.14. Redundancia de las instalaciones de procesamiento de información			x				Planificado y ejecutado, sin medición formal	Se ha implementado algunas medidas básicas de redundancia, como la duplicación de equipos en ciertos entornos críticos. Sin embargo, la implementación no es completa ni consistente en todas las áreas, y no se han realizado pruebas para verificar la efectividad de la redundancia en situaciones de falla.	Implementar medidas de redundancia en todas las instalaciones críticas de procesamiento de información. Esto incluye la configuración de sistemas redundantes para garantizar la continuidad del servicio y la realización de pruebas para asegurar que los mecanismos de recuperación funcionen.

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
74	A.8.15. Registración		x					Control existe de manera informal	No se cuenta con un sistema formal de registros de seguridad. Los eventos no se registran de manera consistente, y no existe una política clara sobre qué información debe ser registrada, cómo debe almacenarse ni cuánto tiempo, lo que dificulta el análisis de los incidentes.	Establecer una política formal de gestión de registros que defina los tipos de eventos que deben registrarse, los responsables del monitoreo, los mecanismos de almacenamiento seguro y los períodos de retención. Además, de implementar herramientas de registro (logs) automatizados.
75	A.8.16. Actividades de supervisión		x					Control existe de manera informal	No se cuenta con un proceso estructurado para monitorear de forma continua las actividades relacionadas con la seguridad de la información. Las acciones de seguimiento son esporádicas, sin herramientas ni procedimientos definidos para la detección de incidentes.	Implementar un sistema de monitoreo que incluya herramientas de supervisión automatizada, alertas en tiempo real y procedimientos formales para la detección y respuesta a eventos de seguridad. Además, es esencial definir responsabilidades claras.
76	A.8.17. Sincronización de reloj (clock)			x				Planificado y ejecutado, sin medición formal	Se ha implementado una sincronización básica de los relojes de algunos sistemas con servidores, pero no existe una política formal ni un control uniforme en todos los equipos. Esto puede generar inconsistencias en los registros de eventos y afectar la traza de incidentes	Establecer una política formal de sincronización de tiempo que asegure que todos los sistemas críticos estén configurados para sincronizarse automáticamente con fuentes de tiempo confiables y seguras.
77	A.8.18. Uso de programas de utilidad privilegiados.				x			Documentado, estandarizado y comunicado	La entidad ha implementado controles adecuados para el uso de programas especializados (ERP) privilegiados, incluyendo la restricción de acceso a estos solo para personal autorizado y la supervisión de su uso.	Mejorar el monitoreo y auditoría de estos programas, implementando alertas de seguridad para detectar accesos no autorizados o usos indebidos, y asegurarse de que todos los accesos sean documentados.
78	A.8.19. Instalación de software en sistemas operacionales			x				Planificado y ejecutado, sin medición formal	Se ha establecido controles básicos para la instalación de software, como restricciones de permisos para usuarios finales. Sin embargo, no existe un procedimiento formalizado lo que generar riesgos en instalaciones vulnerables.	Implementar una política formal de gestión de instalaciones de software, que incluya procesos de autorización, registro y control del software instalado en todos los sistemas operativos. Además, en la política se debe prevenir la ejecución de software malicioso.

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
79	A.8.20. Seguridad de redes		x					Control existe de manera informal	La entidad permite el acceso a redes y servicios sin contar con políticas claras ni controles definidos que regulen dicho acceso. Las configuraciones de red no están estandarizadas y el control de usuarios es limitado, lo que expone a la organización a riesgos de accesos indebidos y fugas de información.	establecer una política formal de acceso a redes y servicios, definir controles de autenticación y autorización apropiados, y aplicar medidas técnicas como firewalls, VLANs y monitoreo de tráfico, asegurando una gestión más segura y estructurada del entorno de red.
80	A.8.21. Seguridad de los servicios de red.		x					Control existe de manera informal	Carece de controles formales para garantizar la seguridad de los servicios de red. No se cuenta con políticas definidas ni mecanismos para proteger la infraestructura de red, lo que expone a la entidad a riesgos como accesos no autorizados o ataques a los servicios críticos.	Establecer e implementar una política de seguridad de red que incluya el uso de firewalls, segmentación de red, sistemas de detección y prevención de intrusos, y cifrado de datos en tránsito. Además, es fundamental realizar evaluaciones de riesgos en la red.
81	A.8.22. Segregación de redes		x					Incompleto	No se ha implementado medidas formales de segregación de redes. La infraestructura de red es plana, sin separación entre segmentos críticos como la red administrativa, de usuarios o servidores, lo que incrementa los riesgos.	Diseñar e implementar una arquitectura de red segmentada que separe los entornos según su nivel de sensibilidad. Esto debe incluir el uso de VLANs, firewalls internos y reglas de acceso entre segmentos. Adicionalmente, se debe establecer políticas de control de red.
82	A.8.23. Filtrado web					x		Monitoreado y medido	Al estar tercerizado el servicio de internet, la entidad depende del proveedor para la aplicación y actualización de ciertas reglas de filtrado, lo que puede limitar el control directo y la respuesta oportuna ante nuevas amenazas.	Establecer reglas según las necesidades internas. Asimismo, se debe solicitar informes regulares de actividad web y eventos de seguridad relacionados, con el fin de mantener una supervisión activa.
83	A.8.24. Uso de criptografía		x					Incompleto	No se ha establecido una política formal sobre el uso de controles criptográficos. No existen directrices claras sobre cuándo y cómo aplicar la criptografía para proteger la información sensible, ni se han identificado los procesos o activos que requieren este tipo de protección.	Desarrollar y formalizar una política de criptografía que defina los requisitos para su implementación, incluyendo métodos criptográficos apropiados, la gestión de claves y la protección de datos tanto en reposo como en tránsito.

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
84	A.8.25. Desarrollo seguro del ciclo de vida						x	Mejora Continua	Dado que el desarrollo de software es tercerizado, existe una dependencia con el proveedor externo para asegurar que estos controles se apliquen con el mismo nivel de rigor, lo cual requiere verificación continua.	Mantener una supervisión activa mediante revisiones técnicas, participación en etapas clave del desarrollo y verificación independiente del cumplimiento de los controles de seguridad establecidos.
85	A.8.26. Requerimientos de seguridad en aplicaciones						x	Monitoreado y medido	Al estar el desarrollo de software tercerizado mediante contrato, se identifican oportunidades de mejora en la validación del cumplimiento de estos requisitos por parte del proveedor.	Establecer mecanismos de seguimiento, como auditorías técnicas y la revisión de entregables, para asegurar que los requisitos de seguridad sean efectivamente aplicados durante todo el ciclo de desarrollo.
86	A.8.27. Principios de arquitectura de sistemas e ingeniería seguras						x	Monitoreado y medido	Dado que el desarrollo de software está tercerizado mediante contrato, se identifica una dependencia del proveedor externo para mantener estos principios, lo que requiere mecanismos de verificación adicionales.	Incorporar en los contratos cláusulas que obliguen al proveedor a aplicar principios de ingeniería segura y a documentar la arquitectura de los sistemas desarrollados. Se deben establecer revisiones técnicas.
87	A.8.28. Codificación segura						x	Monitoreado y medido	Al estar el desarrollo tercerizado mediante contrato, la implementación efectiva de estos estándares depende de la correcta ejecución por parte del proveedor, lo que requiere monitoreo constante.	Fortalecer los acuerdos contractuales incorporando requisitos específicos sobre codificación segura basados en marcos como OWASP, así como la obligación de realizar análisis de código estático y dinámico.
88	A.8.29. Pruebas de seguridad en desarrollo y aceptación				x			Documentado, estandarizado y comunicado	Como se encuentra tercerizado el desarrollo mediante contrato, la responsabilidad operativa recae en el proveedor, lo que requiere asegurar que estas pruebas se realicen conforme a los estándares establecidos por la organización	Formalizar en los contratos la obligatoriedad de ejecutar pruebas de seguridad durante todo el ciclo de desarrollo, incluyendo pruebas de penetración, escaneo de vulnerabilidades y validaciones automatizadas.
89	A.8.30. Desarrollo tercerizado						x	Monitoreado y medido	Se gestiona el desarrollo subcontratado, incluyendo evaluaciones de proveedores, sin embargo, aún existen oportunidades de mejora en la automatización del monitoreo y en la trazabilidad de las actividades del proveedor.	Fortalecer los mecanismos de control mediante el uso de plataformas que permitan un seguimiento en tiempo real del desarrollo subcontratado, como la implementación de indicadores de desempeño (KPIs).

Tabla 23 (Continuación)*Evaluación de Controles ISO 27001 con COBIT*

No.	Control ISO 27001	Nivel COBIT						Descripción del nivel	Evidencia /Observaciones	Recomendaciones
		0	1	2	3	4	5			
90	A.8.31. Separación de los entornos de desarrollo, prueba y producción				x			Documentado, estandarizado y comunicado	Persisten algunas limitaciones en la visibilidad y control directo sobre la infraestructura del proveedor, lo que podría generar riesgos si no se asegura el cumplimiento estricto de la separación en todas las fases del desarrollo.	Reforzar los acuerdos contractuales incluyendo requisitos específicos sobre la separación de entornos, y establecer mecanismos de supervisión técnica, como revisiones, auditorías con evidencias.
91	A.8.32. Gestión de cambios			x				Planificado y ejecutado, sin medición formal	Se ha establecido procedimientos para la gestión de cambios, como la autorización previa de algunas modificaciones. Sin embargo, los procedimientos no se aplican y no se realiza una evaluación de riesgos.	Fortalecer el proceso de gestión de cambios mediante la estandarización y aplicación de las etapas clave: solicitud, análisis de impacto, aprobación, implementación controlada y revisión posterior.
92	A.8.33. Información de prueba				x			Documentado, estandarizado y comunicado	Al estar el desarrollo de software subcontratado, se observa una limitada visibilidad sobre cómo el proveedor gestiona la información de prueba.	Establecer cláusulas contractuales claras que obliguen al proveedor a aplicar controles estrictos sobre el uso de información en entornos de prueba, incluyendo dato sensible
93	A.8.34. Protección de los sistemas de información durante las pruebas de auditoría			x				Planificado y ejecutado, sin medición formal	No existen procedimientos formalizados ni controles técnicos robustos que aseguren la protección integral de los sistemas durante estos procesos.	Implementar procedimientos específicos para la ejecución segura de auditorías, incluyendo controles de acceso temporales, entornos de prueba controlados.

Nota. Evaluación de controles ISO 27001 con COBIT (Autoría Propia)

Análisis General del Estado de Madurez

Tabla 24

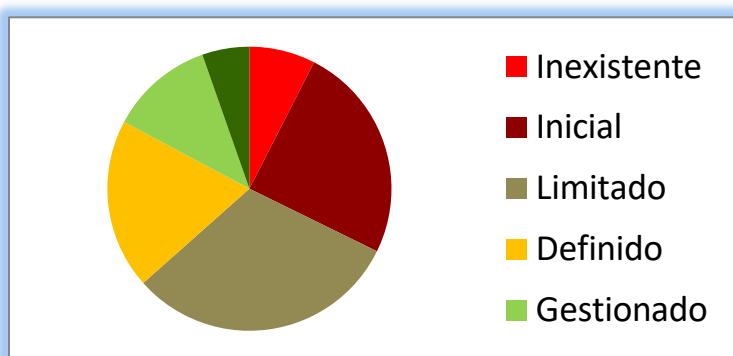
Status Controles ISO 27001

Estatus	Significado	Nivel de Madurez
Inexistente	Ausencia completa de una política, procedimiento, control, etc. Legibles	8%
Inicial	El desarrollo apenas ha comenzado y requerirá un trabajo significativo para satisfacer los requisitos	25%
Limitado	Progresando bien pero no completado aún	31%
Definido	El desarrollo está más o menos completo, aunque con ausencia de detalles y/o no está aún implementado, en cumplimiento vigente ni activamente avalado por la alta dirección.	19%
Gestionado	El desarrollo está completo, el proceso / control ha sido implementado y recientemente comenzó a operar	12%
Optimizado	El requisito está plenamente conforme, está plenamente operativo como se espera, está siendo activamente supervisado y mejorado, y hay evidencia sustancial para demostrar todo lo antedicho a los auditores	5%

Nota. Status Controles ISO 27001 (Autoría Propia)

Figura 13

Nivel de Madurez Controles ISO 27001



Nota. Nivel de Madurez Controles ISO 27001 (Autoría Propia)

Controles en niveles bajos de madurez (Inexistente, Inicial y Limitado) representan el 64% del total:

- Inexistente (8%): Aunque es un porcentaje relativamente bajo, la ausencia total de ciertos controles es crítica, ya que estos representan puntos ciegos de alto riesgo en el sistema de gestión de seguridad de la información.
- Inicial (25%): Una cuarta parte de los controles se encuentra en etapas muy tempranas, lo que indica que requieren esfuerzos significativos de desarrollo e integración en la gestión institucional.
- Limitado (31%): Es el grupo más numeroso. Los controles están en proceso, pero aún no se han completado, lo que sugiere una necesidad urgente de seguimiento, recursos y compromiso institucional para su maduración.
- Controles con desarrollo estructurado (Definido y Gestionado) suman el 31%:
- Definido (19%): Aunque ya hay documentación o políticas formales, la falta de implementación o validación por parte de la alta dirección limita su efectividad real.
- Gestionado (12%): Estos controles ya están operativos, pero posiblemente aún no se ha consolidado una supervisión sólida ni procesos de mejora continua.
- Controles altamente maduros (Optimizado) apenas representan el 5%, lo cual evidencia que solo una mínima parte cumple de manera plena con los requisitos del estándar, incluyendo monitoreo activo, mejora continua y trazabilidad.

Análisis del Nivel de Madurez por Controles de Seguridad de la Información

A5 Controles Organizacionales

Controles en nivel Inexistente (6 controles): Controles como la definición de roles y responsabilidades (A.5.2), segregación de tareas (A.5.3), contactos con grupos de interés (A.5.6), uso de servicios en la nube (A.5.23), y revisión independiente de seguridad (A.5.35) están completamente ausentes. Esto representa un alto riesgo organizacional, ya que compromete la gobernanza, el monitoreo externo y la seguridad en entornos tercerizados o distribuidos.

- Controles en nivel Inicial (11 controles): Controles como gestión de incidentes (A.5.25 - A.5.28), inteligencia de amenazas (A.5.7), o responsabilidades de gestión (A.5.4) están en etapas muy tempranas de desarrollo. Denota una ausencia de procedimientos claros y falta de implementación activa, especialmente en gestión de incidentes, un área crítica.

- Controles en nivel Limitado (12 controles): Muchos controles técnicos y operacionales, como autenticación (A.5.17), control de acceso (A.5.15), continuidad del negocio (A.5.30) y protección de registros (A.5.33), tienen avances, pero están aún incompletos. Indican progreso, pero es necesario acelerar su formalización e implementación para que sean efectivos y auditables.

- Controles Definidos (9 controles): Controles como políticas de seguridad (A.5.1), clasificación de información (A.5.12), seguridad en contratos y proveedores (A.5.19-A.5.20) están formalizados y documentados. Aún necesitan validación, implementación plena y respaldo de la alta dirección para ser gestionados.

- Controles Gestionados (3 controles): Se encuentran en esta categoría aspectos como el inventario de activos (A.5.9), devolución de activos (A.5.11) y requisitos legales

(A.5.31), lo cual indica que algunos procesos clave ya operan regularmente. Esto refleja un nivel positivo de avance en gestión documental y cumplimiento normativo.

- Control Optimizado (1 control): Solo el control sobre derechos de propiedad intelectual (A.5.32) alcanza el nivel más alto, lo que evidencia que la mejora continua y el monitoreo sistemático están muy poco presentes en los controles organizacionales.

A6. Controles Orientados a las Personas

Controles en nivel Optimizado (3 controles): A.6.1 Revisión de antecedentes, A.6.2 Términos y condiciones de empleo y A.6.6 Acuerdos de confidencialidad o no revelación muestran un nivel excelente de implementación. Esto indica una gestión madura de los riesgos antes y durante la relación laboral, así como la adecuada protección de la información a través de acuerdos legales sólidos. Son evidencia de un entorno laboral con buen control de acceso basado en confianza y legalidad, y prácticas preventivas bien institucionalizadas.

- Controles Definidos (2 controles): A.6.4 Proceso disciplinario y A.6.7 Trabajo remoto están documentados y formalizados, pero aún necesitan ser plenamente implementados y respaldados activamente por la alta dirección. Esto sugiere que existen políticas, pero no necesariamente se aplican de forma sistemática o auditada.

- Controles en nivel Limitado (2 controles): A.6.3 Concientización, educación y entrenamiento en seguridad y A.6.8 Reportes de eventos de seguridad muestran avances iniciales, pero aún no consolidan su operación como parte del día a día. Representa un riesgo importante en la prevención y detección temprana de incidentes, pues el personal podría no estar suficientemente preparado ni motivado para reportar o responder adecuadamente.

- Control Gestionado (1 control): A.6.5 Responsabilidades luego de la finalización o cambio de empleo está en funcionamiento regular, lo cual garantiza el control de accesos y deberes posteriores al contrato. Este control es crucial para evitar fugas de información y mantener la trazabilidad y responsabilidad de excolaboradores.

A7. Controles físicos

Control Gestionado (1 control): A.7.1 Perímetros de seguridad física.

Indica que los accesos externos están bien definidos y con medidas estables de control. Fortalece la primera línea de defensa frente a intrusiones o accesos no autorizados.

- Controles Definidos (4 controles): A.7.2 Entrada física, A.7.8 Emplazamiento y protección de equipos, A.7.11 Servicios de suministro, A.7.14 Eliminación segura de equipos. Estos controles tienen políticas o procedimientos documentados, pero podrían no estar totalmente implementados o auditados. Se observa intención estructural de control, pero no se asegura una ejecución efectiva o continua.

- Controles Limitados (7 controles): Controles como A.7.3, A.7.4, A.7.5, A.7.6, A.7.9, A.7.12, A.7.13 están en etapas básicas de implementación. Reflejan una protección física reactiva y parcial, con poco monitoreo, mantenimiento preventivo débil y escasa preparación ante amenazas ambientales. La seguridad interna de instalaciones, equipos y cableado requiere atención urgente, pues son puntos vulnerables explotables.

- Controles Iniciales (2 controles): A.7.7 Escritorio y pantalla limpios, A.7.10 Medios de almacenamiento. Estos controles críticos están prácticamente ausentes o en una fase de adopción mínima. Implican un alto riesgo de fugas accidentales de información confidencial por desorganización, falta de hábitos seguros o exposición visual de datos. La gestión de medios (USB, discos, backups físicos) es un punto ciego importante.

A8. Controles tecnológicos

Altamente maduros (Gestionado/Optimizado) 8 controles: Controles: A.8.4, A.8.23,

A.8.25,

A.8.26, A.8.27, A.8.28, A.8.30. Áreas fuertes:

Desarrollo seguro, arquitectura de software y filtrado web. Implica una cultura técnica consolidada en entornos de desarrollo y buenas prácticas en el ciclo seguro del software por el outsourcing del servicio.

- Definido 4 controles: Controles: A.8.18, A.8.29, A.8.31, A.8.33 Se han establecido procedimientos básicos en uso de herramientas privilegiadas y separación de entornos, aunque aún se requiere validación de su efectividad.

- Limitado 11 controles: Controles: A.8.2, A.8.6, A.8.9, A.8.10, A.8.13, A.8.14, A.8.17, A.8.19, A.8.32, A.8.34. Se nota un esfuerzo parcial en operaciones críticas como respaldo, sincronización, y gestión de cambios, pero con riesgos por falta de control completo o monitoreo eficaz. Estos controles requieren fortalecimiento para mejorar la resiliencia tecnológica.

- Inicial 13 controles: Controles: A.8.1, A.8.3, A.8.5, A.8.7, A.8.8, A.8.11, A.8.12, A.8.15, A.8.16, A.8.20, A.8.21. Áreas débiles: dispositivos finales, autenticación, malware, redes, monitoreo, registro y acceso a información. Estos aspectos son críticos para la ciberseguridad diaria y representan las mayores vulnerabilidades actuales.

- Inexistente 2 controles: Controles: A.8.22 (Segregación de redes), A.8.24 (Uso de criptografía). La falta total de criptografía y segmentación de red implica un riesgo grave de compromisos internos o externos. Son controles base en cualquier arquitectura de defensa.

Mejoras en la Implementación de Controles de Seguridad

En relación con los controles organizacionales establecidos en la norma ISO/IEC 27001 (A.5), se identifican oportunidades clave de mejora orientadas a fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI). Es fundamental formalizar las políticas de seguridad de la información mediante su adecuada documentación, aprobación por la alta dirección y difusión a todo el personal involucrado, garantizando así su cumplimiento. Asimismo, es necesario asignar roles y responsabilidades de seguridad de manera clara, estableciendo responsables definidos para la gestión de riesgos, continuidad del negocio y cumplimiento normativo.

Otro aspecto prioritario es optimizar la gestión de riesgos, implementando metodologías sistemáticas y actualizadas para identificar, evaluar y tratar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información. Se recomienda establecer un programa estructurado de auditorías internas y revisiones por la dirección, que permita verificar el grado de cumplimiento de los controles y la mejora continua del SGSI. Estas acciones permitirán alinear los controles organizacionales con los requisitos de la norma y fortalecer la gobernanza de la seguridad en la entidad.

Así mismo, los controles orientados a las personas (A.6) de la norma ISO/IEC 27001 requieren mejoras clave para fortalecer la seguridad institucional. Es fundamental implementar programas continuos de capacitación en ciberseguridad, incluyendo simulacros de phishing, y promover una cultura de reporte de incidentes mediante canales accesibles y seguros. Además, deben actualizarse las políticas de trabajo remoto con medidas como cifrado y acceso seguro, y reforzarse el proceso disciplinario con acciones claras frente a incumplimientos. Estas acciones

ayudarán a consolidar un entorno más consciente y responsable frente a la seguridad de la información.

Por consiguiente, los controles físicos (A.7) requieren un fortalecimiento integral para garantizar la protección de los activos frente a amenazas físicas y ambientales. Es fundamental implementar medidas avanzadas como vigilancia electrónica permanente, sistemas de control de acceso biométrico y una gestión rigurosa de visitantes, asegurando la trazabilidad y restricción de accesos no autorizados. Además, deben aplicarse políticas estrictas de escritorio limpio y supervisión constante, especialmente en áreas sensibles. El almacenamiento de medios con información confidencial debe realizarse en espacios seguros, con acceso controlado. Finalmente, es prioritario revisar y proteger el cableado estructurado y mejorar la seguridad de las áreas críticas, garantizando la continuidad operativa y la confidencialidad de la información.

Por último, Para garantizar una protección tecnológica robusta conforme a los controles A.8 de la ISO/IEC 27001, es esencial adoptar un enfoque integral que combine tecnologías avanzadas con una gestión efectiva. La implementación de soluciones EDR (Endpoint Detection and Response) y antivirus centralizados permite una detección proactiva de amenazas, respuesta automatizada ante incidentes y visibilidad centralizada del entorno. La gestión de vulnerabilidades debe ser sistemática, mediante escaneos técnicos regulares, evaluación del riesgo asociado a cada hallazgo y aplicación de parches bajo políticas de cambio controlado.

La autenticación multifactor (MFA) debe ser obligatoria para todo acceso administrativo y sistemas sensibles, integrando tokens físicos o aplicaciones móviles seguras. Es fundamental emplear criptografía robusta (como AES-256 para cifrado de datos y RSA-2048 para intercambio seguro de claves), asegurando el cifrado de datos en tránsito (TLS 1.2 o superior) y en reposo,

especialmente en dispositivos móviles, respaldos y bases de datos. Además, la segmentación lógica de redes mediante VLANs y firewalls internos contribuye a contener brechas y limitar movimientos laterales. Finalmente, se debe reforzar la seguridad de redes inalámbricas con WPA3, limitar el uso de SSIDs abiertos y revisar periódicamente la configuración de routers y switches, implementando listas de control de acceso (ACL), desactivando servicios innecesarios y habilitando registros de auditoría para detectar anomalías.

Formular las Políticas de Seguridad de la Información, así como el Alcance del SGSI, la Identificación de los Procesos Críticos, los Servicios Involucrados y las Partes Interesadas

El diseño del Sistema de Gestión de Seguridad de la Información (SGSI) para la Personería Municipal de Armenia se llevó a cabo con base en los principios y requisitos establecidos por la norma internacional ISO/IEC 27001, adaptados al contexto organizacional, tecnológico y normativo de la entidad. Este diseño responde a la necesidad de contar con un marco estructurado que permita gestionar de manera proactiva los riesgos que amenazan la seguridad de la información, especialmente en una institución que maneja datos sensibles de la ciudadanía.

El proceso de diseño partió de un diagnóstico previo que identificó los activos críticos, las amenazas principales y las brechas existentes frente a los controles recomendados por el Anexo A de la norma. A partir de ello, se estructuró un conjunto coherente de políticas y procedimientos de seguridad orientados a establecer directrices claras para la protección de la información en sus diferentes fases: creación, procesamiento, almacenamiento, transmisión y eliminación.

El SGSI propuesto incluye además un modelo organizativo con la asignación de roles y responsabilidades claras en materia de seguridad, alineado con los principios de gobernanza de TI del marco COBIT. Este diseño no solo busca responder a los requerimientos normativos, sino también fortalecer la confianza institucional y garantizar que la información se maneje bajo criterios sólidos de seguridad, resiliencia y responsabilidad.

Alcance del SGSI

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) diseñado para la Personería Municipal de Armenia contempla la protección de los activos de información relacionados con los procesos misionales, administrativos y de atención al ciudadano, teniendo en cuenta su importancia crítica para el cumplimiento de las funciones constitucionales y legales de la entidad.

Este diseño considera los riesgos internos y externos identificados durante el diagnóstico, las capacidades tecnológicas disponibles, las obligaciones normativas aplicables a entidades públicas, y los compromisos institucionales en materia de protección de datos personales y transparencia.

En consecuencia, el alcance se limita a la fase de diseño del SGSI, alineado con la norma ISO/IEC 27001, e incluye la definición de políticas, procedimientos, roles, controles y mecanismos de seguimiento aplicables a los procesos y activos de información gestionados directamente por la Personería. Este diseño no contempla la implementación operativa del sistema, pero deja estructurado un modelo base para su futura ejecución y mejora continua.

Procesos

La seguridad de la información es un aspecto transversal y crítico en todos los procesos de la Personería Municipal de Armenia, ya que la entidad maneja información sensible que involucra derechos fundamentales de la ciudadanía, registros legales, y datos personales. El diseño del Sistema de Gestión de Seguridad de la Información (SGSI), alineado con la norma ISO/IEC 27001, contempla la identificación, análisis y tratamiento de los riesgos que puedan afectar estos procesos. A continuación, se describen los principales procesos cubiertos en el alcance del diseño del SGSI.

Procesos Misionales: Los siguientes son los procesos misionales de la entidad:

- Atención al ciudadano: incluye la recepción, análisis y seguimiento de peticiones, quejas, reclamos y denuncias.
- Defensa y promoción de los derechos humanos: gestión de casos relacionados con vulneración de derechos fundamentales.
- Intervención en procesos judiciales y administrativos: manejo de documentación y soporte legal en nombre de la ciudadanía.

Procesos de Apoyo: Los procesos de apoyo son los que se mencionan a continuación:

- Gestión documental: administración de archivos físicos y digitales que contienen información confidencial y sensible.
- Talento humano: manejo de datos personales y laborales del personal vinculado a la entidad.
- Recursos físicos y financieros: control de inventarios, compras, contrataciones y ejecución presupuestal.

Procesos Estratégicos: Los procesos estratégicos se relacionan a continuación:

- Planeación institucional: definición de metas, programas y proyectos que orientan la gestión de la Personería.
- Evaluación y control: seguimiento al cumplimiento de objetivos, gestión de indicadores y auditorías internas.
- Gestión de tecnologías de la información: soporte técnico, administración de redes, sistemas de información y protección de la infraestructura tecnológica.

Cada uno de estos procesos será abordado en el diseño del SGSI mediante la identificación de activos de información, análisis de vulnerabilidades, evaluación de controles actuales y definición de políticas y procedimientos que aseguren su protección. Esto permitirá establecer un modelo estructurado de seguridad que contribuya al cumplimiento legal, la eficiencia operativa y la confianza ciudadana.

Servicios

La Personería Municipal de Armenia desempeña un papel fundamental como entidad del Ministerio Público a nivel local, brindando servicios esenciales orientados a la defensa de los derechos humanos, el control administrativo y la atención al ciudadano. La seguridad de la información es crítica para garantizar la confianza, legalidad y confidencialidad en la prestación de estos servicios, especialmente al tratar datos sensibles y actuaciones de interés público. Los principales servicios que presta la Personería y que serán tenidos en cuenta en el SGSI son:

- Atención y orientación al ciudadano: Recepción y gestión de peticiones, quejas, reclamos, sugerencias y denuncias (PQRSD), que implican el tratamiento de información personal, sensible y confidencial.

- Defensa y promoción de los derechos humanos: Intervención en casos de presuntas vulneraciones a derechos fundamentales, lo que conlleva el manejo de información jurídica y social de alta sensibilidad.
- Intervención en procesos disciplinarios y judiciales: Participación como representante del Ministerio Público en actuaciones judiciales, con acceso y manejo de expedientes y pruebas documentales.
- Vigilancia de la función pública: Control de la conducta de servidores públicos del municipio, gestión de denuncias y procesos disciplinarios, con documentación confidencial y administrativa.
- Participación ciudadana y control social: Promoción de mecanismos de participación y control comunitario, con apoyo en plataformas tecnológicas para la interacción ciudadana.

El diseño del SGSI tendrá en cuenta estos servicios para identificar los activos de información involucrados, evaluar los riesgos asociados y establecer políticas y controles de seguridad que aseguren la confidencialidad, integridad y disponibilidad de la información, alineados con los principios de la norma ISO/IEC 27001.

Partes Interesadas

En el contexto del diseño del Sistema de Gestión de Seguridad de la Información (SGSI) para la Personería Municipal de Armenia, las partes interesadas comprenden a todos los actores internos y externos que tienen responsabilidad, influencia o interés directo en la protección de la información institucional. Estas partes son esenciales para garantizar el éxito y sostenibilidad del

SGSI, ya que su compromiso y participación son fundamentales para la implementación efectiva de políticas y controles. Entre las partes interesadas más relevantes se encuentran:

- Personal interno: funcionarios de planta, contratistas y practicantes que acceden, procesan o custodian información institucional. Su nivel de concienciación y cumplimiento de las políticas de seguridad es determinante para reducir los riesgos.
- Área de tecnología (sistemas): Encargada de administrar la infraestructura tecnológica y apoyar la implementación de controles técnicos como autenticación, respaldo, monitoreo, entre otros.
- Directivos y alta dirección: Responsables de proporcionar liderazgo, recursos y apoyo estratégico al SGSI, así como de tomar decisiones basadas en los informes de riesgos y cumplimiento.
- Ciudadanía y usuarios externos: Beneficiarios de los servicios misionales de la Personería, quienes confían en la confidencialidad y disponibilidad de su información personal y de sus trámites.
- Organismos de control y entes reguladores: Entidades como la Procuraduría General de la Nación o la Superintendencia de Industria y Comercio, que pueden auditar o vigilar el cumplimiento normativo relacionado con la protección de datos y la transparencia.
- Proveedores y terceros: Empresas o personas que prestan servicios tecnológicos, jurídicos o administrativos y que tienen acceso a información sensible o sistemas institucionales.

Estas partes interesadas serán consideradas en el diseño del SGSI mediante mecanismos de comunicación, capacitación, y asignación de responsabilidades claras, con el fin de garantizar

la alineación entre los objetivos institucionales y las buenas prácticas de seguridad de la información.

Política General de Seguridad y Privacidad de la Información

La Personería Municipal de Armenia, consciente de la importancia de una gestión adecuada de la información como activo estratégico, asume el compromiso de proporcionar un entorno de confianza en el ejercicio de sus funciones constitucionales, especialmente en la defensa de los derechos humanos, el interés público y el control de la administración. Este compromiso se encuentra alineado con la normativa vigente, así como con la misión y visión institucional.

La protección de la información busca reducir al máximo el impacto de los riesgos identificados sobre los activos institucionales, garantizando así la confidencialidad, integridad y disponibilidad de la información que se administra, sin importar su formato, medio o canal de procesamiento. Esta gestión se orienta a satisfacer los requerimientos y expectativas de los diferentes grupos de interés.

Esta política es de aplicación obligatoria para todos los funcionarios, contratistas, terceros, proveedores y ciudadanos que interactúan con la Personería Municipal de Armenia, de acuerdo con lo definido en el alcance del SGSI. Además, deberá ser comunicada, comprendida y aplicada por todas las partes interesadas, y estará disponible para su consulta pública a través de los medios institucionales.

Asimismo, las decisiones y acciones adoptadas en materia de seguridad de la información estarán fundamentadas en los siguientes principios:

- Reducir los riesgos asociados a las funciones críticas de la entidad.

- Cumplir con los principios fundamentales de la seguridad de la información.
- Actuar en concordancia con los principios de la administración pública.
- Fortalecer la confianza de la ciudadanía, aliados institucionales y demás partes interesadas.

- Promover el uso seguro y responsable de las tecnologías de la información.
- Salvaguardar los activos de información y tecnológicos.
- Establecer y aplicar políticas, procedimientos y directrices que regulen la seguridad de la información.

- Fomentar una cultura organizacional basada en la protección de la información.
- Asegurar la continuidad institucional ante posibles incidentes de seguridad.

Los siguientes compromisos guían la implementación y operación del Sistema de Gestión de Seguridad de la Información:

- Las responsabilidades en materia de seguridad de la información deben estar claramente asignadas, documentadas, difundidas y asumidas por todos los funcionarios, contratistas, aliados y terceros relacionados.
- Se protegerá la información gestionada por la entidad, así como los sistemas y recursos tecnológicos utilizados, frente a los riesgos derivados de accesos indebidos o de servicios prestados por terceros.
- La información institucional será resguardada para evitar impactos legales, económicos o reputacionales, mediante controles adecuados conforme a su clasificación y sensibilidad.

- Se garantizará la disponibilidad de los procesos misionales y el funcionamiento continuo de la entidad frente a eventos adversos.
- Se dará estricto cumplimiento a las normas legales, contractuales y regulatorias aplicables en materia de seguridad de la información.
- Se impulsará una cultura institucional de responsabilidad, sensibilización y buenas prácticas en torno a la gestión segura de la información.

La presente política deberá ser aprobada por el Comité de Calidad de la entidad, y su cumplimiento será supervisado mediante los procesos definidos en el Sistema de Gestión de Seguridad de la Información, los cuales incluyen la evaluación continua, auditorías internas, revisión por la dirección y mecanismos de mejora continua.

Políticas Específicas de Seguridad y Privacidad de la Información

A continuación, se presenta las políticas específicas de seguridad de la información alineadas con los controles definidos en el plan de tratamiento y con base en los lineamientos de la norma ISO/IEC 27001, en el marco del SGSI para la Personería Municipal de Armenia.

Inteligencia de Amenazas: El objetivo es proveer a la organización de información oportuna sobre amenazas que puedan afectar sus activos, facilitando decisiones de protección proactivas, y las consideraciones son:

- Se debe establecer un sistema de monitoreo de fuentes confiables de inteligencia de amenazas (CERT, CSIRT, boletines).
- Los incidentes de seguridad deben analizarse y documentarse para identificar patrones o tendencias.

- La información de amenazas debe ser evaluada y usada para ajustar los controles de seguridad existentes.

Seguridad de la Información en la Gestión de Proyectos: El objetivo es integrar medidas de seguridad de la información desde las fases tempranas de planificación y ejecución de proyectos institucionales y las consideraciones:

- Todos los proyectos nuevos deben incluir un análisis de riesgos de seguridad de la información.
- Se deben asignar roles de seguridad dentro del equipo de gestión de proyectos.
- La aprobación final del proyecto deberá incluir una validación de cumplimiento con los requisitos de seguridad.

Responsabilidades de Gestión: El objetivo es asegurar que la alta dirección y los responsables de áreas clave ejerzan funciones de liderazgo y toma de decisiones relacionadas con la seguridad de la información, alineadas con la estrategia institucional, y las consideraciones:

- Los directores, jefes de área y líderes de procesos serán responsables de implementar y supervisar controles de seguridad en sus respectivas unidades.
- La seguridad de la información deberá integrarse como objetivo en los planes de gestión y se deberán destinar recursos para tal fin.
- Los responsables de gestión deben recibir formación específica sobre gobierno de seguridad, ISO/IEC 27001 y su rol como parte del SGSI.

Dispositivos Terminales de Usuario

El objetivo es proteger los dispositivos terminales (computadores, portátiles, móviles) utilizados por el personal frente a accesos no autorizados, malware y pérdida de datos, y las consideraciones:

- Todo dispositivo debe estar protegido con credenciales individuales y políticas de bloqueo automático tras inactividad.
- Todo dispositivo debe tener instalado y actualizado un software de protección contra malware autorizado por la organización.
- Solo personal autorizado podrá instalar aplicaciones. Los usuarios estándar no tendrán permisos administrativos.
- Los discos duros de los portátiles deben estar cifrados para proteger la información ante pérdida o robo.
- Los dispositivos deberán ser revisados periódicamente por TI para asegurar que cuentan con parches y actualizaciones críticas.

Restricción de Acceso a la Información

El objetivo es garantizar que el acceso a la información esté limitado únicamente al personal autorizado según el principio de “mínimo privilegio”, protegiendo la confidencialidad e integridad de los datos, y las consideraciones:

- Se debe implementar un esquema de roles donde cada usuario solo acceda a la información necesaria para su función.
- Se debe realizar auditorías trimestrales de los permisos asignados para verificar que sigan siendo apropiados.

- Cualquier cambio de funciones, salida del personal o finalización de contratos implicará la revocación inmediata de accesos.
- Se debe evitar que una misma persona tenga control total sobre procesos críticos sin revisión por parte de otro responsable.
- Se habilitará el registro y monitoreo de accesos a servidores, bases de datos y archivos sensibles.

Autenticación Segura

El objetivo es establecer mecanismos robustos de autenticación que garanticen la verificación segura de la identidad de los usuarios y eviten accesos no autorizados; y las consideraciones:

- Las contraseñas deben tener al menos 12 caracteres, incluir letras mayúsculas, minúsculas, números y símbolos especiales.
- Las contraseñas deberán cambiarse al menos cada 90 días y no podrán repetirse entre los últimos 5 ciclos.
- Se implementará MFA en los accesos remotos, correos electrónicos, VPNs y aplicaciones críticas.
- Las cuentas se bloquearán tras 5 intentos fallidos de autenticación y solo podrán desbloquearse con intervención de TI.
- Ningún usuario está autorizado a compartir sus credenciales en ninguna circunstancia.

Protección Contra Código Malicioso (Malware)

El objetivo es Prevenir, detectar y responder a la presencia de software malicioso en los

sistemas informáticos que pueda afectar la disponibilidad o integridad de los activos; y

las consideraciones:

- Todos los dispositivos conectados a la red deberán tener un antivirus actualizado aprobado por la entidad.
- Los mecanismos de defensa contra malware deben mantenerse actualizados automáticamente desde el fabricante.
- No se debe permitir la ejecución de archivos con extensión .exe, .bat, .msi, .vbs u otros no autorizados sin previa validación.
- Se restringirá el uso de medios extraíbles. Su utilización deberá estar autorizada y controlada por el área de TI.

Gestión de Vulnerabilidades Técnicas

El objetivo es identificar, evaluar y mitigar oportunamente las vulnerabilidades técnicas en los sistemas de información, reduciendo el riesgo de explotación por amenazas externas o internas; y las consideraciones:

- Se realizarán análisis automatizados mensuales para identificar vulnerabilidades en sistemas, redes y aplicaciones.
- Todos los sistemas deberán aplicar parches de seguridad en un plazo no mayor a 15 días tras su publicación.
- Se utilizará una escala de criticidad (por ejemplo, CVSS) para priorizar la atención de vulnerabilidades encontradas.
- Cada vulnerabilidad será documentada desde su detección hasta su mitigación, con responsables y fechas de cierre.

Enmascarado de Datos

El objetivo es proteger la confidencialidad de los datos sensibles mediante técnicas de enmascaramiento que impidan su exposición en entornos de desarrollo, prueba o acceso no autorizado; y las consideraciones:

- Los campos como número de identificación, datos bancarios o clínicos serán visibles completos solo para perfiles con privilegios.
- Toda base de datos utilizada en entornos de prueba deberá contener datos enmascarados o anonimizados.
- Se debe limitar el despliegue de información sensible en aplicaciones, paneles de usuario o reportes.
- Los accesos a información confidencial serán registrados y auditados periódicamente para detectar usos indebidos.

Prevención de Filtración de Datos

El objetivo es evitar la fuga o exposición no autorizada de información confidencial o sensible desde los sistemas institucionales; y las consideraciones:

- Se implementará un sistema que detecte y bloquee el envío no autorizado de información por correo, USB o nube.
- No se permite usar cuentas personales de Google Drive, Dropbox, etc., para almacenar o compartir información institucional.
- Se auditarán los accesos a carpetas en red, evitando que datos sensibles estén disponibles para todos los usuarios.
- Todos los correos que contengan adjuntos con datos personales o confidenciales deben ser cifrados.

Uso de Criptografía

El objetivo es proteger la confidencialidad, integridad y autenticidad de la información mediante el uso seguro y efectivo de mecanismos criptográficos; y las consideraciones:

- Toda información clasificada como confidencial o crítica deberá ser cifrada en tránsito (TLS 1.2+) y en reposo (AES-256 o superior).
- Se implementará un sistema para la gestión del ciclo de vida de las claves criptográficas (generación, distribución, rotación y eliminación segura).
- Los discos duros de laptops y dispositivos móviles serán cifrados con soluciones como BitLocker o LUKS.
- Los sistemas web institucionales deberán utilizar certificados digitales válidos, emitidos por autoridades confiables.

Derechos de Acceso Privilegiado

El objetivo es controlar y supervisar el uso de accesos privilegiados para minimizar riesgos de abuso, modificación no autorizada o filtración de información crítica; y las consideraciones:

- Los derechos de acceso privilegiado solo deben ser asignados previa aprobación formal del responsable de seguridad o TI, con justificación documentada.
- Se realizará una revisión mensual de todos los accesos privilegiados, verificando su necesidad y vigencia, revocando los innecesarios.
- Todas las sesiones con privilegios elevados deben ser registradas y auditadas, incluyendo comandos ejecutados, accesos a archivos y cambios de configuración.
- No se permitirá que un mismo usuario con privilegios elevados realice actividades de validación o auditoría sobre sus propias acciones.

Respaldo de Información

El objetivo es asegurar la disponibilidad y recuperación de la información crítica mediante la implementación de políticas de respaldo fiables y regulares; y las consideraciones:

- Se deben realizar respaldos diarios automáticos de todos los sistemas críticos y semanales de sistemas no críticos, incluyendo bases de datos, archivos compartidos y configuraciones.
- Al menos una copia de los respaldos deberá almacenarse en una ubicación externa segura o en la nube con cifrado.
- Se deben realizar pruebas de restauración trimestrales para garantizar la integridad y funcionalidad de los respaldos.
- Todos los respaldos deben estar cifrados y su acceso limitado al personal autorizado mediante credenciales fuertes y doble autenticación.

Definir Roles, Responsabilidades y Mecanismos de Seguimiento del SGSI con base en

Principios de Gobernanza de TI Establecidos en COBIT

La correcta definición de roles, responsabilidades y mecanismos de seguimiento dentro del Sistema de Gestión de Seguridad de la Información (SGSI) es fundamental para garantizar una gestión efectiva, transparente y alineada con los intereses institucionales. En ausencia de una estructura de gobierno clara, los procesos relacionados con la seguridad de la información tienden a fragmentarse, generar duplicidad de funciones o dejar vacíos críticos de responsabilidad. Esto puede traducirse en fallos de cumplimiento normativo, debilidad en la gestión de riesgos, y baja capacidad de respuesta ante incidentes de seguridad.

Análisis de Principios de COBIT Aplicables al SGSI

El modelo de gobernanza propuesto por COBIT 2019 constituye una guía robusta y adaptable para estructurar responsabilidades, mecanismos de control y principios de supervisión sobre la tecnología y la información. Su aplicación al diseño del SGSI permite garantizar que las decisiones sobre seguridad estén alineadas con los objetivos organizacionales, sean consistentes y auditables, y contribuyan a la generación de valor a través de la minimización de riesgos.

Además, se compone de:

- Objetivos de gobierno (EDM): Enfocados en establecer la dirección estratégica y la supervisión.
- Objetivos de gestión (APO, BAI, DSS, MEA): Dirigidos a la planificación, ejecución, entrega y monitoreo.

Se priorizarán aquellos que impactan directamente la gobernanza y gestión de la seguridad de la información, en la siguiente tabla:

Tabla 25*Componentes de COBIT Relevantes para el SGSI*

Objetivo COBIT	Nombre	Aplicación al SGSI
EDM01	Asegurar el marco de gobierno	Define estructuras y principios de gobernanza, incluyendo autoridad para decisiones de seguridad.
EDM03	Asegurar la optimización del riesgo	Relacionado con el riesgo de seguridad, define responsabilidades para gestionarlo y supervisarlos.
APO01	Gestionar el marco de gestión de TI	Permite diseñar políticas, procesos, y establecer roles y niveles de autoridad en seguridad.
APO07	Gestionar recursos humanos	Vincula la seguridad a la gestión del talento, define roles, competencias y formación en seguridad.
APO13	Gestionar la seguridad	Objetivo central para estructurar el SGSI: define políticas, responsables y controles necesarios.
MEA01	Monitorear el desempeño y conformidad	Establece indicadores, mecanismos de revisión y roles para la evaluación continua del SGSI.

Nota. Componentes de COBIT Relevantes para el SGSI (Autoría Propia)

COBIT 2019 propone seis principios que rigen el diseño de un sistema de gobernanza efectivo para la información y la tecnología. Estos principios constituyen la base conceptual para asegurar una gestión estructurada, alineada con los objetivos institucionales y adaptable a contextos específicos, como lo requiere un SGSI.

Principio 1: Satisfacer las Necesidades de las Partes Interesadas Proporcionando**Resultados Procesables y Beneficios Mensurables.**

Este principio establece que el sistema de gobernanza debe crear valor para las partes interesadas, equilibrando la generación de beneficios, la optimización de riesgos y la utilización de recursos.

- El SGSI no debe enfocarse exclusivamente en la protección técnica de la información, sino en responder a las expectativas de los ciudadanos, entes de control, funcionarios y usuarios internos.
- Se debe vincular la seguridad de la información con los objetivos institucionales de confianza, transparencia y cumplimiento normativo, para asegurar que se perciba como un habilitador del servicio público y no como una carga operativa.

Principio 2: Cubrir Toda la Empresa, no Centrarse sólo en TI

El sistema de gobernanza debe considerar todos los componentes que interactúan para lograr los objetivos organizacionales: procesos, estructuras organizativas, principios, información, personas, habilidades, servicios, infraestructura y aplicaciones.

- Al definir responsabilidades, se deben considerar no solo cargos formales, sino también flujos de información, conocimientos clave, cultura organizacional y sistemas tecnológicos.

Principio 3: Permitir un Enfoque Holístico Considerando todos los Componentes de Gobernanza

El sistema de gobernanza debe diseñarse como un conjunto de componentes interdependientes, integrados y coordinados que funcionen juntos de forma coherente.

- No basta con definir roles de manera aislada. Las responsabilidades deben interconectarse a través de procesos, flujos de trabajo y mecanismos de seguimiento estructurados.
- Cada componente del SGSI (control de accesos, formación, gestión de incidentes, continuidad) debe tener responsables y estructuras de supervisión coordinadas, no fragmentadas.

Principio 4: Aplicar un Marco Único e Integrado para Gestionar la Gobernanza en Múltiples Dominios

El sistema de gobernanza debe poder evolucionar y adaptarse a los cambios en el entorno interno y externo de la organización.

- La asignación de roles debe respetar las capacidades existentes (ej. disponibilidad de personal, funciones actuales, nivel de formación).
- Los mecanismos de seguimiento deben ser proporcionales: no excesivamente complejos, pero sí suficientes para garantizar trazabilidad, mejora y cumplimiento.

Principio 5: Separar Claramente la Gobernanza de la Gestión, donde la Gobernanza

Establece la Dirección y Evalúa los Resultados, y la Gestión Ejecuta los Planes.

COBIT distingue claramente la gobernanza (establecer dirección, evaluar y monitorear) de la gestión (planear, construir, ejecutar y controlar).

- La estructura de roles debe diferenciar quiénes toman decisiones estratégicas (gobernanza: alta dirección, comité de seguridad), y quiénes las ejecutan en la operación (gestión: coordinador del SGSI, personal TIC, líderes de procesos).

Identificación y Estructuración de Roles Clave en el SGSI

La correcta identificación y asignación de roles y responsabilidades es un pilar fundamental para garantizar la eficacia, sostenibilidad y gobernanza del Sistema de Gestión de Seguridad de la Información (SGSI). Esta actividad busca definir quién hace qué, cómo, con qué autoridad y bajo qué mecanismos de supervisión, asegurando así la trazabilidad, responsabilidad y alineación institucional.

Principios de Estructuración de Roles: La definición de roles en el SGSI debe basarse en:

- Separación de funciones (principio de gobernanza de COBIT y buenas prácticas de seguridad): Evitar que una misma persona diseñe, ejecute y audite un control.
- El modelo RACI es una herramienta de gestión que se utiliza para asignar y clarificar roles y responsabilidades en procesos, proyectos o actividades específicas dentro de una organización. Es ampliamente usado en la gestión de proyectos, la gobernanza de TI (incluido en COBIT), y en la implementación de sistemas como el SGSI (Sistema de Gestión de Seguridad de la Información) bajo ISO/IEC 27001

Roles clave propuestos para la Personería Municipal de Armenia: A continuación, se detallan los principales roles necesarios para el funcionamiento del SGSI, con sus funciones y dependencia jerárquica sugerida:

Tabla 26

Roles Propuestos para la Personería Municipal de Armenia

Rol	Descripción del rol	Funciones principales	Relación jerárquica y operativa
Alta Dirección / Dirección General	Máxima autoridad institucional	• Aprobar políticas y objetivos del SGSI. • Asignar recursos y respaldar la implementación. • Revisar y evaluar la eficacia del SGSI.	Responsable final del sistema. Informa al Comité de Control Interno.
Comité de Seguridad de la Información	Asesor	• Analizar riesgos. • Recomendar decisiones estratégicas. • Coordinar áreas implicadas.	Conformado por TIC, jurídica, talento humano, control interno. Consultado por el Coordinador SGSI.
Coordinador del SGSI	Líder operativo del sistema	• Diseñar y mantener el SGSI. • Coordinar auditorías. • Informar a la dirección. • Supervisar la implementación de controles.	Responsable de ejecución. Reporta directamente a la Alta Dirección.
Responsables de proceso / jefes de dependencia	Líderes de cada área funcional	• Aplicar políticas del SGSI en su proceso. • Identificar riesgos específicos. • Proponer controles.	Consultados en la gestión de riesgos. Informados de hallazgos y acciones.

Tabla 26 (Continuación)*Roles Propuestos para la Personería Municipal de Armenia*

Rol	Descripción del rol	Funciones principales	Relación jerárquica y operativa
Oficina TIC	Encargados de la infraestructura tecnológica	• Implementar controles técnicos (firewalls, backups, accesos). • Documentar configuraciones. Monitorear eventos de seguridad.	Responsables de medidas técnicas. Consultados por el Coordinador SGSI.
Control Interno / Auditoría	Órgano evaluador independiente	• Realizar auditorías periódicas del SGSI. • Verificar cumplimiento normativo. Emitir informes y recomendaciones.	Independiente de la ejecución.
Usuarios finales / funcionarios	Personal de planta y contratistas	• Cumplir con políticas y procedimientos. • Reportar incidentes. • Participar en capacitaciones.	Informados y responsables de su propia conducta en seguridad.

Nota. Roles propuestos para la Personería Municipal de Armenia (Autoría Propia)

Esquema Funcional de Gobernanza y Gestión del SGSI: La implementación de un SGSI requiere una estructura organizacional clara, en la que se definan de forma precisa los niveles de autoridad, responsabilidad y supervisión de todas las partes involucradas. Este esquema funcional debe responder a los principios de gobernanza de TI establecidos en COBIT, así como a los requisitos de liderazgo, apoyo y mejora continua de la norma ISO/IEC 27001. Las características clave del esquema:

- Alta Dirección como ente estratégico: asume el rol de autoridad máxima, responsable de establecer la política de seguridad, asignar recursos, definir el apetito de riesgo y aprobar las acciones de mejora. Se alinea con el objetivo de gobernanza EDM01 (Asegurar la gobernanza) de COBIT.
- Coordinador del SGSI como eje operativo: lidera la ejecución del SGSI, dirige el análisis de riesgos, controla la implementación de controles y rinde informes a la alta dirección. Se vincula con los objetivos de gestión APO12 (Gestión del riesgo) y BAI01 (Gestión de programas y proyectos).
- Comité de Seguridad de la Información como cuerpo asesor y coordinador: está conformado por representantes clave (TIC, jurídica, talento humano, control interno, procesos). Facilita la toma de decisiones informadas y permite la colaboración interdepartamental.
- Responsables de procesos / dependencias: ejecutan los controles en sus respectivas áreas, reportan incidentes, identifican riesgos y aplican correctivos.
- Control Interno / Auditoría como órgano de evaluación y supervisión independiente: audita el cumplimiento del SGSI, emite recomendaciones y verifica la eficacia.

Diseño de Mecanismos de Seguimiento del SGSI

El seguimiento efectivo del Sistema de Gestión de Seguridad de la Información (SGSI) es un componente esencial dentro de un marco de gobernanza de TI, toda vez que permite asegurar la alineación estratégica con los objetivos institucionales, verificar el cumplimiento normativo, y promover la mejora continua. Para esto, el marco COBIT proporciona principios, prácticas y estructuras de control que permiten diseñar mecanismos de seguimiento sólidos y orientados a resultados. Por lo anterior, los mecanismos de seguimiento se fundamentan especialmente en los siguientes principios de COBIT:

- **Evaluar, Dirigir y Monitorear (EDM):** Este dominio guía la alta dirección en la supervisión de los sistemas de TI, incluyendo el SGSI. En particular:
 - **EDM01: Asegurar la gobernanza del valor:** Verifica que el SGSI aporte valor.
 - **EDM03: Asegurar la optimización del riesgo:** Incluye el monitoreo del riesgo de seguridad de la información.
 - **EDM05: Asegurar la transparencia del desempeño y la conformidad:** Es el principio rector para establecer indicadores, reportes y auditorías del SGSI.

Indicadores Clave en el Seguimiento del SGSI: Estos indicadores deben ser SMART (específicos, medibles, alcanzables, relevantes y con un tiempo definido), y estar vinculados a los objetivos del SGSI, conforme a COBIT.

Tabla 27*Indicador Tiempo Promedio de Respuestas a Incidentes*

Nombre del Indicador: Tiempo promedio de respuesta a incidentes	
Objetivo	Evaluar la eficiencia en la gestión de incidentes
Fórmula	$\sum \text{tiempos de respuesta} / \text{N.º incidentes reportados}$
Variables	Tiempo de respuesta Número de incidentes
Responsables	Administrador de sistemas Coordinador SGSI
Frecuencia de Medición	Trimestral
Valoración del Indicador	>24h: Deficiente 8–24h: Aceptable <8h: Óptimo

Nota. Indicador Tiempo promedio de respuestas a incidentes (Autoría Propia)**Tabla 28***Indicador Funcionarios Capacitados en Seguridad*

Nombre del Indicador: funcionarios capacitados en seguridad	
Objetivo	Medir el nivel de cobertura de capacitaciones
Fórmula	$(\text{funcionarios capacitados} / \text{Total funcionarios}) \times 100$
Variables	Funcionarios capacitados Total, funcionarios
Responsables	Talento Humano Coordinador SGSI
Frecuencia de Medición	Trimestral
Valoración del Indicador	<70%: Bajo 70–89%: Medio ≥90%: Alto

Nota. Indicador funcionarios capacitados en seguridad (Autoría Propia)

Tabla 29*Indicador Número de Incidentes Críticos*

Nombre del Indicador: Número de Incidentes críticos	
Objetivo	Identificar la frecuencia de incidentes que afectan gravemente la seguridad
Fórmula	Total, de incidentes críticos registrados en el trimestre
Variables	Incidentes críticos: incidentes clasificados como de severidad alta por impacto o disponibilidad
Responsables	Administrador de sistemas - Coordinador SGSI
Frecuencia de Medición	Trimestral
Valoración del Indicador	0: Óptimo 1–2: Aceptable >2: Crítico

Nota Indicador Número de incidentes críticos (Autoría Propia)**Tabla 30***Porcentaje de Vulnerabilidades sin Mitigar*

Nombre del Indicador: Porcentaje de vulnerabilidades sin mitigar	
Objetivo	Medir el nivel de exposición ante debilidades no corregidas
Fórmula	$\left(\frac{\text{Vulnerabilidades no mitigadas}}{\text{Total vulnerabilidades detectadas}} \right) \times 100$
Variables	Vulnerabilidades detectadas (por escáner o revisión), vulnerabilidades sin gestionar
Responsables	Administrador de sistemas - Coordinador SGSI
Frecuencia de Medición	Mensual
Valoración del Indicador	<10%: Óptimo 10–25%: Riesgo moderado >25%: Riesgo alto

Nota. Porcentaje de vulnerabilidades sin mitigar (Autoría Propia)

Tabla 31*Numero de Accesos no Autorizados Detectados*

Nombre del Indicador: Numero de accesos no autorizados detectados	
Objetivo	Controlar la eficacia de los controles de acceso en sistemas críticos
Fórmula	Total, de accesos no autorizados detectados en el periodo
Variables	Accesos no autorizados: intentos o accesos confirmados sin permisos, registrados en los logs
Responsables	Administrador de sistemas - Coordinador SGSI
Frecuencia de Medición	Mensual
Valoración del Indicador	0: Óptimo 1–3: Riesgo moderado >3: Riesgo alto

Nota. Numero de accesos no autorizados detectados (Autoría Propia)

Tabla 32*Porcentaje de Acciones de Mejora Implementadas*

Nombre del Indicador: Porcentaje de acciones de mejora implementadas	
Objetivo	Evaluar la ejecución de planes correctivos y de mejora
Fórmula	$(\text{Acciones completadas} / \text{Acciones planificadas}) \times 100$
Variables	Acciones completadas Acciones planificadas
Responsables	Coordinador SGSI líderes de procesos
Frecuencia de Medición	Trimestral
Valoración del Indicador	<70%: Deficiente 70–89%: Parcial ≥90%: Cumplido

Nota. Porcentaje de acciones de mejora implementadas (Autoría Propia)

Este enfoque garantiza que los mecanismos de seguimiento no solo respondan a los requisitos de la norma ISO/IEC 27001, sino que se articulen dentro de un modelo integral de

gobierno de TI, como lo establece COBIT. Esto permite integrar la gestión de la seguridad con la estrategia institucional, así como justificar recursos para el SGSI con base en evidencia medible y demostrar transparencia y rendición de cuentas en los temas de seguridad de la información.

En conclusión, la definición de roles, responsabilidades y mecanismos de seguimiento del SGSI, sustentada en los principios de gobernanza de TI establecidos en COBIT, proporciona una base sólida para asegurar la transparencia, trazabilidad y eficacia en la gestión de la seguridad de la información. La integración de indicadores, estructuras de supervisión y flujos de autoridad definidos no solo garantiza la alineación con los objetivos institucionales, sino que también fortalece la capacidad organizacional para identificar desviaciones, gestionar riesgos y aplicar mejoras correctivas oportunas.

Conclusiones

A partir del diagnóstico institucional y del desarrollo de los objetivos específicos planteados en este proyecto, se evidenció que la Personería Municipal de Armenia enfrenta debilidades significativas en la gestión de la seguridad de la información, tanto a nivel técnico como organizacional. El análisis de la situación actual permitió establecer las bases para el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO/IEC 27001 y apoyado en principios de gobernanza de TI establecidos en COBIT, como respuesta estructurada y estratégica a los riesgos identificados.

En primer lugar, la identificación y clasificación de los activos de información permitió visibilizar cuáles son los elementos más críticos para la operación institucional. La falta de un inventario actualizado y formal de activos representaba un riesgo latente, al no existir una base clara sobre la cual priorizar las acciones de protección. Este proceso permitió definir el valor de cada activo en función de su importancia para los procesos misionales, lo que facilitó la priorización de medidas de seguridad acordes a las necesidades reales de la entidad.

Posteriormente, al evaluar el estado actual de los controles de seguridad en la organización, se confirmó un nivel de madurez insuficiente. Muchos de los controles presentaban un estado “inexistente” o “inicial”, especialmente en áreas críticas como la gestión de accesos, el tratamiento de incidentes, la continuidad del negocio y la concienciación del personal. Esta situación evidenció una alta exposición a riesgos tecnológicos y operacionales, y demostró la necesidad urgente de adoptar un marco de gestión estructurado como ISO/IEC 27001.

En respuesta a estas brechas, se desarrollaron políticas específicas para los controles con bajo nivel de cumplimiento, con el objetivo de proporcionar directrices claras, formales y

aplicables. Estas políticas no solo constituyen un instrumento normativo para la protección de la información, sino también un mecanismo para institucionalizar buenas prácticas, asegurar el cumplimiento regulatorio y fomentar la cultura de seguridad dentro de la entidad.

Uno de los aspectos más relevantes abordados fue la definición de roles, responsabilidades y mecanismos de seguimiento del SGSI. Se evidenció que la falta de una estructura organizacional formal, con funciones claramente asignadas y mecanismos de supervisión efectivos, limitaba la capacidad de la institución para gestionar la seguridad de manera proactiva. Con base en los principios de COBIT y en la cláusula 5 de la norma ISO/IEC 27001, se propuso un modelo de gobernanza funcional que asigna responsabilidades mediante una matriz RACI, establece flujos jerárquicos de autoridad y define procesos de seguimiento mediante indicadores clave de desempeño, auditorías internas y revisiones periódicas por parte de la alta dirección.

En conjunto, los resultados alcanzados a través del desarrollo de estos objetivos permiten concluir que el diseño del SGSI propuesto representa una solución integral y realista frente a las debilidades diagnosticadas. Este sistema proporciona una base normativa, técnica y organizacional que permitirá mejorar la protección de los activos de información, reducir la exposición al riesgo, y garantizar la continuidad de los servicios institucionales.

Recomendaciones

La seguridad de la información se ha consolidado como un componente esencial para la gestión pública, dado que permite proteger los activos institucionales, fortalecer la confianza de la ciudadanía y garantizar la continuidad de los servicios.

En este contexto, en primer lugar, se recomienda que la Personería Municipal de Armenia formalice y mantenga un inventario actualizado y clasificado de los activos de información, identificando su criticidad e impacto sobre los procesos misionales. Este inventario debe ser gestionado por personal designado dentro del SGSI y utilizarse como base para priorizar la implementación de medidas de protección, garantizando una asignación eficiente de recursos y una mayor resiliencia frente a amenazas.

En segundo lugar, es necesario fortalecer la gestión de los controles de seguridad de la información mediante un plan de implementación progresiva basado en la norma ISO/IEC 27001. Se recomienda iniciar por las áreas con mayor exposición, como la gestión de accesos, el tratamiento de incidentes, la continuidad del negocio y la formación del personal. Esto permitirá elevar el nivel de madurez de los controles existentes y reducir la vulnerabilidad institucional ante amenazas internas y externas.

Como tercera medida, se aconseja formalizar y socializar las políticas específicas de seguridad desarrolladas para cubrir los controles en estado “inexistente”, “inicial” o “limitado”. Estas políticas deben integrarse en la normativa interna de la entidad, difundirse a todo el personal, y evaluarse periódicamente para asegurar su efectividad. Además, deben ser tratadas como instrumentos clave para consolidar una cultura organizacional basada en la protección de la información y el cumplimiento normativo.

En cuarto lugar, se sugiere que toda política, estructura o procedimiento que forme parte del SGSI sea aprobado por el Comité de Calidad de la entidad, como órgano garante de la alineación con los objetivos institucionales. Además, debe asegurarse que estos elementos sean supervisados de manera continua por los procesos definidos dentro del sistema, garantizando su cumplimiento, revisión periódica y adecuación frente a cambios tecnológicos o normativos.

Finalmente, se recomienda estructurar formalmente el modelo de gobierno del SGSI, asignando responsabilidades mediante matrices RACI, estableciendo líneas jerárquicas claras y asegurando mecanismos eficaces de supervisión. Esta estructura debe respaldarse con indicadores de desempeño, auditorías internas y procesos de mejora continua, facilitando así una gestión proactiva y controlada de la seguridad de la información en la entidad.

Referencias Bibliográficas

- Alemán, h., & Rodríguez, C. (29 de 01 de 2019). *Metodologías Para el Análisis de Riesgos en los SGSI*. <http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874>
- Blerton, A. (2025). Building resilience: A strategic framework for managing information security risks. *Edelweiss Applied Science and Technology*.
- De León Camelo, J. (2019). *Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001 para entidades del estado*.
<https://repository.unad.edu.co/bitstream/handle/10596/27821/%20%09jcdeleonc.pdf?sequence=3&isAllowed=y>
- Funcion Publica. (2020). *Políticas de Operación Proceso de Tecnologías de la Información*. Seguridad de la Información Documento Técnico Marzo de 2020:
<https://www1.funcionpublica.gov.co/documents/418537/36701283/politica-de-seguridad-de-la-informacion.pdf.pdf/325019e5-a92f-0b44-3676-2356bd71240c?t=1586355315672>
- Función Publica. (2021). *Ley 1581 de 2012 - Gestor Normativo*.
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>
- Función Pública. (2022). *Ley 1712 de 2014 - Gestor Normativo*.
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882>
- Guacanes Castro , M., & Vilatuña Morales, J. (2022). *Propuesta de diseño de un SGSI basado en la norma ISO/IEC 27001. Caso de estudio la empresa Ultralink*.
<https://bibdigital.epn.edu.ec/handle/15000/22812>

- Hernandez Sampieri, R., & Mendoza Torres, C. (2018). *Metodologia de la investigacion. Las rutas cuantitativa, cualitativa y mixta*. Mexico.
- IBM. (2020). *¿Qué es el marco de ciberseguridad del NIST?* <https://www.ibm.com/mx-es/topics/nist>
- ISACA. (2019). *COBIT 2019: Framework for Governance and Management of Enterprise IT*. <https://www.isaca.org/resources/cobit>
- ISO. (2018). *ISO/IEC 27000 family*. <https://www.iso.org/standard/iso-iec-27000-family>
- ISO. (2022). *ISO/IEC 27005:2022*. https://www-iso-org.translate.goog/standard/80585.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc
- 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 (Switzerland)*.
- La Red de Investigación en Ciberdelincuencia y Ciberseguridad. (2025). *Ciberataques a Entidades Públicas en Colombia* . <https://www.redciber.org/post/ciberataques-a-entidades-p%C3%BAblicas-en-colombia-2021-2023>
- López Aguado, M., & Gutiérrez Provecho, L. (2019). Cómo realizar e interpretar un análisis factorial exploratorio utilizando SPSS. *REIRE* , 1-14.
- Martelo, R., Maderay, J., & Betín , A. (2016). Software para gestión documental, un componente modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Informacion Tecnologica*, 129-134.

Ministerio de Hacienda y Administraciones Públicas. (2014). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid.

Ministerio de Hacienda y Administraciones Públicas. (2014). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid.

MinTIC. (2018). *Guía para la Gestión y Clasificación de Activos de Información*.

https://gobiernodigital.mintic.gov.co/692/articles-150528_G5_Gestion_Clasificacion.pdf

MinTIC. (2018). *Implementación de la Política de Gobierno Digital*.

https://gobiernodigital.mintic.gov.co/692/channels-594_manual_gd.pdf

MinTIC. (2021). *Política de Seguridad Digital*. <https://mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Preguntas-frecuentes/15430:Politica-de-Seguridad-Digital>

MinTIC. (2021). *Política General de Seguridad y Privacidad de la Información*.

https://gobiernodigital.mintic.gov.co/692/articles-176922_recurso_1.docx

Monev, V. (2024). Suitability of Information Security Frameworks for an IT-Centric ISMS. 2024 38th International Conference on Information Technologies, InfoTech 2024 - Proceedings.

Morales, M. (2019). "Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte.". *Revista peruana de computación y sistemas* 2.2 , págs. 43-60.

Moses, F., & Sandkuhl, K. (2025). Information Security in Small Public Sector Organizations: Design and Evaluation of Procedural Approach. En *Lecture Notes in Networks and Systems* (págs. 295 - 307).

Niemeläinen, A., Waseem, M., & Mikkonen, T. (2025). Enhancing Productivity with AI During the Development of an ISMS: Case Kempower. *Lecture Notes in Computer Science*.

- Personería Municipal de Armenia. (2023). *Portafolio de Servicios*. https://personeria-municipal-de-armenia.micolombiadigital.gov.co/sites/personeria-municipal-de-armenia/content/files/000021/1020_portafolio-servicios.pdf
- Personería Municipal de Armenia en Quindío. (2024). *Personería Municipal de Armenia en Quindío*. <https://www.personeria-armenia.gov.co/entidad/mision-y-vision>
- Portafolio. (2023). *Las entidades y procesos afectados por ciberataque que siente Colombia*. <https://www.portafolio.co/economia/gobierno/entidades-y-procesos-en-colombia-que-fueron-afectados-por-ciberataque-589111>
- Robles Chaparro, E., Riatiga Ibañez, J., & Delgado Romero, A. (2023). *Guía de Derecho de Autor*. DNA Dirección Nacional del Derecho de Autor: <https://www.derechodeautor.gov.co/sites/default/files/2024-03/Gu%C3%ADa-de-Derecho-de-Autor-para-creadores-y-usuarios.pdf>
- Ruiz Peña, J. (2018). *Diseño de un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO/IEC 27001: 2013, en la Cooperativa Multiactiva del personal del Sena, en Bogotá*. <https://repository.unad.edu.co/bitstream/handle/10596/17300/80267708.pdf?sequence=1&isAllowed=y>
- Soluciones de Software OTRS. (2025). *SGSI – Sistema de Gestión de Seguridad de la Información*. <https://otrs.com/es/casos-de-uso/sgsi/#:~:text=%C2%BFQu%C3%A9%20es%20un%20SGSI%3F,que%20deben%20llevarse%20a%20cabo>

- Tintin , R., & Hidalgo , M. (2023). Could an ISMS Model (ISO/IEC 27001:2013 Standard) Implementation Really Protect Public Data? *2023 9th International Conference on eDemocracy and eGovernment, ICEDEG 2023*.
- Toala , I., & Yomar , I. (2021). *Delitos informáticos frecuentes en el Ecuador: casos de estudio*. <https://dspace.ups.edu.ec/handle/123456789/20942>
- Tonysé de la Rosa, M. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001. *Universidad y Sociedad*, 495-506.
- Whitman, M., & Mattord, H. (2021). *A Model Curriculum for Programs of Study in Information Security/Cybersecurity*. <https://www.kennesaw.edu/coles/centers/cyber-center/resources/docs/model-curriculum-2021.pdf>

Apéndices

Apéndice A

Carta de Aceptación Proyecto Aplicado



PERSONERÍA
Municipal de Armenia

Armenia, 8 de mayo de 2025

Señores

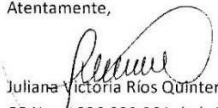
Universidad Nacional Abierta y a Distancia UNAD
Escuela de Ciencias Básicas, tecnología e ingeniería
Dosquebradas

Yo **Juliana Victoria Ríos Quintero** identificada con CC 1.096.032.381 de la Tebaida Quindío, en mi calidad de Personera Municipal de Armenia Quindío, autorizo a Lady Johanna Vera Torres, estudiante del programa **Especialización en Seguridad Informática** de la **Universidad Nacional Abierta y a Distancia**, a utilizar la información de la empresa para el proyecto denominado **Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en las normas ISO/IEC 27001 para la Personería Municipal de Armenia**. Como condiciones, el estudiante se obliga a (1) no divulgar ni usar para fines personales la información (documentos, expedientes, escritos, artículos, contratos, estados de cuenta y demás materiales que, con objeto de la relación de trabajo, le fue suministrada; (2) no proporcionar a terceras personas, verbalmente o por escrito, directa o indirectamente, información alguna de las actividades y/o procesos de cualquier clase que fuesen observadas en la empresa durante la duración del proyecto y (3) no utilizar completa o parcialmente ninguno de los productos (documentos, metodología, procesos y demás relacionadas con el proyecto. El estudiante asume que toda información y el resultado del proyecto será de uso exclusivamente académico.

El material suministrado por la empresa será la base para la construcción de un estudio de caso. La información y resultado que se obtenga del mismo podrían llegar a convertirse en una herramienta didáctica que apoye la formación de los estudiantes de la Escuela de Ciencias Básicas, Tecnología e Ingeniería.

En caso de que alguna(s) de las condiciones anteriores sea(n) infringida(s), el estudiante queda sujeto a la responsabilidad civil por daños y perjuicios que cause a la **Personería Municipal de Armenia**, así como a las sanciones de carácter penal o legal a que se hiciere acreedor.

Atentamente,


Juliana Victoria Ríos Quintero
CC-No. 1.096.032.381 de la Tebaida, Q.
Personería Municipal

Apéndice B

Instrumento de Caracterización de Seguridad Informática

Objetivo: Recopilar datos relevantes sobre la percepción y conocimiento de los empleados respecto a la seguridad de la información dentro de la Personería de Armenia

Instrucciones: Marque en la casilla el valor correspondiente a cada opción acorde con el estado y conocimiento de seguridad de la información de la siguiente manera:

5. Dinámico (Excelente cumplimiento y aplicación de medidas de seguridad), 4. Influyente (Buen cumplimiento con algunas mejoras necesarias), 3. Estándar (Cumplimiento moderado, con oportunidades de mejora), 2. Aplicado (Cumplimiento deficiente, con alto margen de riesgo), 1. Caótico (No se aplica, riesgo inminente)

1. Datos Generales

Cargo en la entidad:

☐ Administrativo ☐ Técnico ☐ Jurídico ☐ Directivo ☐ Asistencial

Vinculación laboral con la entidad:

☐ Carrera Administrativa ☐ Provisional ☐ Libre Nombramiento ☐ Contratista

Años de experiencia en la entidad:

☐ Menos de 1 año ☐ 1-3 años ☐ 4-6 años ☐ Más de 6 años

2. Conocimientos Generales

¿Qué tan involucrado está en el uso de sistemas informáticos dentro de la entidad?

☐ 5. Uso constante y avanzado

☐ 4. Uso frecuente con conocimientos básicos

☐ 3. Uso moderado con conocimiento limitado

☐ 2. Uso esporádico con baja interacción

☐ 1. Casi nunca usa los sistemas

¿Cómo considera su conocimiento en seguridad informática?

☐ 5. Avanzado, domina conceptos y herramientas

☐ 4. Intermedio, aplica medidas básicas

☐ 3. Básico, conoce solo lo esencial

☐ 2. Muy limitado, requiere capacitación

☐ 1. Desconoce completamente

¿Con qué frecuencia accede a información sensible dentro de la entidad?

☐ 5. Diariamente

☐ 4. Varias veces a la semana

☐ 3. Ocasionalmente

☐ 2. Rara vez

☐ 1. Nunca

3. Capacitación y Sensibilización

¿Con qué frecuencia recibe capacitación en seguridad informática?

☐ 5. Cada 3 meses o menos

☐ 4. Cada 6 meses

☐ 3. Una vez al año

☐ 2. Hace más de un año

☐ 1. Nunca

¿Cómo califica la efectividad de la capacitación recibida?

☐ 5. Totalmente efectiva, aplica lo aprendido

☐ 4. Efectiva, pero con áreas de mejora

☐ 3. Moderadamente útil, poco aplicable

☐ 2. Poco efectiva, difícil de aplicar

☐ 1. No ha recibido capacitación o no es útil

¿Considera que la capacitación en seguridad informática está alineada con los riesgos reales a los que se enfrenta la entidad?

☐ 5. Totalmente alineada, cubre todas las amenazas posibles

☐ 4. Bien alineada, pero falta abordar ciertos riesgos específicos

☐ 3. Parcialmente alineada, algunos riesgos no son cubiertos

☐ 2. Poco alineada, se enfoca en aspectos no prioritarios

☐ 1. Nada alineada, la capacitación no aborda los riesgos reales

4. Prácticas de Seguridad Informática

¿Con qué frecuencia cambia sus contraseñas de acceso a los sistemas de la entidad?

☐ 5. Cada 3 meses o menos

☐ 4. Cada 6 meses

☐ 3. Una vez al año

☐ 2. Solo cuando es obligatorio

☐ 1. Nunca cambia sus contraseñas

¿Usa diferentes contraseñas para cada sistema que maneja?

☐ 5. Siempre, cada sistema tiene una única contraseña

☐ 4. Casi siempre, pero reutiliza algunas

☐ 3. A veces, usa la misma en algunos sistemas

☐ 2. Casi nunca, usa la misma en la mayoría

☐ 1. Siempre usa la misma contraseña en todos

¿Cómo almacena sus contraseñas?

☐ 5. Gestor de contraseñas seguro

☐ 4. Memorizadas o en un documento cifrado

☐ 3. Escritas en papel o documento sin seguridad

☐ 2. Comparte sus contraseñas con otros

☐ 1. No las recuerda, usa la misma en todo

¿Cómo reacciona ante un correo sospechoso de phishing?

☐ 5. Lo reporta y no lo abre

☐ 4. Lo elimina sin abrir

☐ 3. Lo revisa antes de tomar acción

☐ 2. Lo abre si parece importante

- ☐ 1. Lo abre y sigue enlaces sin verifica

5. Seguridad en los Sistemas de la Entidad

¿Cómo considera la seguridad de los sistemas internos de la entidad?

- ☐ 5. Muy segura, con protocolos avanzados
- ☐ 4. Segura, con algunas áreas de mejora
- ☐ 3. Moderadamente segura
- ☐ 2. Poca seguridad, alto riesgo
- ☐ 1. Sin medidas de seguridad efectivas

¿Los dispositivos USB y discos externos son revisados antes de ser usados en los equipos de la entidad?

- ☐ 5. Siempre, con análisis antivirus obligatorio
- ☐ 4. Casi siempre, pero no siempre con análisis
- ☐ 3. A veces, solo si hay sospecha de virus
- ☐ 2. Rara vez
- ☐ 1. Nunca

¿Cómo calificaría la efectividad del área de soporte técnico en respuesta a incidentes de seguridad?

- ☐ 5. Excelente, respuesta rápida y efectiva
- ☐ 4. Buena, pero con margen de mejora
- ☐ 3. Aceptable, pero con algunas fallas

- ☐ 2. Deficiente, poca respuesta efectiva

6. Cultura de Seguridad y Prevención

¿Qué tan comprometida cree que está la entidad con la seguridad informática?

- ☐ 5. Totalmente comprometida
- ☐ 4. Comprometida, pero con oportunidades de mejora
- ☐ 3. Moderadamente comprometida
- ☐ 2. Poco comprometida
- ☐ 1. Nada comprometida

¿Sabe a quién reportar un incidente de seguridad informática dentro de la entidad?

- ☐ 5. Sí, y lo haría de inmediato
- ☐ 4. Sí, pero dudo en algunos casos
- ☐ 3. No estoy seguro a quién reportar
- ☐ 2. No sé si hay un área encargada
- ☐ 1. No tengo idea de qué hacer

¿Considera que la entidad fomenta una cultura de seguridad informática en sus colaboradores?

- ☐ 5. Sí, constantemente promueve buenas prácticas y prevención
- ☐ 4. Sí, pero solo en ciertas áreas o en momentos específicos
- ☐ 3. Neutral, hay esfuerzos, pero no son constantes
- ☐ 2. No mucho, la seguridad informática no es una prioridad clara

☐ 1. No, no hay ninguna promoción o cultura de seguridad