UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE SOFTWARE

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SOFTWARE

“Propuesta de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la Empresa Pública de Agua Potable y Alcantarillado de Antonio Ante (EPAA-AA) en base a la normativa ISO/IEC 27001.”

AUTOR:

Jonathan David Segovia Chiza

DIRECTOR:

PhD. Irving Marlon Reascos Paredes

Ibarra-Ecuador

2026

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1004470272		
APELLIDOS Y NOMBRES:	Segovia Chiza Jonathan David		
DIRECCIÓN:	San Roque, Pukará		
EMAIL:	jdsegoviac@utn.edu.ec / segoviajonathan57@gmail.com		
TELÉFONO FIJO:		**TELF. MÓVIL**	0967618627

DATOS DE LA OBRA	
TÍTULO:	Propuesta de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la Empresa Pública de Agua Potable y Alcantarillado de Antonio Ante (EPAA-AA) en base a la normativa ISO/IEC 27001.
AUTOR (ES):	Segovia Chiza Jonathan David
FECHA: AAAAMMDD	2026/02/06
CARRERA/PROGRAMA:	■ **GRADO** ☐ **POSGRADO**
TÍTULO POR EL QUE OPTA:	Ingeniero en Software
DIRECTOR:	Ph.D. Irving Marlon Reascos Peredes
ASESOR:	Ph.D. Marco Remigio Pusdá Chulde

AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Segovia Chiza Jonathan David, con cédula de identidad Nro. 1004470272, en calidad de autor (es) y titular (es) de los derechos patrimoniales de la obra o trabajo de integración curricular descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.

Ibarra, a los 6 días del mes de febrero de 2026

EL AUTOR:

Firmado electrónicamente por:
JONATHAN DAVID
SEGOVIA CHIZA
Validar únicamente con FirmaEC

Jonathan David Segovia Chiza

CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 6 días, del mes de febrero de 2026

EL AUTOR:

Jonathan David Segovia Chiza

CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 6 de febrero de 2026

Ph.D. Irving Marlon Reascos Paredes

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular "Propuesta de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la Empresa Pública de Agua Potable y Alcantarillado de Antonio Ante (EPAA-AA) en base a la normativa ISO/IEC 27001", el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

IRVING MARLON REASCOS PAREDES

Firmado digitalmente por IRVING MARLON REASCOS PAREDES
Fecha: 2026.02.06 08:44:29 -05'00'

Ph.D. Irving Marlon Reascos Paredes

C.I. 1001501400

DIRECTOR DE TRABAJO DE GRADO

DEDICATORIA

Este trabajo se lo dedico a todos mis seres queridos, amigos y personas que han estado siempre conmigo en este largo proceso, apoyándome, animándome, dándome consejos de vida para que pueda lograr y cumplir esta meta que me había propuesto.

A mi madre Rosa Segovia, por estar siempre apoyándome en todo momento y ser mi pilar fundamental, mi más claro ejemplo de lucha y por demostrar el gran amor incondicional que tiene hacia mí.

A mi tía Eugenia Segovia, que ha sido como mi segunda madre, quien confió plenamente en mí desde el principio y siempre me ha brindado su apoyo mediante sus sabios consejos, su amor sincero y por siempre estar siempre cuando más lo necesitaba.

A mis familiares cercanos, por brindarme su cariño, apoyo, por esas pequeñas palabras que me decían que para mí eran un respaldo y una fuente de energía para seguir adelante.

A mis amigos cercanos y docentes de la Universidad, porque sin ellos este sueño no sería posible alcanzarlo, ya que compartimos juntos esta travesía universitaria, con enseñanzas, aprendizaje, unión, felicidad y sobre por convertirse en mi segunda familia.

Este logro es tan de ustedes como mío. Hoy puedo decir que lo logré… pero lo logramos juntos.

Jonathan David Segovia Chiza

AGRADECIMIENTO

He llegado a este punto tan importante en mi vida, donde quiero expresar mi sincero agradecimiento a todas las personas que me brindaron su apoyo, orientación y acompañamiento durante esta travesía.

Quiero agradecer primeramente a Dios, por brindarme fortaleza, salud, sabiduría y por ser mi fuente de energía y vida, por guiarme y demostrarme que confiando en él lo puedo conseguir todo y que sin su ayuda esto no sería posible.

A mi madre, porque es lo más importante, único y valioso que tengo en mi vida, por cada madrugada, por cada lágrima derramada hacia mí, por cada oración, desvelo, lucha, amor incondicional y esfuerzo, a pesar de estar sola nunca hubo impedimento para estar siempre conmigo, por cada palabra que me levantó cuando sentía que no podía más, y por enseñarme que no importa lo difícil que sea el camino, siempre se puede llegar si se avanza con el corazón firme.

A mi tía, porque siempre me apoyo tanto económica y emocionalmente para alcanzar este sueño, sin cuestionarme y dándome la confianza en su totalidad sin importarle lo que decían los demás, agradezco cada palabra de motivación que me da para no rendirme y seguir adelante a pesar de las adversidades que se presentan.

A mi familia por confiar en mi y estuvieron presentes para darme una palabra de ánimo o una mano cuando más lo necesité.

Y por último agradecer a mis amigos y compañeros de la carrera con los que hemos compartido momentos de alegría, tristeza, triunfos, ya que a pesar de todo seguíamos unidos apoyándonos el uno al otro, sin cuestionarnos con el fin de llegar al mismo propósito que era cumplir nuestros sueños. También expresar un agradecimiento especial a mi director y asesor de tesis, cuyo acompañamiento, dedicación y orientación fueron fundamentales para el desarrollo de este trabajo y extender mi gratitud a la entidad que, de alguna forma, colaboraron para que este trabajo pudiera realizarse de manera exitosa.

Jonathan David Segovia Chiza

RESUMEN EJECUTIVO

La seguridad de la información es un aspecto esencial para las organizaciones públicas que gestionan información crítica y prestan servicios básicos. La protección de los activos de información, junto con los procesos, personas y recursos tecnológicos que los soportan, es fundamental para garantizar la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de los procesos institucionales. En este contexto, la norma ISO/IEC 27001 constituye un referente para la gestión sistemática de la seguridad de la información.

En la Empresa Pública de Agua Potable y Alcantarillado de Antonio Ante (EPAA-AA), los activos de información, los procesos institucionales, los sistemas tecnológicos y el personal se encuentran expuestos a diversos peligros de seguridad, tales como accesos no autorizados, pérdida o alteración de la información, interrupciones en los servicios, deficiencias en la gestión de riesgos y vulnerabilidades tecnológicas, lo que incrementa la probabilidad de incidentes que afectan la continuidad operativa.

El objetivo general de la investigación fue desarrollar una propuesta de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la EPAA-AA, basada en la norma ISO/IEC 27001. El estudio se desarrolló con un enfoque aplicado y una metodología cuantitativa, empleando análisis documental y encuestas al personal, lo que permitió realizar un diagnóstico del estado actual de la seguridad de la información.

Como resultado del diagnóstico, se identificaron brechas relacionadas con la ausencia de políticas de seguridad, debilidades en la gestión de activos, falta de un proceso estructurado de gestión de riesgos, controles insuficientes y limitada concienciación del personal. A partir de estos resultados, se elaboró la propuesta de un SGSI, que contempla la identificación y valoración de activos, el análisis y tratamiento de riesgos mediante MAGERIT v3, y la definición de políticas, controles y planes de acción alineados a la ISO/IEC 27001.

Finalmente, se concluye que los peligros identificados representan una amenaza significativa para la información y los procesos institucionales de la EPAA-AA, por lo que la propuesta desarrollada constituye una base técnica y normativa para fortalecer la gestión de la seguridad de la información.

Palabras clave: Sistema de Gestión de la Seguridad de la Información, ISO/IEC 27001, Magerit, Gestión de riesgos.

ABSTRACT

Information security is an essential aspect for public organizations that manage critical information and provide basic services. The proper protection of information assets, together with the processes, people, and technological resources that support them, is fundamental to ensure the confidentiality, integrity, and availability of information, as well as the continuity of institutional processes. In this context, the ISO/IEC 27001 standard constitutes a reference framework for the systematic management of information security.

At the Antonio Ante Public Water Supply and Sewerage Company (EPAA-AA), information assets, institutional processes, technological systems, and personnel are exposed to various **security threats**, such as unauthorized access, loss or alteration of information, service disruptions, deficiencies in risk management, and technological vulnerabilities, which increase the likelihood of incidents affecting operational continuity.

The general objective of this research was to develop a proposal for an Information Security Management System (ISMS) for EPAA-AA, based on the ISO/IEC 27001 standard. The research was conducted using an applied approach with a quantitative methodology, employing documentary analysis and staff surveys, which made it possible to carry out a diagnosis of the current state of information security.

As a result of the diagnosis, gaps were identified related to the absence of security policies, weaknesses in asset management, the lack of a structured risk management process, insufficient security controls, and limited staff awareness. Based on these results, an ISMS proposal was developed, which includes the identification and valuation of assets, risk analysis and treatment using the MAGERIT v3 methodology, and the definition of policies, controls, and action plans aligned with ISO/IEC 27001.

Finally, it is concluded that the identified threats represent a significant risk to the information and institutional processes of EPAA-AA; therefore, the proposed ISMS constitutes a technical and regulatory foundation to strengthen information security management and serve as a reference for future implementation.

Keywords: Information Security Management System, ISO/IEC 27001, Magerit, Risk Management.

LISTA DE SIGLAS

BS 7799: Norma Británica relacionada con la seguridad de la información

CID: Confidencialidad, integridad y disponibilidad

COBIT: Objetivos de Control para la Información y Tecnologías Relacionadas

EPAA-AA: Empresa Pública de Agua Potable y Alcantarillado de Antonio Ante

IEC: Comisión Electrotécnica Internacional

ISO: International Organization for Standardization

ISO/IEC 27001: norma internacional para el SGSI, creada por la ISO y la IEC

ITIL: Biblioteca de Infraestructura de Tecnologías de la Información

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

NIST: Instituto Nacional de Estándares y Tecnología

OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation

PDCA / PHVA: Planificar – Hacer – Verificar – Actuar (ciclo de mejora continua)

RMF: Marco de gestión de riesgos

SI: Seguridad de la información

SGSI: Sistema de Gestión de la Seguridad de la Información

TIC: Tecnologías de la Información y Comunicación

TI: Tecnologías de la Información

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Problema de investigación

La creciente digitalización y dependencia de sistemas informáticos en la EPAA-AA ha evidenciado la necesidad de fortalecer la seguridad de la información con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de los datos, aspectos críticos en el funcionamiento institucional [1]; en este sentido, la empresa enfrenta desafíos significativos en la protección de información sensible y confidencial.

Según el informe de ESET Security Report de 2023, el phishing presenta una de las mayores amenazas con una probabilidad de ocurrencia del 70%, seguido de la infección con códigos maliciosos (63%) y el robo de credenciales de acceso (56%), en el mismo estudio se identifican los países más afectados: Ecuador (8%), seguido por Costa Rica (7.2%), Colombia (5.7%), Guatemala (5.2%) y El Salvador (5.1%) [2].

La carencia de un marco estructurado para la gestión de la seguridad de la información expone a la institución a riesgos tales como: la vulnerabilidad de los sistemas, la pérdida o filtración de datos, el acceso no autorizado, la confidencialidad y disponibilidad de la información institucional , cuya protección representa grandes desafíos relacionados con la limitación de recursos, la resistencia al cambio organizativo y complejidades inherentes a la adaptación de estándares internacionales a la realidad local.

Frente a estos desafíos, el presente estudio se centra en desarrollar una propuesta de SGSI basada en la normativa ISO/IEC 27001, que integre un enfoque sistemático para la identificación, evaluación y mitigación de riesgos; para lo cual, mediante la aplicación de metodologías como Magerit v3 y el ciclo PDCA, se busca proporcionar a la EPAA-AA un marco integral que no solo optimice sus procesos de seguridad, sino que también fortalezca la confianza de los ciudadanos y asegure la continuidad operativa.

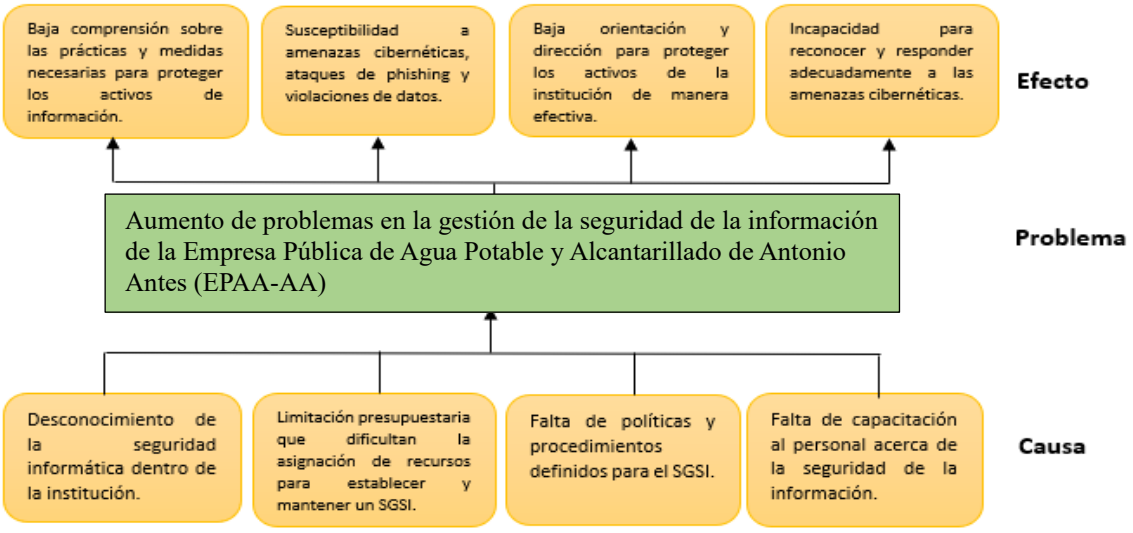

Figura 1: Árbol de problemas.

Justificación

La presente investigación está alineada con el objetivo 16 de los Objetivos de Desarrollo Sostenible, que se enfoca en promover sociedades justas, pacíficas e inclusivas, y en específico se relaciona con la meta 16.6 que busca crear capacidades para que todos los niveles instituciones rindan cuentas [3]. Además, coopera con el cumplimiento del Objetivo 9 del Plan de Creación de Oportunidades 2021-2025 que establece: "Garantizar la seguridad ciudadana, orden pública y gestión de riesgos" [4].

Justificación Metodológica. – La metodología Magerit v3, proporciona un marco probado para guiar el proceso, asegurando la efectividad y coherencia, facilitando la evaluación continua y la mejora de las prácticas de seguridad, garantizando la adaptabilidad y la respuesta efectiva ante las amenazas en constante evolución.

Justificación Tecnológica. - El desarrollo de este trabajo reside en la creciente importancia de proteger los activos de información, que son cada vez más vulnerables a amenazas, fortaleciendo la capacidad de la institución para salvaguardar la confidencialidad, integridad y disponibilidad de los datos.

Objetivos

Objetivo General

Desarrollar una propuesta de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la Empresa Pública de Agua Potable y Alcantarillado de Antonio Ante (EPAA-AA) en base a la normativa ISO/IEC 27001.

Objetivo específico

- Establecer un marco teórico acerca la Gestión de Seguridad de la Información dentro de las instituciones públicas en base a la Norma ISO/IEC 27001.
- Realizar un diagnóstico sobre la Seguridad de la Información de la Empresa Pública de Agua Potable y Alcantarillado de Antonio Ante (EPAA-AA) en base a la norma ISO 27001 y la metodología Magerit v3.
- Construir la propuesta del Sistema de Gestión de Seguridad de la Información (SGSI), mediante la integración de los requisitos de la norma ISO/IEC 27001.

CAPÍTULO I

MARCO TÓRICO

1.1 Introducción a la Seguridad de la Información (SI)

1.1.1 Definición

La SI es una disciplina que tiene como objetivo proteger los datos y activos informáticos frente a amenazas internas y externas para evitar accesos no autorizados, modificaciones indebidas, pérdida o destrucción de la información, por lo que la gestión adecuada de la seguridad de la información es fundamental para garantizar que los datos críticos estén protegidos y disponibles cuando se los necesite [5].

La SI no solo se limita al uso de tecnologías como antivirus, firewalls o cifrado, sino que también incluye la creación de políticas organizacionales, procedimientos administrativos y programas de concienciación dirigidos al personal, considerando que el factor humano es uno de los elementos más importantes y, a la vez, más vulnerables dentro de la gestión de seguridad, lo que genera la necesidad de incorporar procesos sostenidos de capacitación con el objetivo de reducir riesgos asociados a errores, negligencia o malas prácticas [6].

Adicionalmente se debe considerar que en la actualidad las organizaciones dependen en gran medida de la tecnología para la generación de sus productos y servicios, por lo que la SI se ha convertido en un factor de suma importancia que va más allá de proteger datos sino también salvaguarda la reputación, incrementar la confianza del cliente y finalmente el cumplimiento de normativas legales.

1.1.2 Principios de confidencialidad, integridad y disponibilidad (CID)

Acorde a lo indicado por [5], en la figura 2 se muestra la protección eficaz de los datos que se apoya en tres pilares fundamentales:

- Confidencialidad: es la garantía de que la información solo sea accesible para personas, entidades o procesos debidamente autorizados, el objetivo es la protección de los datos

sensibles frente a accesos no autorizados, fugas de información o divulgaciones involuntarias.

- Integridad: consiste en garantizar que la información se conserve completa, exacta y consistente, sin modificaciones no autorizadas, desde su creación hasta su eliminación o destrucción. El objetivo es la preservación de la validez junto con la confiabilidad de los datos para así prevenir alteraciones accidentales.
- Disponibilidad: garantiza que la información y los servicios asociados se encuentren accesibles u operativos cuando se requieran. La finalidad es minimizar interrupciones en procesos y servicios críticos mediante políticas de continuidad del negocio, planes de recuperación ante desastres, así como también con una gestión eficaz de incidentes.

Figura 2: Pilares fundamentales para la protección. Adaptado de [5]

1.1.3 Riesgos y amenazas en la gestión de la SI

Entender las diferencias y semejanzas entre riesgos y amenazas es necesario para optimizar la gestión de la SI.

- Los riesgos se refieren a la probabilidad de que ocurra un incidente que comprometa la CID de los datos [7].
- Las amenazas son los agentes o eventos que explotan esas vulnerabilidades y pueden causar daños a la información [8].

1.1.4 Activos de información y su clasificación

Acorde a lo indicado por [9]; a continuación, se describen los activos de información a ser considerados:

- **Datos y bases de datos:** información digital que respalda operaciones, registros de clientes, transacciones, etc
- **Software y aplicaciones:** programas y sistemas operativos que permiten el procesamiento y la gestión de datos
- **Hardware y equipos:** computadoras, servidores, dispositivos móviles y otros equipos físicos
- **Documentación y archivos:** manuales, políticas, procedimientos, informes y documentación técnica
- **Infraestructura de redes:** elementos de conectividad, dispositivos de red y sistemas de telecomunicación
- **Reputación e imagen corporativa:** la percepción y credibilidad que la organización tiene en el mercado
- **Conocimiento y experiencia:** know-how y habilidades del personal que aportan valor estratégico

La comprensión de esta clasificación permite asignar niveles de protección específicos según la sensibilidad de la información, de la misma manera el impacto potencial que su divulgación, alteración o pérdida podría generar en la organización [10] de acuerdo con la siguiente categorización:

- **Confidencial:** información altamente sensible que solo puede ser accedida por personal autorizado, su divulgación podría causar daños significativos
- **Interno:** información restringida a empleados o departamentos específicos dentro de la organización, cuya exposición no autorizada podría comprometer la operatividad o seguridad interna
- **Público:** información destinada a ser difundida o compartida con el público general, sin que ello implique riesgos para la organización

1.1.5 Normas y estándares internacionales para la SI

Desde la década de los 80 se han establecido buenas prácticas y estándares que se han posicionado a nivel mundial, los más representativos se detallan a continuación:

- **ISO/IEC 27001:** estándar internacional para la implementación de un SGSI
- **ISO/IEC 27002:** código de buenas prácticas para la gestión de la SI, que complementa la ISO/IEC 27001
- **ISO/IEC 27005:** enfocado en la gestión de riesgos de SI, proporcionando directrices para identificar, evaluar y tratar los riesgos
- **NIST Cybersecurity Framework:** marco de ciberseguridad que establece procedimientos para la identificación, protección, detección, respuesta y recuperación ante incidentes de seguridad
- **NIST SP 800-53:** conjunto de controles de seguridad y privacidad recomendado para el ámbito gubernamental y la infraestructura crítica
- **COBIT:** marco de referencia para la gobernanza y gestión de las TI, que incluye directrices para la SI
- **PCI-DSS:** estándar de seguridad enfocado en proteger los datos de los titulares de tarjetas y garantizar transacciones seguras

1.1.6 Importancia de la SI en la era digital

En la era digital, la creciente dependencia de sistemas informáticos, redes y plataformas en línea ha generado una cantidad masiva de datos que requieren protección constante (información confidencial de clientes o estrategias empresariales de crecimiento), lo que ha generado que la SI se convierta en un pilar para el funcionamiento de todo tipo de organización [5].

Uno de los principales riesgos en el entorno digital es la exposición a amenazas cibernéticas, como el robo de información, ataques de malware, phishing o secuestro de datos (ransomware), cuyos resultados pueden atraerles a las empresas pérdidas económicas, interrupciones en los servicios, sanciones legales y desconfianza por parte de los clientes y socios estratégicos, lo que genera la necesidad de contar con un enfoque sólido de SI que permita anticiparse a estas amenazas y de

tener las herramientas necesarias para responder de forma eficaz ante incidentes, minimizando su impacto [6].

1.2 Normativa ISO/IEC 27001

1.2.1 Historia y evolución

Su historia se inicia con la serie denominada BS 7799, desarrollada en el Reino Unido entre las décadas de los 80 y los 90 que se centró en la creación de un marco de trabajo que permitiera a las organizaciones gestionar de manera sistemática la seguridad de sus activos informativos con el objetivo de establecer procedimientos y controles efectivos en un entorno donde las amenazas a la seguridad comenzaban a tomar relevancia [11].

A medida que el entorno tecnológico evolucionó y las necesidades empresariales se tornaron más complejas, surgió la necesidad de formalizar y estandarizar las prácticas de SI a nivel internacional, lo que desencadenó que la ISO y la IEC adoptaron la serie BS 7799, transformándola en lo que hoy conocemos como la norma ISO/IEC 27001, lo que marcó un hito sin precedentes en la industria ya que se generaron los mecanismos necesarios para la adopción de un SGSI capaz de ser adaptado y acoplado a todo tipo de industrias [12].

Con estas consideraciones la versión 2005 introdujo importantes mejoras y clarificaciones llegando a consolidar un marco capaz de integrar tanto aspectos técnicos como organizacionales; finalmente, la versión de 2013 se enfocó en generar lineamiento que faciliten implementación de un SGSI en diferentes tipos de organizaciones e introdujo un fuerte componente enfocado en promover una cultura de mejora continua en la gestión de la SI [11]; finalmente, la versión 2022 integra una estructura más armonizada y clara conforme al enfoque de alto nivel (Annex SL), lo cual facilita la integración del SGSI con otros sistemas de gestión como ISO 9001 o ISO 14001; así como la mayor claridad en los requisitos sobre auditoría interna, revisión por la dirección y comunicación [12], tal como se ilustra en la Figura 3.

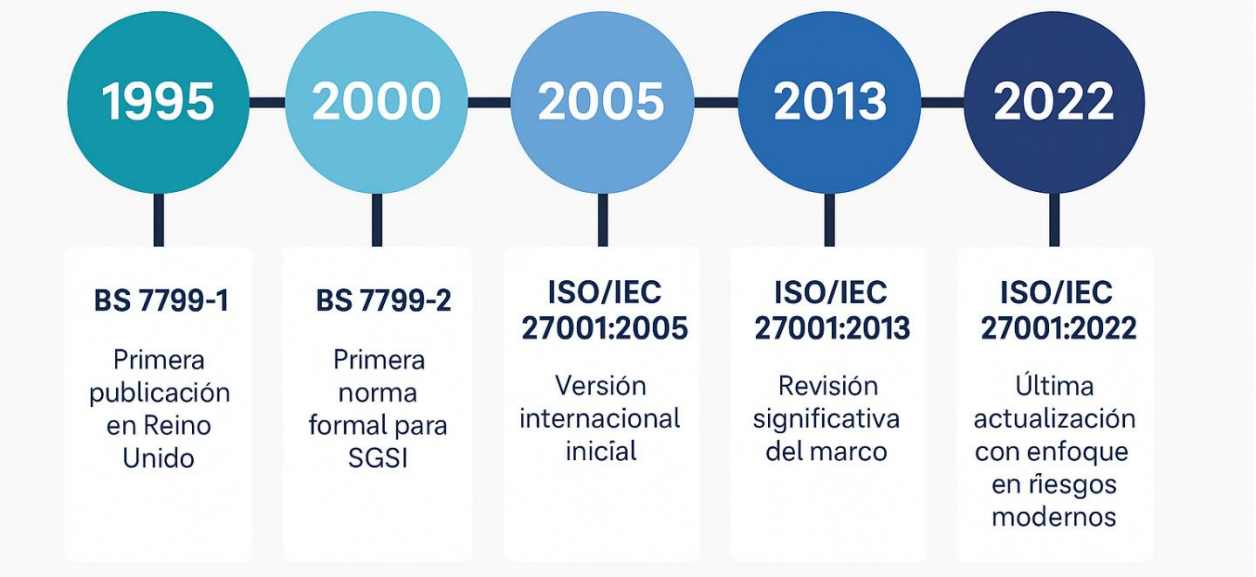

Figura 3: Línea del tiempo de la ISO/IEC 27001. Adaptado de [11] y [12].

1.2.2 Estructura y requisitos principales de la norma

La ISO/IEC 27001 es una norma internacional que establece los requisitos para implementar, mantener, así como mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI) cuya estructura se basa en el modelo de alto nivel (High Level Structure – HLS) común a otras normas ISO, lo que facilita su integración con otros sistemas de gestión, como los de calidad (ISO 9001) o medio ambiente (ISO 14001) [10]. Las principales cláusulas de la norma se resumen en la TABLA 1.

TABLA 1
Principales cláusulas de la norma.

Cláusula	Descripción
Cláusula 4	Se enfoca en comprender el contexto de la organización, identificando factores internos y externos, y definiendo el alcance del SGSI.
Cláusula 5	Establece la necesidad del liderazgo y compromiso de la alta dirección, así como la definición de una política de seguridad de la información.
Cláusula 6	Aborda la planificación, donde se deben identificar los riesgos y oportunidades, establecer objetivos de seguridad y planificar acciones para abordarlos.
Cláusula 7	Se enfoca en el soporte, abarcando la gestión de recursos, la competencia del personal, la concienciación, la comunicación y el control de la documentación.
Cláusula 8	Se centra en la operación, incluye la implementación y control de procesos necesarios para alcanzar los objetivos del SGSI, incluyendo el tratamiento de riesgos.
Cláusula 9	Se centra en la evaluación del desempeño, exigiendo el monitoreo, medición, análisis, auditoría interna y revisión por la dirección del sistema.
Cláusula 10	Establece los requisitos para la mejora continua, incluyendo la gestión de no conformidades y acciones correctivas.

Nota: La table describe las principales cláusulas a ser consideradas. Adaptado de [13].

Además de las cláusulas principales, la norma incluye el Anexo A, que contiene una lista de controles de seguridad clasificados en 4 grandes áreas temáticas (organizacionales, de personas, físicos y tecnológicos) y divididos en 93 controles en la versión 2022 que se utiliza como referencia para seleccionar los controles que sean relevantes según los riesgos identificados en la organización.

1.2.3 Beneficios de implementar un SGSI basado en ISO/IEC 27001

En concordancia con [14] en la TABLA 2 se describen los principales beneficios de implementar un SGSI basado en ISO/IEC 27001.

TABLA 2
Principales beneficios de implementar un SGSI.

Beneficio	Descripción
Protección integral de la información	Salvaguarda la confidencialidad, integridad, junto con la disponibilidad de los datos
Reducción de riesgos	Identifica mientras mitiga amenazas, vulnerabilidades y brechas de seguridad de forma estructurada

Beneficio	Descripción
Cumplimiento normativo	Facilita la conformidad con leyes de protección de datos y regulaciones internacionales
Mejora de la reputación y confianza	Aumenta la confianza de clientes, proveedores y partes interesadas al demostrar compromiso con la seguridad
Ventaja competitiva en el mercado	Diferencia a la organización frente a competidores que no tienen un SGSI certificado
Continuidad del negocio	Reduce el impacto de incidentes de seguridad y mejora la capacidad de recuperación ante crisis
Eficiencia operativa	Optimiza procesos internos mediante la documentación, monitoreo y mejora continua
Cultura organizacional proactiva en seguridad	Fomenta la concienciación del personal y la participación activa en la protección de la información
Facilidad para auditorías internas y externas	Estandariza procesos y controles que permiten una mejor preparación para auditorías
Adaptabilidad frente a nuevas amenazas	Permite ajustar el sistema de forma dinámica según el entorno tecnológico y los riesgos emergentes

Nota: La tabla describe los principales beneficios de un SGSI. Adaptado de [14]

1.3 Sistemas de Gestión de la Seguridad de la Información (SGSI)

1.3.1 Definición

Los SGSI se enfocan en proteger los activos de información en el ámbito empresarial de manera continua y estructurada [15] mediante la incorporación de aspectos técnicos (soluciones de cifrado, firewalls o sistemas de detección de intrusiones) y de componentes organizacionales y humanos (formación y concienciación del personal, la asignación de responsabilidades claras, y la elaboración de procedimientos y políticas que organicen el manejo de la información) [16].

El SGSI se fundamenta en el ciclo PDCA (Planificar, Hacer, Verificar y Actuar), que permite adaptar y actualizar las medidas de seguridad de acuerdo con las nuevas amenazas, tecnologías emergentes y cambios en el entorno organizacional con el objetivo de garantizar que el sistema no solo se mantenga efectivo en a través del paso del tiempo, sino que también evolucione y mejore en respuesta a los desafíos dinámicos de la SI [15]. Finalmente, la implementación de un SGSI proporciona una base que garantiza el cumplimiento de requisitos legales, normativos y

contractuales, lo que genera beneficios adicionales a las organizaciones como la mejora en la reputación de la organización.

1.3.2 Elementos clave de un SGSI

En concordancia con [16]; a continuación, se describen los elementos esenciales que conforman un SGSI integral, los cuales se presentan en la TABLA 3.

TABLA 3
Elementos de un SGSI.

Elemento	Descripción
Política de SI	Es el documento que establece el compromiso, objetivos, junto con las directrices para proteger los activos de información empresariales
Gestión de activos	Implica la identificación, clasificación, junto con la valoración de los activos de información, de modo que se puedan definir los niveles de protección adecuados
Gestión de riesgos	Consiste en el análisis y evaluación de las amenazas con vulnerabilidades existentes, para de esa manera establecer medidas de control o tratamiento que minimicen el impacto potencial
Controles de seguridad	Son las medidas tanto técnicas, organizativas, como físicas que permiten mitigar los riesgos
Capacitación y concienciación	Se refiere a la formación continua del personal para promover buenas prácticas junto con una cultura de seguridad
Monitoreo y auditoría	Involucra el seguimiento constante del desempeño del SGSI mediante revisiones, auditorías internas, junto a análisis de incidentes
Mejora continua	Basada en el ciclo PDCA, este elemento garantiza que el SGSI se actualice mientras se optimiza de forma regular para adaptarse a nuevas amenazas

Nota: La tabla describe los elementos clave de un SGSI. Adaptado de [16]

1.3.3 Ciclo PDVA (Planificar, Hacer, Verificar, Actuar)

Es una metodología de mejora continua que permite gestionar de forma dinámica y adaptativa la SI; a continuación, en concordancia con [17] se describen las fases que lo conforman, tal como se ilustra en la Figura 4.

Figura 4: Ciclo PDVA. Tomado de [17]

1.3.4 Responsabilidades y roles en la gestión de la SI

A continuación se detallan los roles importantes junto con las responsabilidades asociadas que garantizan la protección integral de los activos informativos en la organización [15]:

- **Alta dirección:** es el nivel ejecutivo que establece la visión estratégica, aprueba las políticas y asigna los recursos para la protección de datos
- **Responsable de SI:** este rol se encarga de diseñar, implementar y mantener el SGSI, coordinando las acciones de seguridad
- **Equipo de seguridad y TIC:** compuesto por administradores de sistemas, redes y aplicaciones, este equipo implementa controles técnicos, monitorea sistemas, gestiona actualizaciones y responde ante incidentes de seguridad

- **Auditores internos de seguridad:** su función es realizar auditorías que permitan identificar áreas de mejora y verificar la eficacia de los controles implementados
- **Responsable de continuidad del negocio:** su objetivo es asegurar que, en caso de incidentes, las operaciones críticas de la organización puedan reanudarse con la menor interrupción posible
- **Usuarios y personal de la organización:** la concienciación, capacitación y el reporte oportuno de incidentes son fundamentales para mantener un entorno seguro y protegido
- **Gestor de riesgos:** encargado de identificar, evaluar y monitorear los riesgos asociados a la SI, adicionalmente se encarga de desarrollar estrategias de mitigación y participa en la toma de decisiones para minimizar el impacto de posibles amenazas en la organización

1.4 Implementación de un SGSI en Base a ISO/IEC 27001

1.4.1 Análisis del contexto organizacional y partes interesadas

Se trata de un proceso fundamental que permite comprender los factores internos y externos que pueden influir en el logro de los objetivos del SGSI, el cual comprende el estudio del entorno legal, tecnológico, económico, social y cultural, así como la evaluación de las capacidades internas de la organización, como su estructura, procesos, recursos y cultura organizacional con el objetivo principal de establecer un marco claro sobre la realidad en la que opera la institución, lo cual permite definir un SGSI alineado a sus necesidades, amenazas y prioridades reales [18].

La identificación de las partes interesadas implica el reconocimiento de todos los actores que pueden afectar, verse afectados o tener expectativas respecto al SGSI, con eso se comprende tanto sus necesidades como requisitos en relación con la SI, lo cual permite alinear los objetivos de seguridad con los intereses organizacionales y del entorno, fortaleciendo la toma de decisiones estratégicas junto con la eficacia general del sistema [19].

1.4.2 Evaluación de riesgos y tratamiento de riesgos de SI

La evaluación permite identificar, analizar y valorar las amenazas que podrían comprometer la confidencialidad, integridad o disponibilidad de los activos informáticos; para lo cual, según [20] es necesario:

- Identificar los activos de información existente
- Determinar sus vulnerabilidades
- Evaluar las posibles amenazas a las que están expuestos
- Calcular el nivel de riesgo en función de la probabilidad de ocurrencia y el impacto potencial.

Por otro lado, el tratamiento de riesgos es la fase en la que se decide cómo abordar los riesgos identificados durante la evaluación mediante la aplicación de diferentes estrategias como mitigarlo, transferirlo a terceros o aceptarlo si su nivel es tolerable; en este sentido, el tratamiento de riesgos es una actividad dinámica que debe revisarse continuamente para adaptarse a los cambios tecnológicos, organizacionales o regulatorios, garantizando así una protección constante y eficaz de la información. [21].

1.4.3 Definición de la política de SI

Es un proceso que permite establecer el marco general sobre el cual se desarrollarán todos los controles, procedimientos y actividades relacionadas con la protección de los activos informáticos, para lo cual, acorde a lo determinado por [18] se deben cumplir con las siguientes actividades:

- Compromiso de la alta dirección, quien debe liderar y aprobar el desarrollo de la política, garantizando que esté alineada con los objetivos estratégicos de la organización, el contexto en el que opera y los requisitos legales o normativos aplicables.
- Identificación de los principios fundamentales que deben regir el comportamiento de la organización en relación con la seguridad de la información, esto incluye aspectos como la confidencialidad, integridad con disponibilidad de los datos, la asignación de responsabilidades, la concienciación del personal, el cumplimiento normativo o el tratamiento de incidentes.
- Definición de los objetivos de seguridad y el establecimiento de criterios de cumplimiento que permitan medir la efectividad de la política durante el tiempo de ejecución.

Finalmente, es importante recalcar que la política debe ser formalmente documentada, comunicada y difundida a todos los empleados y partes interesadas relevantes, considerando adicionalmente

proceso de sensibilización y formación continua al personal como mecanismos para garantizar que la política no solo se conozca, sino que también se aplique en la práctica [19].

1.4.4 Controles y medidas de seguridad según el Anexo A de ISO/IEC 27001

El Anexo A de la norma ISO/IEC 27001 constituye un compendio de controles y medidas de seguridad que sirven como referencia para el tratamiento de los riesgos identificados en el SGSI, este anexo agrupa 93 controles organizados en diversas áreas, tales como la seguridad organizacional, la gestión de activos, el control de acceso, la seguridad en las comunicaciones, la protección física, la seguridad de las operaciones y la gestión de incidentes, entre otras (ver Anexo 1).

1.4.5 Auditoría y mejora continua del SGSI

Se trata de un proceso sistemático y documentado que permite evaluar la manera en que el sistema cumple con los requisitos establecidos por la organización y por la norma ISO/IEC 27001 con el propósito de evidenciar la eficacia de los controles implementados; para lo cual, se detectan posibles desviaciones, se identifican áreas de mejora y se garantiza que el sistema se mantenga alineado con los objetivos estratégicos [22].

La mejora continua del SGSI es un principio fundamental que asegura su evolución y adaptación frente a nuevas amenazas, cambios tecnológicos y necesidades organizacionales que se basa en el ciclo PHVA (Planificar, Hacer, Verificar, Actuar) con el objetivo de corregir deficiencias y fortalecer la efectividad del sistema como mecanismo estratégico para la gestión proactiva del riesgo y la protección de los activos de información [23].

1.5 Modelos y metodologías para la gestión de riesgos

1.5.1 Metodología OCTAVE

La metodología OCTAVE es un enfoque integral para la gestión de riesgos impulsada por el Instituto de Ingeniería de Software de la Universidad Carnegie Mellon con el objetivo de identificar los activos de información más importantes, evaluar las amenazas y vulnerabilidades asociadas, y determinar los riesgos que deben ser tratados para proteger la información crítica [24].

Uno de los elementos distintivos es su enfoque participativo a través del involucramiento activo del personal de la organización en el proceso de análisis mediante técnicas cualitativas como talleres, entrevistas y grupos de trabajo que permiten recopilar información directa de quienes conocen a fondo los procesos y los riesgos del entorno operativo con el objetivo de identificar de manera más precisa las amenazas y tener una mejor comprensión de la relación entre los activos de información, los procesos de negocio y los posibles impactos.

1.5.2 Metodología MAGERIT

La metodología MAGERIT es un enfoque estructurado desarrollado por la administración pública española, con el objetivo de identificar, analizar y gestionar los riesgos asociados a los sistemas de información que permite garantizar la seguridad de los activos de información mediante un análisis sistemático de las amenazas, vulnerabilidades y consecuencias potenciales, proporcionando a las organizaciones una base sólida para la toma de decisiones en materia de protección de datos [25].

Una de las ventajas de MAGERIT es su alineación con los principios de la gestión de riesgos y las normativas internacionales, como la ISO/IEC 27001 mediante procesos que permiten evaluar y tratar los riesgos de forma metódica, fomentando una cultura de gestión proactiva de la seguridad, permitiendo a las organizaciones proteger sus sistemas de información, cumplir con la normativa vigente y asegurar la continuidad de sus operaciones frente a posibles incidentes [25].

1.5.3 Metodología NIST RMF

La metodología NIST RMF es un marco desarrollado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, diseñado para proporcionar un enfoque estructurado y flexible en la gestión de riesgos en sistemas de información con el objetivo de integrar la gestión de riesgos de seguridad y privacidad dentro del ciclo de vida de los sistemas, ayudando a las organizaciones a tomar decisiones informadas sobre la protección de sus activos informáticos y a cumplir con requerimientos normativos y regulatorios [26].

Una de las principales fortalezas de esta metodología es su enfoque dinámico y cíclico, que promueve la mejora continua y la capacidad de adaptación frente a amenazas emergentes y cambios tecnológicos, lo cual la diferencia del resto de enfoques estáticos proporcionando proporciona una

base sólida para gestionar la seguridad y la privacidad de la información de manera proactiva, integrando la gestión de riesgos con los procesos organizativos.

1.6 Beneficios y desafíos de la implementación de un SGSI

1.6.1 Beneficios operacionales y estratégicos

Para [22] la implementación de un SGSI aporta los siguientes beneficios operacionales:

- Permite que la organización optimice sus procesos internos y mejore la eficiencia en la gestión de la SI
- Reduce los incidentes y vulnerabilidades mediante la aplicación de controles sistemáticos y protocolos de seguridad
- Reduce los tiempos de interrupción operacionales
- Permite tener la capacidad de dar respuesta rápida ante los incidentes
- Brinda herramientas para la identificación de áreas de mejora

Desde una perspectiva estratégica, un SGSI robusto fortalece la confianza de clientes, socios y partes interesadas, mejorando la reputación de la organización en el mercado, lo que respalda el compromiso de la empresa con la seguridad y la protección de datos, lo cual puede ser un factor decisivo en licitaciones, contratos y relaciones comerciales [22].

1.6.2 Desafíos para la implementación de un SGSI

A continuación, en concordancia con [21] se describen los principales desafíos para la implementación de un SGSI:

- **Limitaciones de recursos:** la implementación requiere inversiones en tecnología, capacitación y personal especializado.
- **Compromiso de la alta dirección:** la ausencia de un liderazgo comprometido dificulta la asignación de recursos y el impulso de una cultura de seguridad.
- **Resistencia al cambio organizacional:** la introducción de nuevos procesos y controles puede generar resistencia entre los empleados.

- **Integración con procesos existentes:** adaptar y alinear el SGSI con las operaciones y sistemas actuales de la organización puede suponer un reto importante para asegurar la coherencia y efectividad del sistema.
- **Costos asociados:** los gastos en tecnología, consultoría y formación pueden ser significativos, lo que dificulta la implementación en organizaciones con presupuestos ajustados.
- **Mantenimiento y mejora continua:** el SGSI requiere un monitoreo constante, auditorías y actualizaciones para mantenerse efectivo ante nuevas amenazas y cambios en el entorno.

1.6.3 Factores de éxito para la certificación en ISO/IEC 27001

Para [23] los principales factores de éxito que permiten alcanzar la certificación en la Norma ISO son:

- **Compromiso de la alta dirección:** su compromiso garantiza la asignación de recursos, la definición de políticas y la promoción de una cultura enfocada en la seguridad
- **Definición y comunicación de la política de seguridad:** establecer una política clara y bien comunicada es fundamental para orientar todas las actividades
- **Gestión integral de riesgos:** un enfoque sistemático permite priorizar las amenazas y vulnerabilidades, facilitando la implementación de medidas preventivas y correctivas
- **Capacitación y concienciación del personal:** un equipo bien formado y comprometido es capaz de cumplir y hacer cumplir las políticas de seguridad
- **Implementación y documentación de controles:** la adopción de controles de seguridad adecuados asegura que las medidas implementadas sean coherentes y replicables
- **Auditoría interna y revisión periódica:** permite verificar el cumplimiento de las políticas y asegurar que los controles funcionen de manera efectiva
- **Asignación de recursos adecuados:** una asignación adecuada de recursos asegura que las acciones se ejecuten correctamente y sean sostenibles a lo largo del tiempo

1.6.4 Casos de éxito y estudios de implementación de SGSI

- Tras la implementación de un SGSI robusto, IBM fortaleció significativamente sus procesos de gestión de la SI, permitiendo una identificación temprana para mitigar de manera eficaz las amenazas cibernéticas [27]
- Microsoft adoptó un SGSI integral para salvaguardar su vasto ecosistema digital, lo que le permitió establecer controles rigurosos y protocolos de respuesta ante incidentes, permitiéndole a la empresa mejorar su gestión de riesgos y la continuidad operativa de sus servicios [28]
- Telefónica ha logrado integrar un SGSI capaz de gestionar de manera proactiva los riesgos de SI cuyos resultados evidenciaron una considerable reducción de los incidentes de seguridad y mejorar la eficiencia operativa [29]
- Google ha consolidado su estrategia de seguridad mediante la implementación de un SGSI que cubre todos los niveles de su operación global, lo que le permite responder ágilmente a las amenazas y mantener la confidencialidad, integridad y disponibilidad de los datos [30]

CAPÍTULO II

MATERIALES Y MÉTODOS

2.1 Tipo y enfoque de investigación

Para el presente estudio se aplicó la investigación del tipo aplicada cuya principal característica es su orientación práctica y su enfoque en la solución de problemas reales dentro de un entorno específico, en este, el desarrollo de un SGSI para la EPAA-AA que permita mejorar la protección de sus activos informáticos y optimizar la gestión de riesgos asociados a la seguridad de la información.

Se recurrió al enfoque híbrido (cuantitativo, cualitativo) que permita no solo comprender en profundidad las percepciones, prácticas o políticas existentes en la EPAA-AA, sino también medir de forma objetiva el estado actual de la seguridad, identificar brechas, así como también sustentar la propuesta de mejora con datos empíricos.

2.2 Método de investigación

El método seleccionado fue el estudio de caso, esto debido a su capacidad para examinar la problemática de una forma contextualizada que integra el análisis de los procesos, los actores involucrados, los recursos disponibles, junto con las condiciones particulares de la organización, este enfoque resulta fundamental para el diseño de una propuesta de SGSI ajustada a las necesidades específicas de la entidad.

Con este método existe el beneficio de combinar diferentes fuentes de datos de consulta, lo que facilita la identificación precisa de las actuales debilidades y fortalezas en términos de seguridad, además de las posibilidades de mejora lo que permite el desarrollo de un diagnóstico exacto y la elaboración de sugerencias prácticas fundamentadas en pruebas tangibles.

Como complemento al estudio de caso, se empleó el método de encuesta mediante la aplicación de cuestionarios estructurados dirigidos al personal clave de la institución. Este método permitió recopilar información cuantitativa relacionada con el nivel de cumplimiento de los controles establecidos en el Anexo A de la norma ISO/IEC 27001, facilitando la identificación objetiva de

brechas de seguridad y fortaleciendo el diagnóstico sobre el estado actual de la seguridad de la información. La combinación de ambos métodos posibilitó un análisis integral, sustentado tanto en evidencia contextual como en datos medibles.

2.3 Diseño de la investigación

El presente proyecto adopta un diseño de investigación de tipo transversal, cuya principal característica es la recolección de datos en un único momento en el tiempo que permitió tener "fotografía" clara del estado actual de la SI en EPAA-AA identificando las brechas de seguridad, vulnerabilidades y riesgos que sustenten de manera óptima la propuesta de implementación del SGSI conforme a la norma ISO/IEC 27001.

2.4 Técnicas e instrumentos de recolección de datos

Para la recolección de datos se utilizaron las siguientes técnicas que permitieron obtener información completa y contextualizada sobre el estado actual de la SI:

- Revisión documental de normativas internacionales, estudios previos, metodologías de análisis de riesgos y literatura especializada en SI.
- Las entrevistas semiestructuradas permitieron complementar la información obtenida mediante el cuestionario, aportando criterios sobre prácticas actuales, roles institucionales y necesidades relacionadas con la seguridad de la información.
- Cuestionario estructurado al personal clave de la organización para contar con información cuantitativa valiosa sobre la realidad interna en materia de seguridad; para lo cual, se organizaron equipos de levantamiento de información para cada una de las 4 secciones del Anexo A.

La elaboración de un cuestionario que permita la identificación del nivel de cumplimiento de los controles establecidos en el Anexo A de la norma ISO/IEC 27001, se desarrolló de manera participativa al interior de la institución para lo que se involucró a un equipo multidisciplinario conformado por representantes de áreas importantes como tecnología, administración, procesos y gestión documental, con lo que se pudo adaptar el contenido del instrumento al contexto organizacional, garantizando su pertinencia.

El cuestionario fue sometido a un proceso de validación por parte de un experto en seguridad de la información, quien evaluó la coherencia técnica, la adecuación a los criterios de la norma, junto con la capacidad del instrumento en la obtención de información confiable, asegurando su validez antes de su aplicación definitiva (ver Anexo 2).

Adicionalmente, se emplearon entrevistas semiestructuradas dirigidas a personal clave de la EPAA-AA, perteneciente a áreas estratégicas como tecnología, administración, procesos y gestión documental. Esta técnica permitió profundizar en el conocimiento de las prácticas actuales de seguridad de la información, los roles y responsabilidades asociados, así como en la identificación de problemáticas operativas, riesgos percibidos y necesidades institucionales no evidenciadas únicamente a través del cuestionario.

La información obtenida mediante las entrevistas complementó los resultados cuantitativos, facilitando una interpretación contextualizada del estado de la seguridad de la información y aportando insumos cualitativos relevantes para la formulación de la propuesta del SGSI, asegurando su alineación con la realidad organizacional de la institución.

CAPÍTULO III

DIAGNÓSTICO DE LA EMPRESA

3.1 Antecedentes de la empresa

La EPAA-AA es una entidad municipal creada con el propósito de gestionar de manera técnica, eficiente y sostenible los servicios de agua potable y alcantarillado en el cantón Antonio Ante, provincia de Imbabura, cuya misión es fundamental para garantizar el acceso equitativo al agua segura y al saneamiento básico, contribuyendo así a la salud pública, el desarrollo social y la protección ambiental de la región [31].

Para cumplir con su misión la empresa se encarga del diseño, operación, mantenimiento y expansión de la infraestructura relacionada con la captación, tratamiento, distribución de agua potable y recolección de aguas residuales; para lo cual, en su accionar se aplican principios de calidad, responsabilidad social, transparencia en la gestión pública y compromiso con el desarrollo territorial [31].

Figura 5: Logo de la EPAA-AA. Tomado de [31].

Además, trabaja en coordinación con los gobiernos parroquiales, los municipios vecinos, la ciudadanía y otras entidades gubernamentales para fortalecer la gobernanza del agua, promover la educación ambiental y asegurar el cumplimiento de las normativas técnicas y legales vigentes que garanticen el servicio de dotación agua potable [31].

La empresa en los últimos años ha buscado la modernización de sus procesos mediante la incorporación de tecnologías de información, la actualización de sus sistemas operativos, así como la implementación de políticas orientadas a procesos tales como la eficiencia energética, la reducción de pérdidas o la mejora en la atención al usuario.

3.2 Organigrama de la empresa

La Figura 6 describe el organigrama que se encuentra vigente en la EPAA-AA.

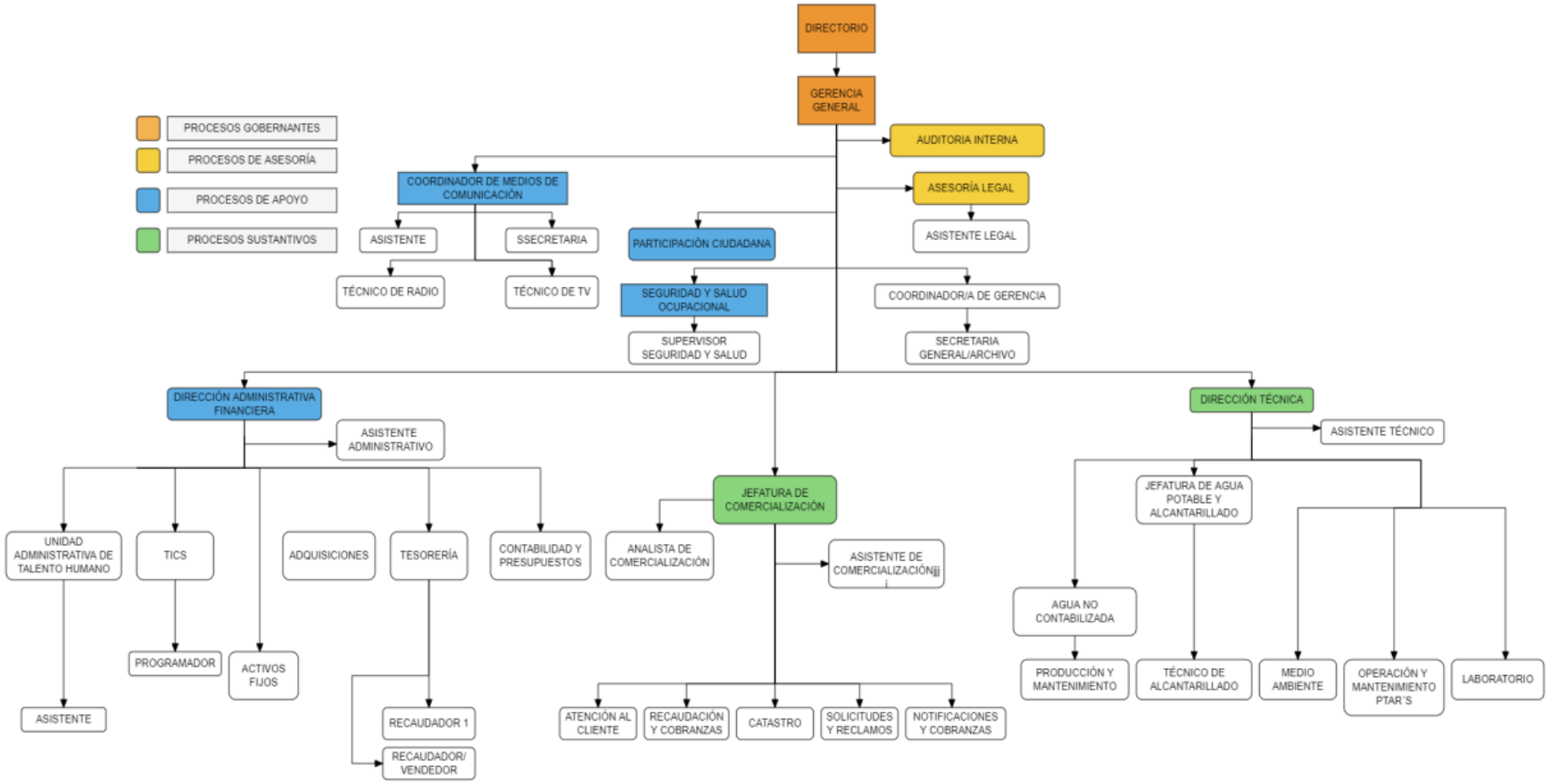

Figura 6: Organigrama de la EPAA-AA. Tomado de [31].

La EPAA-AA presenta una estructura jerárquica alineada a principios de gestión técnica y administrativa que permite una operación eficiente de los servicios de agua potable y alcantarillado en la ciudad [31]:

- En la cúspide del organigrama se encuentra la gerencia general, encargada de la dirección estratégica de la empresa así como de la toma de decisiones importantes
- La dirección administrativa financiera es responsable de la gestión de los recursos de la institución (financieros y humanos)
- La existencia de dependencias técnicas como las áreas operativas de agua potable y alcantarillado, encargadas de la planificación, ejecución, con mantenimiento de la infraestructura

3.3 Enunciados de planificación

A continuación se describen los enunciados de planificación que guía a la institución [32] para brindar los servicios de agua potable:

- Misión: proveer servicios de agua potable y alcantarillado de manera eficiente, oportuna y con responsabilidad social y ambiental, garantizando el acceso a servicios básicos de calidad para la población del cantón Antonio Ante. La misión refleja el compromiso de la empresa con la salud pública, la sostenibilidad del recurso hídrico y el desarrollo territorial
- Visión: consolidarse como una empresa pública técnica, moderna y sostenible, reconocida por su eficiencia en la gestión de servicios básicos, su compromiso con la mejora continua y su capacidad para responder a las necesidades presentes y futuras
- Objetivos institucionales
    - Garantizar la prestación continua y de calidad de los servicios de agua potable y alcantarillado sanitario, promoviendo la eficiencia en la distribución, el uso racional del recurso hídrico y el cumplimiento de normas técnicas y ambientales
    - Fortalecer la gestión institucional mediante procesos administrativos, financieros y técnicos eficaces, que aseguren la transparencia, el buen uso de los recursos y la mejora continua del servicio

- Ampliar la cobertura de los servicios básicos en zonas urbanas y rurales del cantón Antonio Ante, mediante obras de infraestructura que respondan al crecimiento poblacional y a las necesidades sociales
- Impulsar la sostenibilidad ambiental, mediante el tratamiento adecuado de aguas residuales, la protección de fuentes de agua y la implementación de buenas prácticas de gestión ambiental
- Promover la participación ciudadana y la educación sanitaria y ambiental, fortaleciendo la corresponsabilidad entre la empresa y los usuarios en el cuidado del agua y la infraestructura

3.4 Definición de partes interesadas

Las partes interesadas internas son aquellas personas, unidades o áreas que forman parte de la estructura organizacional de una entidad y que, debido a sus funciones, responsabilidades o acceso a la información, tienen un impacto directo en el funcionamiento y cumplimiento de los objetivos del SGSI; a continuación, en la TABLA 4 se describen las partes internas interesadas que se han identificado.

TABLA 4
Partes internas interesadas

Elemento	Descripción
Gerencia general	Su compromiso es fundamental para asignar recursos, definir prioridades institucionales y garantizar el cumplimiento de los objetivos del SGSI, alineándolo con la misión organizacional
Dirección técnica	Es una parte interesada clave, ya que maneja información operativa crítica, infraestructura conectada a sistemas digitales y procesos que deben ser protegidos para garantizar la continuidad del servicio
Jefatura de comercialización	Maneja información sensible de los usuarios, como datos personales, consumos y facturación, lo que hace que su rol en el SGSI sea esencial, ya que debe garantizar la confidencialidad y protección de la información de los clientes, en cumplimiento con normativas legales y de seguridad
Dirección administrativa financiera	La administración de información financiera crítica tiene un rol decisivo en la inversión en tecnologías y medidas necesarias para el funcionamiento del SGSI

Elemento	Descripción
Asesoría legal	Su participación como parte interesada es crucial para garantizar que las políticas del SGSI estén alineadas con la legislación vigente sobre protección de datos, contratación pública y responsabilidad institucional

Nota: La tabla describe las partes interesadas en el desarrollo del proyecto. Adaptado de [32].

3.5 Definición de procesos core del negocio

Los procesos core del negocio son aquellas actividades esenciales y estratégicas que constituyen la razón de ser de una organización, ya que generan directamente valor para sus clientes o usuarios y están estrechamente alineadas con su misión, visión y objetivos institucionales, para la identificación de estos procesos en la EPAA-AA se realizaron las siguientes actividades:

- Revisión de la misión, visión y objetivos institucionales
- Análisis de la cadena de valor de la organización
- Revisión de la estructura orgánica y los manuales de procesos
- Entrevistas con responsables de área y personal clave
- Identificación de los servicios principales ofrecidos a la ciudadanía

A continuación, en la TABLA 5 se detallan los procesos identificados en este ejercicio que fue realizado con el personal de la EPAA-AA.

TABLA 5
Procesos core identificados

Elemento	Descripción
Captación, tratamiento y distribución de agua potable	Este es el proceso esencial que responde directamente a la misión de garantizar el acceso al agua segura para la población e incluye las actividades de captación desde fuentes naturales, potabilización, control de calidad y distribución a través de la red hidráulica
Recolección, conducción y tratamiento de aguas residuales	Vinculado con la sostenibilidad ambiental y la salud pública, este proceso incluye el mantenimiento del sistema de alcantarillado sanitario y el tratamiento de aguas servidas, conforme a normativas técnicas y ambientales
Gestión comercial y atención al cliente	Este proceso es clave para garantizar la sostenibilidad financiera y la satisfacción del usuario, alineado con los objetivos de eficiencia y transparencia que se lo realiza mediante actividades como la

Elemento	Descripción
	lectura de medidores, facturación, recaudación, gestión de convenios y atención de reclamos
Gestión de mantenimiento de redes e infraestructura	Comprende la planificación y ejecución de tareas preventivas y correctivas en las redes de agua y alcantarillado, asegurando la continuidad del servicio y la reducción de pérdidas técnicas, lo cual está directamente vinculado con la visión de eficiencia y modernización
Ampliación y mejora de cobertura de servicios	Relacionada con los objetivos de equidad y desarrollo territorial, esta línea de acción incluye proyectos de expansión de redes y construcción de nueva infraestructura en sectores urbanos y rurales no atendidos, fortaleciendo el cumplimiento del derecho al agua

Nota: La tabla define los procesos core del negocio. Adaptado de [32].

3.6 Evaluación de la situación actual

La fase de evaluación de la situación actual en base al Anexo A de la norma ISO/IEC 27001 permite diagnosticar el estado real de la organización frente a los controles establecidos para identificar brechas y posteriormente definir acciones correctivas y proponer un Sistema de Gestión de Seguridad de la Información (SGSI) adecuado a la realidad de la EPAA-AA. A continuación, en la TABLA 6 se describe la secuencia de actividades a ejecutar:

TABLA 6
Proceso para la evaluación de la situación actual

Actividad	Descripción
Conformar el equipo de evaluación	Organizar con el apoyo de las autoridades un equipo multidisciplinario compuesto por representantes de todas las áreas directamente relacionadas con la seguridad de la información
Diseñar el instrumento para la recolección de información	Se elaboró el cuestionario de preguntas cerradas que permitan contar con información de la situación actual de la empresa
Recopilación de la información	Esta actividad permite verificar la existencia, aplicación, seguimiento y documentación de los controles relacionados con la seguridad de la información
Clasificación de los controles	Para cada control se evaluó su nivel de cumplimiento acorde a los siguientes estados: • No implementado • Implementado sin evidencia formal

Actividad	Descripción
	• Implementado y documentado • Implementado, documentado y revisado periódicamente
Análisis de resultados	Se describe el nivel de cumplimiento de cada control y las brechas detectadas

Nota: La tabla describe el proceso a ejecutar para la evaluación de la situación actual

Para llevar a cabo la evaluación de la situación actual se conformó un equipo multidisciplinario integrado por personal de distintas áreas de la organización, incluyendo tecnología, procesos, gestión documental y administración, con quienes se revisó y analizó cada uno de los 93 controles del Anexo A de la norma para finalmente diseñar una encuesta con preguntas cerradas que permitió recopilar información precisa sobre el grado de implementación de cada uno de los controles, facilitando así un diagnóstico participativo, técnico y alineado a la realidad operativa de la institución.

Cada pregunta fue respondida con base en evidencias objetivas y verificables, tales como políticas documentadas, procedimientos operativos, registros institucionales, informes de auditorías anteriores, configuraciones de sistemas y observaciones directas realizadas por el equipo de trabajo que permitieron garantizar la consistencia y claridad en la evaluación; para lo cual, cada pregunta contó con cuatro opciones de respuesta, definidas según los niveles de cumplimiento establecidos y descritos en la Figura 7.

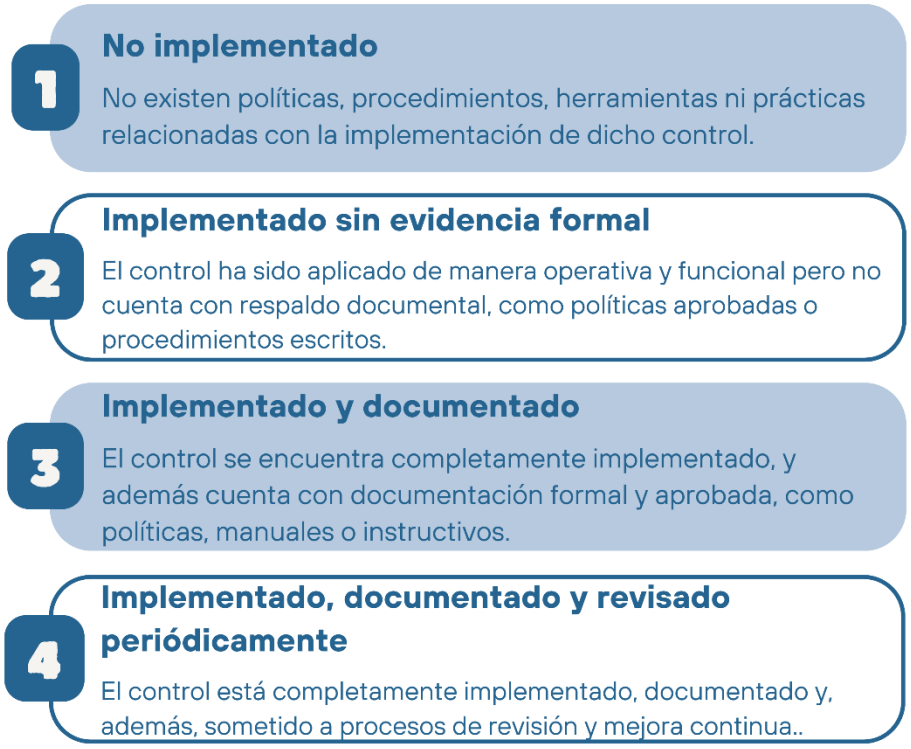

Figura 7: Descripción de las opciones de respuesta.

En los resultados descritos en la Figura 8 se observa que 67 de los 93 controles (72%) no han sido implementados, lo cual representa una brecha crítica de cumplimiento evidenciando que la mayoría de los controles propuestos por la norma aún no han sido abordados por la organización.

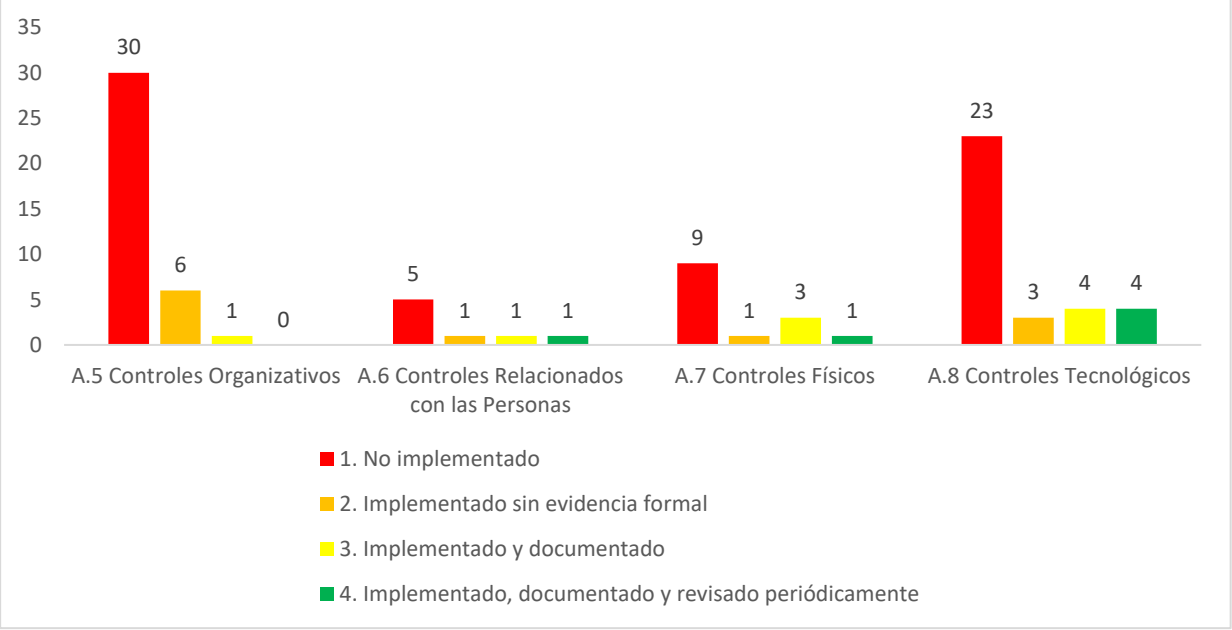

Figura 8: Resultados de la evaluación de la situación actual.

- La evaluación evidencia que 30 de los 37 controles evaluados (81%) se encuentran sin implementación, lo cual refleja una ausencia de políticas formales, definición de roles, estructura de gobierno de seguridad, así como procedimientos organizacionales claros.
- Los controles relacionados con las personas así como los controles físicos presentan un escenario relativamente más favorable, dado que varios de ellos muestran algún nivel de implementación. En el caso de los controles físicos, 5 presentan avances y 1 alcanza el nivel máximo de madurez; sin embargo, debido al número reducido de controles en este dominio, su influencia en el diagnóstico general es limitada.
- En los controles tecnológicos, aunque existe una ligera mejora con 8 controles implementados en diferentes niveles (4 documentados y 4 revisados periódicamente), aún persiste un 68% de controles no implementados (23 de 34), lo que pone en evidencia deficiencias en la infraestructura técnica de protección, como mecanismos de control de acceso, cifrado, monitoreo o gestión de vulnerabilidades.

Los resultados de la figura 8 refuerzan la urgencia de diseñar e implementar un SGSI estructurado, priorizando primero los controles organizacionales y tecnológicos, para de esta manera avanzar hacia un modelo de seguridad integral que sea conforme a la norma ISO/IEC 27001.

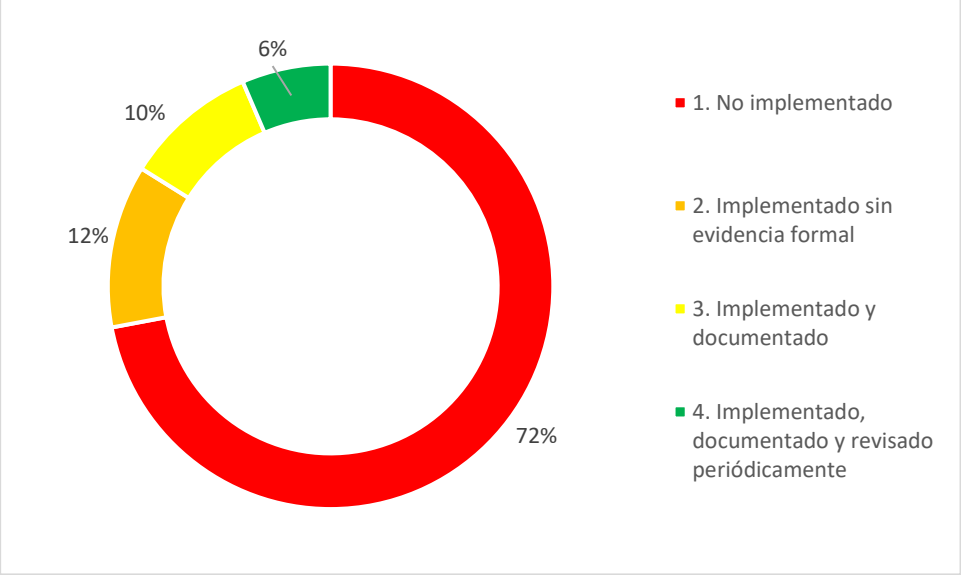

Figura 9: Estados de la evaluación de la situación actual.

3.7 Identificación de brechas

La identificación de brechas en la evaluación de la situación actual se fundamenta en los controles del Anexo A de la norma ISO/IEC 27001 que, según el diagnóstico, no han sido implementados dentro de la organización, representando vacíos en la gestión de la seguridad de la información, ya que no existen mecanismos, procedimientos ni acciones documentadas o aplicadas que den cumplimiento a los requisitos establecidos por la norma.

Los resultados obtenidos en la identificación de brechas reflejan una situación crítica en cuanto al cumplimiento de los controles establecidos ya que se evidencia que el 72,04% (67 controles) del total de controles no han sido implementados en la organización (ver Figura 10). Este alto porcentaje representa una importante brecha de seguridad que pone en riesgo la confidencialidad, integridad y disponibilidad de la información.

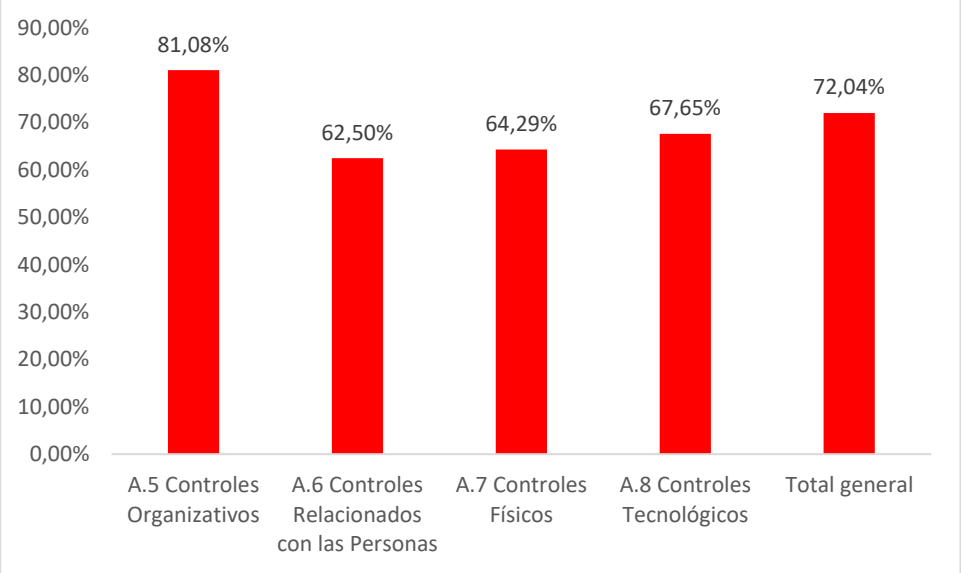

Figura 10: Resultados de la identificación de brechas.

- El dominio con mayores deficiencias corresponde a los controles organizativos (A.5), con un 81,08% de brechas, este resultado indica la ausencia de políticas, procedimientos, así como también estructuras de gobernanza necesarias para establecer una base sólida en la gestión de la seguridad

- En segundo lugar le siguen los controles tecnológicos (A.8) con un 67,65% de brechas, lo que evidencia una debilidad considerable en los mecanismos técnicos de protección, monitoreo o gestión de incidentes
- Los controles físicos (A.7) junto con los controles relacionados con las personas (A.6) presentan también brechas significativas, con 64,29% y 62,50% respectivamente, esto sugiere la necesidad de reforzar las medidas de control de acceso físico, así como las actividades de formación, concienciación, en conjunto con la gestión del recurso humano

3.8 Priorización de brechas

La priorización de brechas es un paso fundamental dentro del proceso de diseño de un SGSI, ya que permite enfocar los esfuerzos y recursos de la organización en aquellas debilidades que representan mayor riesgo para la confidencialidad, integridad y disponibilidad de la información; para lo cual, se debe partir de la premisa que no todas las brechas tienen el mismo impacto por lo que establecer un orden de atención basado en la criticidad de los activos afectados, el nivel de impacto y la urgencia de su implementación, permite una gestión más eficiente y estratégica del SGSI.

Para llevar a cabo esta priorización, se ejecutó la siguiente secuencia de actividades:

- **Consolidación de resultados del diagnóstico:** revisión de los controles evaluados del Anexo A y detección de aquellos que no han sido implementados
- **Identificación de brechas por dominio:** clasificación de las brechas encontradas en los dominios organizativos, humanos, físicos y tecnológicos
- **Vinculación de brechas con activos críticos:** relación directa entre las brechas y los activos de información identificados como prioritarios en el inventario
- **Análisis de riesgos utilizando la metodología MAGERIT v3:** evaluación del impacto y la probabilidad de ocurrencia de amenazas sobre los activos afectados por las brechas
- **Aplicación de una matriz de priorización de riesgos:** asignación de niveles de criticidad (alta, media, baja) a cada brecha, en función del riesgo que representa
- **Elaboración del listado de brechas priorizadas:** generación de un documento que organiza las brechas de mayor a menor prioridad para su atención en el plan de tratamiento

- **Validación del listado con el equipo multidisciplinario:** revisión participativa de los resultados para asegurar la coherencia con el contexto operativo y los recursos disponibles

Para el cálculo de la criticidad de cada brecha se aplicó la siguiente fórmula:

$$Criticidad = Impacto \times Urgencia$$

Para lo cual, el impacto mide el grado de afectación que tendría una brecha sobre la seguridad de la información de acuerdo con las siguientes consideraciones.

- **1 (Bajo):** la brecha tiene un impacto limitado o poco significativo en la seguridad de la información
- **2 (Medio):** la brecha podría ocasionar consecuencias moderadas, como un aumento en los riesgos de seguridad
- **3 (Alto):** la brecha representa un impacto crítico, podría causar interrupciones graves en las operaciones.

La urgencia mide la necesidad inmediata de abordar una brecha considerando el riesgo junto con la probabilidad de que cause un incidente en el corto plazo.

- **1 (Baja):** la brecha no representa una amenaza inmediata y puede ser atendida a largo plazo
- **2 (Media):** la brecha podría agravarse o derivar en incidentes de seguridad, por lo que requiere atención en el mediano plazo
- **3 (Alta):** la brecha necesita atención inmediata pudiendo generar incidentes graves en el corto plazo

Para comprender los resultados de la criticidad se debe realizar la lectura de acuerdo con las siguientes consideraciones.

- **Criticidad baja (1-3):** brechas que pueden ser gestionadas a largo plazo
- **Criticidad media (4-6):** brechas que requieren atención prioritaria en el mediano plazo
- **Criticidad alta (7-9):** brechas que deben ser abordadas de manera inmediata

El análisis de los resultados obtenidos demuestra que, de los 67 controles no implementados, se determinó que 11 (16,42%) tienen un nivel de criticidad alta, 30 (44,78%) son de criticidad media y 26 (38,80%) de criticidad baja, lo que evidencia que casi la mitad de las brechas requieren intervención en el corto y mediano plazo para mitigar riesgos significativos (ver Figura 11).

- Los controles organizativos (A.5) concentran la mayor cantidad de brechas con un total de 30, de las cuales 4 son de alta prioridad, indicando deficiencias importantes en la estructura de gobernanza, políticas y procesos estratégicos de seguridad de la información
- Los controles tecnológicos (A.8) también presentan una carga significativa con 23 brechas, incluyendo 3 de alta prioridad evidenciando vulnerabilidades en la infraestructura técnica, como el control de accesos, cifrado, o monitoreo de incidentes
- Los controles físicos (A.7) junto con los controles relacionados con las personas (A.6) presentan un menor volumen de brechas con 9 y 5 respectivamente, y solo una de alta prioridad en el caso del componente humano

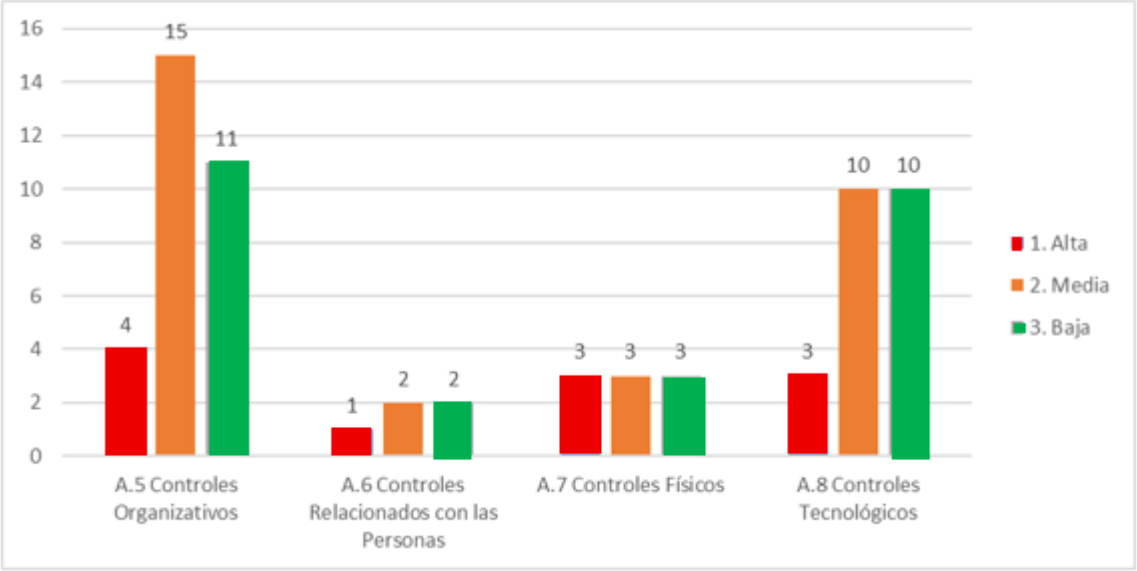

Figura 11: Resultados de la priorización de brechas.

CAPÍTULO IV

DESARROLLO DE LA PROPUESTA DE SGSI

4.1 Objetivos

- Proteger la confidencialidad, integridad y disponibilidad de la información crítica
- Asegurar la continuidad operativa de los servicios de agua potable y alcantarillado
- Reducir y gestionar de manera efectiva los riesgos asociados a la seguridad de la información
- Fomentar una cultura organizacional orientada a la seguridad de la información
- Establecer un marco de mejora continua en la gestión de la seguridad

4.2 Alcance

El SGSI abarca la protección de la información generada, procesada, almacenada y transmitida en los procesos estratégicos, operativos y de apoyo, que garantizan la continuidad y calidad del servicio de agua potable y alcantarillado en el cantón Antonio Ante.

El alcance incluye:

- Las instalaciones físicas de la empresa tales como oficinas administrativas, centro de control, estaciones de bombeo o la sala de servidores
- Los sistemas de información críticos: plataforma SCADA, sistema contable, sistema de facturación, y gestión documental
- Los activos tecnológicos y de comunicación, como estaciones de trabajo, servidores, routers, firewalls, redes internas y sistemas de respaldo
- Los servicios tercerizados relacionados con infraestructura tecnológica, soporte técnico, conectividad y hosting
- El personal interno y externo que interactúa con la información institucional, incluyendo áreas como gerencia general, dirección técnica, dirección administrativa-financiera, jefatura de comercialización y asesoría legal

Exclusiones: Quedan fuera del alcance las áreas o servicios que no procesan, almacenan ni gestionan información crítica de la empresa o que no son relevantes para los objetivos del SGSI.

4.3 Flujo de la información

A continuación, en la Figura 12 se muestra el flujo de información que permitirá la construcción de la propuesta de SGSI acotado a la realidad de la EPAA-AA.

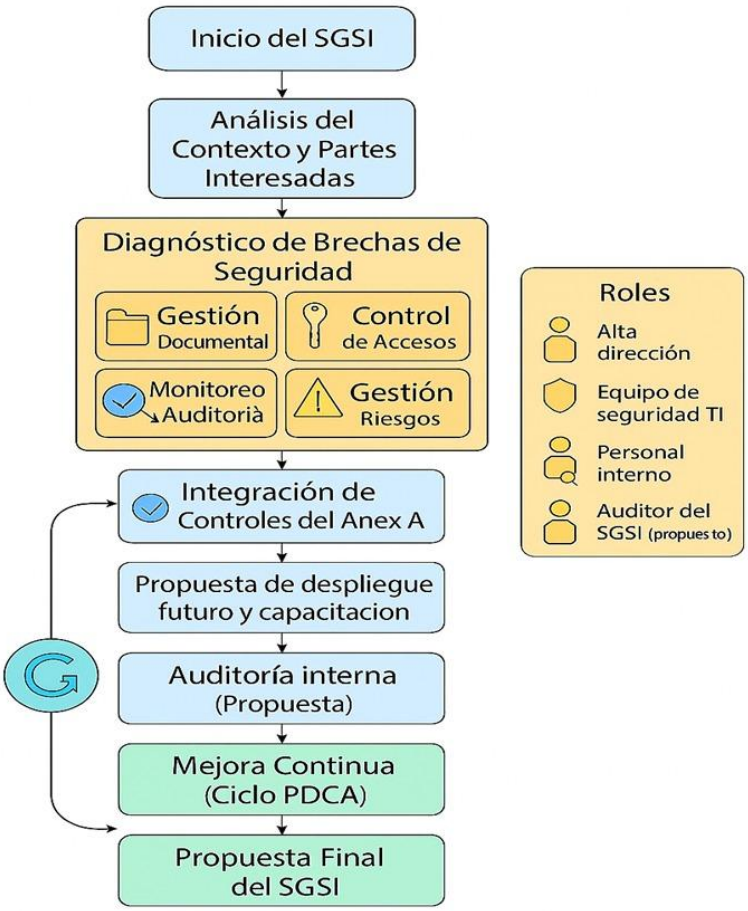

Figura 12: Flujo de la información.

4.4 Identificación y valoración de activos

4.4.1 Identificación de los activos

Esta actividad es un paso fundamental en la implementación del SGSI, ya que permite conocer con claridad qué elementos deben ser protegidos dentro de una organización con el objetivo de identificar los recursos que generan, almacenan, procesan o transmiten información crítica, para

posteriormente evaluar su valor, vulnerabilidades y riesgos asociados; para lo cual, la información se agrupa de acuerdo con las siguientes categorías:

- **Información en papel:** documentos físicos que contienen datos sensibles o críticos
- **Sistemas de información:** plataformas tecnológicas que procesan o almacenan información
- **Bases de datos:** conjuntos de información estructurada que respaldan el funcionamiento de los sistemas de información, donde se almacenan los datos generados por los procesos institucionales
- **Equipos de cómputo:** hardware utilizado por el personal (PCs, laptops, servidores)
- **Redes y comunicaciones:** infraestructura que soporta la conectividad interna y externa
- **Aplicaciones y software:** herramientas informáticas utilizadas para operaciones específicas
- **Usuarios y roles:** personal autorizado que interactúa con los sistemas de información, incluyendo los perfiles, privilegios y niveles de acceso asignados de acuerdo con las funciones que desempeñan dentro de la organización
- **Servicios externos:** proveedores o sistemas de terceros que prestan servicios clave
- **Instalaciones físicas:** oficinas, centros de datos o infraestructuras que albergan otros activos

TABLA 7
Identificación de activos

ID	Categoría	Nombre del activo
A-001	Aplicaciones y software	Antivirus corporativo
A-002	Aplicaciones y software	Correo electrónico
A-003	Aplicaciones y software	Chat institucional
A-004	Equipos de cómputo	Estación de trabajo
A-005	Equipos de cómputo	Router de red
A-006	Equipos de cómputo	Servidores
A-007	Equipos de cómputo	Computadores portátiles
A-008	Información en papel	Manual operativo
A-009	Información en papel	Acta de reunión
A-010	Información en papel	Informe técnico

ID	Categoría	Nombre del activo
A-011	Información en papel	Factura de cliente
A-012	Información en papel	Contrato de servicio
A-013	Instalaciones físicas	Centro de atención al usuario
A-014	Instalaciones físicas	Oficina
A-015	Instalaciones físicas	Centro de control
A-016	Instalaciones físicas	Estación de bombeo
A-017	Instalaciones físicas	Sala de servidores
A-018	Redes y comunicaciones	Punto de acceso Wi-Fi
A-019	Redes y comunicaciones	Switch
A-020	Redes y comunicaciones	VPN de acceso remoto
A-021	Redes y comunicaciones	Firewall
A-022	Servicios externos	Consultoría en TI
A-023	Servicios externos	Proveedor de internet
A-024	Servicios externos	Servicio de hosting
A-025	Servicios externos	Mantenimiento de redes
A-026	Servicios externos	Soporte técnico externo
A-027	Sistemas de información	Aplicación de reclamos en línea
A-028	Sistemas de información	Sistema de gestión documental
A-029	Sistemas de información	Sistema contable
A-030	Sistemas de información	Sistema de facturación
A-031	Sistemas de información	Plataforma SCADA
A-032	Base de datos	Base de datos del sistema contable
A-033	Base de datos	Base de datos del sistema de facturación
A-034	Base de datos	Base de datos de la plataforma SCADA
A-035	Usuarios y roles	Usuarios administrativos
A-036	Usuarios y roles	Usuarios operativos
A-037	Usuarios y roles	Roles y perfiles de acceso

La identificación de los activos presentada en la TABLA 7 se realizó mediante un enfoque de clasificación por categorías, con el fin de agrupar aquellos elementos que cumplen funciones

similares dentro de la organización. Este enfoque permite analizar los activos desde una perspectiva general, orientada a la identificación de riesgos, sin profundizar en detalles técnicos propios de un inventario operativo.

La identificación de los activos por categorías responde al objetivo del estudio, el cual se centra en el análisis de riesgos así como en el diseño de una propuesta de sistema de gestión de la seguridad de la información. La clasificación utilizada facilita la identificación de amenazas, vulnerabilidades, junto con necesidades de control comunes a grupos de activos, tales como estaciones de trabajo, sistemas de información o bases de datos, los cuales presentan niveles de exposición similares.

La gestión detallada de los activos, incluyendo información técnica específica o asignaciones individuales, podrá ser abordada en una etapa posterior durante la implementación del sistema, en donde se puede garantizar una adecuada relación entre la planificación estratégica con la gestión operativa de la seguridad de la información.

4.4.2 Valoración de los activos

El activo se refiere a la importancia que tiene un activo para la organización en función de su utilidad, confidencialidad, impacto en los procesos, y valor estratégico, para su valoración se clasificaron en tres niveles.

- Alto: activos críticos cuya pérdida, alteración o divulgación no autorizada podría generar interrupciones graves, daños económicos significativos o afectación a la reputación institucional
- Medio: activos importantes para la operación, cuya afectación puede ocasionar problemas moderados o interrupciones manejables
- Bajo: activos de bajo impacto, que no comprometen de manera significativa la operatividad o seguridad de la organización

La vulnerabilidad se define como la debilidad o deficiencia en el diseño, implementación o mantenimiento del activo, que puede ser explotada por amenazas para causar daño o pérdida, la cual se evalúa en los siguientes niveles.

- Alta: existen múltiples debilidades conocidas, sin controles implementados o con controles ineficaces
- Media: algunas debilidades están presentes, pero con controles parciales que mitigan el riesgo de forma limitada
- Baja: el activo cuenta con controles adecuados y actualizados que reducen significativamente la probabilidad de explotación

El riesgo se determina combinando el valor del activo y su nivel de vulnerabilidad frente a amenazas potenciales, constituyendo una estimación inicial de la criticidad del activo, que servirá como insumo para el análisis de riesgos detallado desarrollado en las secciones posteriores.

- Crítico: riesgo muy alto; requiere atención inmediata y acciones correctivas urgentes
- Importante: riesgo alto; necesita medidas de mitigación en el corto plazo
- Moderado: riesgo medio; es necesario monitorear y aplicar controles estándar
- Bajo: riesgo bajo; puede aceptarse sin requerir acciones inmediatas, aunque se recomienda revisión periódica

TABLA 8
Valoración de activos

ID	Categoría	Nombre del activo	Valor del activo	Vulnerabilidad	Nivel de riesgo asociado
A-001	Aplicaciones y software	Antivirus corporativo	Alto	Media	Importante
A-002	Aplicaciones y software	Correo electrónico	Medio	Media	Moderado
A-003	Aplicaciones y software	Chat institucional	Medio	Media	Moderado
A-004	Equipos de cómputo	Estación de trabajo	Medio	Alta	Importante
A-005	Equipos de cómputo	Router de red	Alto	Media	Importante
A-006	Equipos de cómputo	Servidores	Alto	Alta	Critico
A-007	Equipos de cómputo	Computadores portátiles	Medio	Alta	Importante
A-008	Información en papel	Manual operativo	Medio	Media	Moderado
A-009	Información en papel	Acta de reunión	Bajo	Media	Bajo
A-010	Información en papel	Informe técnico	Medio	Media	Moderado
A-011	Información en papel	Factura de cliente	Alto	Media	Importante
A-012	Información en papel	Contrato de servicio	Alto	Media	Importante
A-013	Instalaciones físicas	Centro de atención al usuario	Medio	Media	Moderado
A-014	Instalaciones físicas	Oficina	Medio	Media	Moderado
A-015	Instalaciones físicas	Centro de control	Alto	Media	Crítico
A-016	Instalaciones físicas	Estación de bombeo	Alto	Media	Crítico
A-017	Instalaciones físicas	Sala de servidores	Alto	Media	Importante
A-018	Redes y comunicaciones	Punto de acceso Wi-Fi	Medio	Alta	Moderado
A-019	Redes y comunicaciones	Switch	Alto	Media	Importante

ID	Categoría	Nombre del activo	Valor del activo	Vulnerabilidad	Nivel de riesgo asociado
A-020	Redes y comunicaciones	VPN de acceso remoto	Alto	Alta	Crítico
A-021	Redes y comunicaciones	Firewall	Alto	Media	Importante
A-022	Servicios externos	Consultoría en TI	Medio	Media	Moderado
A-023	Servicios externos	Proveedor de internet	Alto	Media	Importante
A-024	Servicios externos	Servicio de hosting	Alto	Media	Importante
A-025	Servicios externos	Mantenimiento de redes	Medio	Media	Moderado
A-026	Servicios externos	Soporte técnico externo	Medio	Media	Moderado
A-027	Sistemas de información	Aplicación de reclamos en línea	Medio	Media	Moderado
A-028	Sistemas de información	Sistema de gestión documental	Alto	Media	Importante
A-029	Sistemas de información	Sistema contable	Alto	Media	Crítico
A-030	Sistemas de información	Sistema de facturación	Alto	Media	Crítico
A-031	Sistemas de información	Plataforma SCADA	Alto	Alta	Crítico
A-032	Base de datos	Base de datos del sistema contable	Alto	Media	Crítico
A-033	Base de datos	Base de datos del sistema de facturación	Alto	Media	Crítico
A-034	Base de datos	Base de datos de la plataforma SCADA	Alto	Alta	Crítico
A-035	Usuarios y roles	Usuarios administrativos	Alto	Alta	Crítico
A-036	Usuarios y roles	Usuarios operativos	Medio	Alta	Importante
A-037	Usuarios y roles	Roles y perfiles de acceso	Alto	Media	Importante

4.4.3 Criterios metodológicos para la determinación del nivel de riesgo asociado

La asignación de niveles de riesgo en la TABLA 8 se basa en una evaluación cualitativa que complementa los criterios numéricos de valor y vulnerabilidad, esta aproximación incorpora consideraciones estratégicas y operativas específicas del contexto de la EPAA-AA, para esto se identificaron y aplicaron los siguientes principios rectores durante la valoración.

1. **Principio de protección esencial:** los activos cuya función principal es la seguridad (por ejemplo, software antivirus, cortafuegos o mecanismos de autenticación) fueron clasificados con un nivel de riesgo elevado, este criterio reconoce que la falla de un control de seguridad, independientemente de su estado actual, compromete la integridad de múltiples sistemas dependientes.
2. **Principio de exposición probabilística:** se asignó una mayor ponderación de riesgo a aquellos activos que, por su naturaleza, constituyen vectores de ataque comunes o puntos de entrada frecuentes para amenazas, esto incluye sistemas de comunicación como el correo electrónico y las herramientas de acceso remoto, cuya probabilidad de ser explotados es inherentemente más alta.
3. **Principio de criticidad operativa:** los activos que sostienen directamente la prestación del servicio de agua potable y alcantarillado (como los sistemas SCADA, de facturación o el centro de control) recibieron una clasificación acorde con su impacto crítico. Una interrupción en estos sistemas tendría consecuencias inmediatas y graves para la operación de la empresa y la comunidad

Con esta metodología de valoración cualitativa, guiada por el conocimiento del contexto institucional y del sector, se garantiza una apreciación integral del riesgo por parte de los resultados. La clasificación preliminar aquí presentada sirvió como insumo base para el posterior análisis cuantitativo detallado, realizado mediante la metodología MAGERIT, la cual validó, así como refinó estos niveles iniciales.

4.5 Identificación de amenazas y vulnerabilidades

Esta fase es crítica en la construcción de un SGSI, ya que permite conocer los posibles escenarios de riesgo que podrían comprometer la confidencialidad, integridad y disponibilidad de los activos

de información (ver TABLA 9). Para su desarrollo, se partió de la categorización de activos previamente definida, analizando el contexto operativo y técnico en el que se desempeña cada uno, así como los procesos, usuarios y entornos que intervienen en su utilización.

En este contexto, las amenazas y vulnerabilidades asociadas a los activos de bases de datos y a los usuarios y roles de acceso fueron consideradas de manera integrada dentro de la categoría de sistemas de información, dado que su exposición al riesgo se manifiesta a través de los sistemas que los administran y de los mecanismos de control de acceso implementados. Esta decisión metodológica permite evitar duplicidades en el análisis y garantizar la coherencia del diagnóstico, para lo cual se realizaron las siguientes actividades.

- Categorización de activos: se utilizó la misma categorización empleada en la identificación de activos
- Análisis del entorno operativo y técnico: implicó examinar el contexto en el que se encuentra cada activo, incluyendo su función dentro de los procesos institucionales, el tipo de información que maneja, los usuarios que lo operan y el entorno físico o digital donde se ubica
- Identificación de amenazas: en esta fase se determinó los eventos o situaciones potenciales (naturales, humanas o tecnológicas) que podrían afectar negativamente a los activos
- Detección de vulnerabilidades: consistió en descubrir debilidades técnicas, procedimentales u organizativas que puedan ser explotadas por amenazas
- Validación del análisis: para garantizar la precisión del diagnóstico, se lleva a cabo una validación con apoyo de equipos multidisciplinarios de la empresa

TABLA 9
Identificación de amenazas y vulnerabilidades

ID	Categoría	Amenaza	Vulnerabilidad
CT-01	Aplicaciones y software	Malware o software malicioso	Falta de actualizaciones de seguridad
		Accesos no autorizados	Gestión deficiente de contraseñas
		Errores en el código	Falta de pruebas y validaciones

ID	Categoría	Amenaza	Vulnerabilidad
CT-02	Equipos de cómputo	Robo o pérdida de dispositivos	Ausencia de sistemas de bloqueo físico
		Fallas de hardware	Mantenimiento inadecuado
		Acceso no autorizado	Falta de autenticación segura
CT-03	Información en papel	Pérdida de documentos	Almacenamiento inseguro
		Acceso no autorizado	Ausencia de controles físicos
		Divulgación accidental	Falta de políticas de confidencialidad
CT-04	Instalaciones físicas	Intrusión física	Sistemas de vigilancia insuficientes
		Daños por desastres naturales	Ausencia de planes de contingencia
		Sabotaje	Falta de control de accesos físicos
CT-05	Redes y comunicaciones	Intercepción de datos	Cifrado inadecuado
		Ataques de denegación de servicio (DDoS)	Falta de protección perimetral
		Acceso no autorizado a la red	Configuraciones inseguras de red
CT-06	Servicios externos	Fallo del proveedor	Dependencia crítica sin respaldo
		Acceso a información sensible	Contratos sin cláusulas de confidencialidad
		Interrupción del servicio	Falta de acuerdos de nivel de servicio (SLA)
CT-07	Sistemas de información	Pérdida de integridad de los datos	Errores en la gestión de la base de datos

ID	Categoría	Amenaza	Vulnerabilidad
		Interrupción del servicio	Falta de redundancia o backup
		Acceso no autorizado	Gestión inadecuada de usuarios y roles

4.5.1 Valoración de las amenazas

Para la ponderación de las amenazas se ha definido una escala del 0 al 5 (ver TABLA 10) considerando que cada activo se encuentra expuesto a diferentes amenazas y vulnerabilidades para su valoración se toma encuesta la probabilidad y la frecuencia de ocurrencia.

TABLA 10
Criterios de valoración de las amenazas

Valor	Escala	Probabilidad	Frecuencia
5	MA	Muy alta	Daño diario
4	A	Alta	Daño mensual
3	M	Media	Más de una vez al año
2	B	Baja	Una vez al año
1	MB	Muy bajo	Rara vez
0	D	Despreciable	Irrelevante a efectos prácticos

Una vez determinada la escala y los factores de valoración se ejecutaron las siguientes actividades para la valoración de las amenazas (ver TABLA 11):

- Asignación de niveles de probabilidad: Se estimó la probabilidad de ocurrencia de cada amenaza, considerando factores como historial de incidentes, exposición del activo y entorno operativo.

- Evaluación de la frecuencia de ocurrencia: Se valoró con qué frecuencia podrían materializarse las amenazas para determinar el nivel de exposición y criticidad de los activos frente a dichas amenazas.
- Valoración numérica de la amenaza: A cada amenaza se le asignó un valor cuantitativo tanto para su probabilidad como su frecuencia, permitiendo realizar comparaciones, clasificaciones y priorizaciones objetivas para futuras acciones de mitigación.

TABLA 11
Identificación de amenazas y vulnerabilidades

ID	Categoría	Amenaza	Vulnerabilidad	Probabilidad	Frecuencia
CT-01	Aplicaciones y software	Malware o software malicioso	Falta de actualizaciones de seguridad	2	5
		Accesos no autorizados	Gestión deficiente de contraseñas	3	4
		Errores en el código	Falta de pruebas y validaciones	2	3
CT-02	Equipos de cómputo	Robo o pérdida de dispositivos	Ausencia de sistemas de bloqueo físico	4	4
		Fallas de hardware	Mantenimiento inadecuado	4	4
		Acceso no autorizado	Falta de autenticación segura	1	5
CT-03	Información en papel	Pérdida de documentos	Almacenamiento inseguro	3	4
		Acceso no autorizado	Ausencia de controles físicos	4	5
		Divulgación accidental	Falta de políticas de confidencialidad	2	3

ID	Categoría	Amenaza	Vulnerabilidad	Probabilidad	Frecuencia
CT-04	Instalaciones físicas	Intrusión física	Sistemas de vigilancia insuficientes	4	5
		Daños por desastres naturales	Ausencia de planes de contingencia	1	2
		Sabotaje	Falta de control de accesos físicos	2	2
CT-05	Redes y comunicaciones	Intercepción de datos	Cifrado inadecuado	4	1
		Ataques de denegación de servicio (DDoS)	Falta de protección perimetral	1	3
		Acceso no autorizado a la red	Configuraciones inseguras de red	3	4
CT-06	Servicios externos	Fallo del proveedor	Dependencia crítica sin respaldo	2	4
		Acceso a información sensible	Contratos sin cláusulas de confidencialidad	5	1

ID	Categoría	Amenaza	Vulnerabilidad	Probabilidad	Frecuencia
		Interrupción del servicio	Falta de acuerdos de nivel de servicio (SLA)	1	4
CT-07	Sistemas de información	Pérdida de integridad de los datos	Errores en la gestión de la base de datos	2	5
		Interrupción del servicio	Falta de redundancia o backup	4	3
		Acceso no autorizado	Gestión inadecuada de usuarios y roles	2	4

4.6 Análisis de riesgos

4.6.1 Impacto

El impacto puede entenderse como el perjuicio que experimenta un activo cuando una amenaza se materializa, para su determinación es necesario considerar cómo se ven comprometidas las dimensiones de confidencialidad, integridad y disponibilidad asociadas a cada activo. La escala utilizada para esta valoración se detalla en la TABLA 12.

TABLA 12
Criterios de valoración del impacto

Valor	Magnitud	Escala	Descripción
5	Muy alta	MA	Cuando se materializa las amenazas se generan grandes impactos en los activos de la organización
4	Alto	A	Cuando se materializa las amenazas se generan altas consecuencias en los activos
3	Medio	M	Cuando se materializa las amenazas se generan consecuencias medias en los activos
2	Bajo	B	Cuando se materializa las amenazas se generan consecuencias bajas en los activos
1	Muy bajo	MB	Cuando se materializa las amenazas se generan consecuencias muy bajas en los activos
0	Despreciable	D	Cuando se materializa las amenazas, pero no tienen afectaciones en la organización

En la TABLA 13 se describe la valoración de cada categoría de activos evidencian la afectación que generaría si se consumara las amenazas a los activos de la empresa. El análisis de impacto se realizó considerando todas las categorías de activos previamente identificadas, en donde se incluyó los sistemas de información dentro de los cuales se evalúan componentes críticos como la gestión de la base de datos o la administración de usuarios y roles. Los elementos fueron analizados en función de su incidencia sobre la confidencialidad, integridad, así como disponibilidad de la información institucional.

TABLA 13
Valoración del impacto de las amenazas en función de la Confidencialidad, Integridad y Disponibilidad (CID)

ID	Categoría	Amenaza	Vulnerabilidad	C	I	D	Total	Impacto	Magnitud
CT-01	Aplicaciones y software	Malware o software malicioso	Falta de actualizaciones de seguridad	4	4	5	13	**5**	**MA**
		Accesos no autorizados	Gestión deficiente de contraseñas	1	2	5	8	**3**	**M**
		Errores en el código	Falta de pruebas y validaciones	2	3	5	10	**4**	**A**
CT-02	Equipos de cómputo	Robo o pérdida de dispositivos	Ausencia de sistemas de bloqueo físico	5	5	5	15	**5**	**MA**
		Fallas de hardware	Mantenimiento inadecuado	3	3	4	10	**4**	**A**
		Acceso no autorizado	Falta de autenticación segura	3	4	4	11	**4**	**A**
CT-03	Información en papel	Pérdida de documentos	Almacenamiento inseguro	3	3	5	11	**4**	**A**
		Acceso no autorizado	Ausencia de controles físicos	5	5	3	13	**5**	**MA**
		Divulgación accidental	Falta de políticas de confidencialidad	2	2	5	9	**3**	**M**

ID	Categoría	Amenaza	Vulnerabilidad	C	I	D	Total	Impacto	Magnitud
CT-04	Instalaciones físicas	Intrusión física	Sistemas de vigilancia insuficientes	4	4	3	11	**4**	**A**
		Daños por desastres naturales	Ausencia de planes de contingencia	2	3	5	10	**4**	**A**
		Sabotaje	Falta de control de accesos físicos	0	2	1	3	**1**	**MB**
CT-05	Redes y comunicaciones	Intercepción de datos	Cifrado inadecuado	5	4	5	14	**5**	**MA**
		Ataques de denegación de servicio (DDoS)	Falta de protección perimetral	1	5	3	9	**3**	**M**
		Acceso no autorizado a la red	Configuraciones inseguras de red	5	5	0	10	**4**	**A**
CT-06	Servicios externos	Fallo del proveedor	Dependencia crítica sin respaldo	4	2	2	8	**3**	**M**
		Acceso a información sensible	Contratos sin cláusulas de confidencialidad	2	3	1	6	**2**	**B**
		Interrupción del servicio	Falta de acuerdos de nivel de servicio (SLA)	4	1	0	5	**2**	**B**

ID	Categoría	Amenaza	Vulnerabilidad	C	I	D	Total	Impacto	Magnitud
CT-07	Sistemas de información	Pérdida de integridad de los datos	Errores en la gestión de la base de datos	3	3	5	11	**4**	**A**
		Interrupción del servicio	Falta de redundancia o backup	1	3	5	9	**3**	**M**
		Acceso no autorizado	Gestión inadecuada de usuarios y roles	2	5	0	7	**3**	**M**

4.6.2 Probabilidad de ocurrencia

En la determinación de la magnitud de la probabilidad de ocurrencia de cada amenaza identificada, se utilizó como referencia la columna “Escala” descrita en la TABLA 10, que corresponde a los criterios de valoración de amenazas, misma que proporciona una clasificación cualitativa y cuantitativa que permite estimar con mayor precisión la frecuencia con la que una amenaza podría materializarse en el entorno organizacional.

Se complementó el análisis con una nueva columna denominada “Magnitud” que refleja el nivel asignado a cada amenaza según la escala mencionada, dando origen a una versión más completa del análisis que se presenta en la TABLA 14, esta actualización facilita la interpretación del riesgo, permitiendo tomar decisiones informadas sobre la priorización junto con el tratamiento de las amenazas dentro del SGSI.

TABLA 14
Valoración de la probabilidad de ocurrencia

ID	Categoría	Amenaza	Vulnerabilidad	Probabilidad	Frecuencia	Total	Valoración	Magnitud
CT-01	Aplicaciones y software	Malware o software malicioso	Falta de actualizaciones de seguridad	2	5	7	**4**	**A**
		Accesos no autorizados	Gestión deficiente de contraseñas	3	4	7	**4**	**A**
		Errores en el código	Falta de pruebas y validaciones	2	3	5	**3**	**M**
CT-02	Equipos de cómputo	Robo o pérdida de dispositivos	Ausencia de sistemas de bloqueo físico	4	4	8	**4**	**A**
		Fallas de hardware	Mantenimiento inadecuado	4	4	8	**4**	**A**
		Acceso no autorizado	Falta de autenticación segura	1	5	6	**3**	**M**
CT-03	Información en papel	Pérdida de documentos	Almacenamiento inseguro	3	4	7	**4**	**A**
		Acceso no autorizado	Ausencia de controles físicos	4	5	9	**5**	**MA**
		Divulgación accidental	Falta de políticas de confidencialidad	2	3	5	**3**	**B**

ID	Categoría	Amenaza	Vulnerabilidad	Probabilidad	Frecuencia	Total	Valoración	Magnitud
CT-04	Instalaciones físicas	Intrusión física	Sistemas de vigilancia insuficientes	4	5	9	**5**	**MA**
		Daños por desastres naturales	Ausencia de planes de contingencia	1	2	3	**2**	**B**
		Sabotaje	Falta de control de accesos físicos	2	2	4	**2**	**B**
CT-05	Redes y comunicaciones	Intercepción de datos	Cifrado inadecuado	4	1	5	**3**	**M**
		Ataques de denegación de servicio (DDoS)	Falta de protección perimetral	1	3	4	**2**	**B**
		Acceso no autorizado a la red	Configuraciones inseguras de red	3	4	7	**4**	**A**
CT-06	Servicios externos	Fallo del proveedor	Dependencia crítica sin respaldo	2	4	6	**3**	**M**
		Acceso a información sensible	Contratos sin cláusulas de confidencialidad	5	1	6	**3**	**M**

ID	Categoría	Amenaza	Vulnerabilidad	Probabilidad	Frecuencia	Total	Valoración	Magnitud
		Interrupción del servicio	Falta de acuerdos de nivel de servicio (SLA)	1	4	5	**3**	**M**
CT-07	Sistemas de información	Pérdida de integridad de los datos	Errores en la gestión de la base de datos	2	5	7	**4**	**A**
		Interrupción del servicio	Falta de redundancia o backup	4	3	7	**4**	**A**
		Acceso no autorizado	Gestión inadecuada de usuarios y roles	2	4	6	**3**	**M**

4.7 Valoración y Gestión de Riesgos

La valoración y gestión de los riesgos se realizó considerando todas las categorías de activos previamente analizadas. En particular, los riesgos relacionados con la gestión de bases de datos y con la administración de usuarios y roles de acceso fueron evaluados de manera integrada dentro de la categoría de sistemas de información, dado que su exposición y criticidad se manifiestan a través de los mecanismos de control, procesamiento y acceso implementados en dichos sistemas.

4.7.1 Riesgo estimado

Para determinar el riesgo estimado se realiza la multiplicación entre el impacto determinado en la TABLA 13 por la probabilidad de ocurrencia definido en la TABLA 14 y tomando como referencia la escala y criterio definidos en la TABLA 15 se determina la magnitud de cada uno de los riesgos.

TABLA 15
Criterios para determinar el riesgo estimado

Escala	Nivel	Criterio	Descripción
20-25	MA	Muy alto	El riesgo que se genera es extremo, su ocurrencia implicaría una pérdida total de la información.
15-19	A	Alto	El riesgo, su ocurrencia implica una pérdida alta de la información.
10-14	M	Moderado	El riesgo es moderado, su ocurrencia implica una manejable de la información.
5-9	B	Bajo	El riesgo es bajo, su ocurrencia implica una pérdida bajo de información.
1-4	MB	Muy bajo	El riesgo es muy bajo, su ocurrencia implica una pérdida casi nula de la información.

TABLA 16
Matriz de estimación del riesgo

ID	Categoría	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Magnitud
CT-01	Aplicaciones y software	Malware o software malicioso	Falta de actualizaciones de seguridad	5	4	**20**	**MA**
		Accesos no autorizados	Gestión deficiente de contraseñas	3	4	**12**	**M**
		Errores en el código	Falta de pruebas y validaciones	4	3	**12**	**M**
CT-02	Equipos de cómputo	Robo o pérdida de dispositivos	Ausencia de sistemas de bloqueo físico	5	4	**20**	**MA**
		Fallas de hardware	Mantenimiento inadecuado	4	4	**16**	**A**
		Acceso no autorizado	Falta de autenticación segura	4	3	**12**	**M**
CT-03	Información en papel	Pérdida de documentos	Almacenamiento inseguro	4	4	**16**	**A**
		Acceso no autorizado	Ausencia de controles físicos	5	5	**25**	**MA**
		Divulgación accidental	Falta de políticas de confidencialidad	3	3	**9**	**B**
CT-04	Instalaciones físicas	Intrusión física	Sistemas de vigilancia insuficientes	4	5	**20**	**A**
		Daños por desastres naturales	Ausencia de planes de contingencia	4	2	**8**	**B**

ID	Categoría	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Magnitud
		Sabotaje	Falta de control de accesos físicos	1	2	**2**	**MB**
CT-05	Redes y comunicaciones	Intercepción de datos	Cifrado inadecuado	5	3	**15**	**A**
		Ataques de denegación de servicio (DDoS)	Falta de protección perimetral	3	2	**6**	**B**
		Acceso no autorizado a la red	Configuraciones inseguras de red	4	4	**16**	**A**
CT-06	Servicios externos	Fallo del proveedor	Dependencia crítica sin respaldo	3	3	**9**	**B**
		Acceso a información sensible	Contratos sin cláusulas de confidencialidad	2	3	**6**	**B**
		Interrupción del servicio	Falta de acuerdos de nivel de servicio (SLA)	2	3	**6**	**B**
CT-07	Sistemas de información	Pérdida de integridad de los datos	Errores en la gestión de la base de datos	4	4	**16**	**A**
		Interrupción del servicio	Falta de redundancia o backup	3	4	**12**	**M**
		Acceso no autorizado	Gestión inadecuada de usuarios y roles	3	3	**9**	**B**

4.7.2 Matriz de calor

La matriz de calor constituye una herramienta visual fundamental para representar de forma clara e intuitiva el nivel de exposición a los diferentes riesgos identificados en el análisis mediante el uso de colores esta matriz permite ubicar cada riesgo dentro de zonas que reflejan su nivel de criticidad, facilitando la priorización en el proceso de toma de decisiones y en la planificación de medidas de mitigación.

Para su elaboración, se definieron previamente los criterios y escalas de valoración, los cuales se detallan en la TABLA 17, donde se establecen los rangos que determinan el nivel del riesgo que fueron aplicados a los resultados cuantitativos obtenidos en la TABLA 16, de esta forma la matriz de calor se convierte en una herramienta estratégica para visualizar de manera consolidada la distribución de los riesgos y enfocar los esfuerzos de seguridad hacia aquellos con mayor relevancia.

TABLA 17
Gama de colores para la matriz de calor

Escala	Nivel	Criterio	Acciones
20-25	MA	Muy alto	Se requiere acciones inmediatas para reducir, compartir o transferir el riesgo
15-19	A	Alto	Se requiere atención urgente y la implementación de medidas que permitan reducir el nivel de riesgo
10-14	M	Moderado	Se requieren implementar medidas que permitan reducir el riesgo a los niveles bajo o muy bajo
5-9	B	Bajo	Se deben implementar medidas preventivas que ayuden a reducir el riesgo
1-4	MB	Muy bajo	Riesgo tolerable que no requiere de la implementación de acciones diferentes a las existentes

TABLA 18
Análisis de riesgo mediante matriz de calor

ID	Categoría	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Magnitud
CT-01	Aplicaciones y software	Malware o software malicioso	Falta de actualizaciones de seguridad	5	4	**20**	**MA**
		Accesos no autorizados	Gestión deficiente de contraseñas	3	4	**12**	**M**
		Errores en el código	Falta de pruebas y validaciones	4	3	**12**	**M**
CT-02	Equipos de cómputo	Robo o pérdida de dispositivos	Ausencia de sistemas de bloqueo físico	5	4	**20**	**MA**
		Fallas de hardware	Mantenimiento inadecuado	4	4	**16**	**A**
		Acceso no autorizado	Falta de autenticación segura	4	3	**12**	**M**
CT-03	Información en papel	Pérdida de documentos	Almacenamiento inseguro	4	4	**16**	**A**
		Acceso no autorizado	Ausencia de controles físicos	5	5	**25**	**MA**
		Divulgación accidental	Falta de políticas de confidencialidad	3	3	**9**	**B**
CT-04	Instalaciones físicas	Intrusión física	Sistemas de vigilancia insuficientes	4	5	**20**	**A**
		Daños por desastres naturales	Ausencia de planes de contingencia	4	2	**8**	**B**

ID	Categoría	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Magnitud
		Sabotaje	Falta de control de accesos físicos	1	2	**2**	**MB**
CT-05	Redes y comunicaciones	Intercepción de datos	Cifrado inadecuado	5	3	**15**	**A**
		Ataques de denegación de servicio (DDoS)	Falta de protección perimetral	3	2	**6**	**B**
		Acceso no autorizado a la red	Configuraciones inseguras de red	4	4	**16**	**A**
CT-06	Servicios externos	Fallo del proveedor	Dependencia crítica sin respaldo	3	3	**9**	**B**
		Acceso a información sensible	Contratos sin cláusulas de confidencialidad	2	3	**6**	**B**
		Interrupción del servicio	Falta de acuerdos de nivel de servicio (SLA)	2	3	**6**	**B**
CT-07	Sistemas de información	Pérdida de integridad de los datos	Errores en la gestión de la base de datos	4	4	**16**	**A**
		Interrupción del servicio	Falta de redundancia o backup	3	4	**12**	**M**
		Acceso no autorizado	Gestión inadecuada de usuarios y roles	3	3	**9**	**B**

4.7.3 Tratamiento del riesgo

Posterior a la evaluación del riesgo es importante considerar los criterios para el tratamiento del riesgo:

- **Aceptar el riesgo:** el nivel es aceptable y puede ser manejado por lo que no es necesario implementar nuevos controles.
- **Reducir el riesgo:** es necesario implementar controles que permitan disminuir el riesgo hasta el nivel de aceptación.
- **Transferir el riesgo:** es utilizado cuando el riesgo puede ser compartido o trasferido de manera completa a una entidad externa que maneje el riesgo.
- **Evitar el riesgo:** cuando los riesgos son muy altos es necesario implementar controles que permitan evitar por completo este tipo de riesgos.

A continuación, en la TABLA 19 se muestra de forma detallada la manera en que se realizará el tratamiento de cada uno de los riesgos identificados durante la etapa de evaluación, el cual ha sido definido con base en los resultados del análisis de riesgos, lo que constituye un insumo clave para la planificación de medidas de seguridad eficaces dentro del SGSI, conforme a los lineamientos de la norma ISO/IEC 27001:2022.

En concordancia con el enfoque adoptado en las fases previas del análisis, los riesgos asociados a la gestión de bases de datos y a la administración de usuarios y roles de acceso fueron tratados de manera integrada dentro de la categoría de sistemas de información. Esta decisión metodológica responde a que dichos riesgos se materializan a través de los sistemas que procesan, almacenan y controlan el acceso a la información institucional, permitiendo definir estrategias de tratamiento coherentes y evitar la duplicación de riesgos dentro del SGSI.

TABLA 19
Tratamiento del riesgo

ID	Categoría	Amenaza	Vulnerabilidad	Riesgo	Magnitud	Tratamiento
CT-01	Aplicaciones y software	Malware o software malicioso	Falta de actualizaciones de seguridad	**20**	**MA**	**Evitar**
		Accesos no autorizados	Gestión deficiente de contraseñas	**12**	**M**	**Reducir**
		Errores en el código	Falta de pruebas y validaciones	**12**	**M**	**Reducir**
CT-02	Equipos de cómputo	Robo o pérdida de dispositivos	Ausencia de sistemas de bloqueo físico	**20**	**MA**	**Evitar**
		Fallas de hardware	Mantenimiento inadecuado	**16**	**A**	**Evitar**
		Acceso no autorizado	Falta de autenticación segura	**12**	**M**	**Reducir**
CT-03	Información en papel	Pérdida de documentos	Almacenamiento inseguro	**16**	**A**	**Evitar**
		Acceso no autorizado	Ausencia de controles físicos	**25**	**MA**	**Evitar**
		Divulgación accidental	Falta de políticas de confidencialidad	**9**	**B**	**Reducir**
CT-04	Instalaciones físicas	Intrusión física	Sistemas de vigilancia insuficientes	**20**	**A**	**Evitar**
		Daños por desastres naturales	Ausencia de planes de contingencia	**8**	**B**	**Aceptar**

ID	Categoría	Amenaza	Vulnerabilidad	Riesgo	Magnitud	Tratamiento
		Sabotaje	Falta de control de accesos físicos	**2**	**MB**	**Aceptar**
CT-05	Redes y comunicaciones	Intercepción de datos	Cifrado inadecuado	**15**	**A**	**Evitar**
		Ataques de denegación de servicio (DDoS)	Falta de protección perimetral	**6**	**B**	**Aceptar**
		Acceso no autorizado a la red	Configuraciones inseguras de red	**16**	**A**	**Reducir**
CT-06	Servicios externos	Fallo del proveedor	Dependencia crítica sin respaldo	**9**	**B**	**Transferir**
		Acceso a información sensible	Contratos sin cláusulas de confidencialidad	**6**	**B**	**Reducir**
		Interrupción del servicio	Falta de acuerdos de nivel de servicio (SLA)	**6**	**B**	**Transferir**
CT-07	Sistemas de información	Pérdida de integridad de los datos	Errores en la gestión de la base de datos	**16**	**A**	**Evitar**
		Interrupción del servicio	Falta de redundancia o backup	**12**	**M**	**Reducir**
		Acceso no autorizado	Gestión inadecuada de usuarios y roles	**9**	**B**	**Reducir**

4.8 Marco normativo

El marco normativo interno del SGSI establece el conjunto de disposiciones formales que respaldan la gestión de los riesgos identificados y el tratamiento propuesto a través de los planes de acción definidos en este capítulo. Su objetivo es proporcionar un sustento normativo claro y coherente que oriente la aplicación de controles de seguridad de la información en la EPAA-AA, alineados con los principios y requisitos de la norma ISO/IEC 27001:2022.

Las políticas de seguridad de la información conforman el eje central del marco normativo porque formalizan los lineamientos generales, los cuales regulan el comportamiento organizacional, técnico y humano frente a los riesgos que afectan a la información institucional. Las políticas de este tipo sirven como instrumento de apoyo directo para la ejecución de los planes de acción propuestos, puesto que aseguran que cada intervención cuente con un respaldo normativo interno que legitime su aplicación.

Se definió un conjunto de políticas marco, cada una de las cuales agrupa dominios de seguridad relacionados mientras da soporte a varios planes de acción, esto considerando la naturaleza de los riesgos identificados y con la finalidad de evitar la dispersión normativa. El enfoque facilita la comprensión, aplicación, así como también la futura gestión del SGSI, al tiempo que mantiene la trazabilidad entre riesgos, controles acciones propuestas.

Políticas de seguridad de la información

Las políticas de seguridad de la información propuestas en esta sección representan una estructura normativa integral que está diseñada para respaldar los 18 planes de acción definidos en la sección *4.9*, cada política aborda un dominio específico de la seguridad de la información y se encuentra alineada tanto con los riesgos identificados como con los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2022.

Las políticas definidas son las siguientes:

- **Política 1:** Gestión de Vulnerabilidades y Seguridad Operacional
- **Política 2:** Control de Accesos y Gestión de Identidades
- **Política 3:** Seguridad Física y del Entorno
- **Política 4:** Continuidad del Servicio y Respaldo de la Información

- **Política 5:** Seguridad en Comunicaciones y Redes
- **Política 6:** Gestión de Proveedores y Servicios Externos
- **Política 7:** Clasificación y Protección de la Información
- **Política 8:** Concienciación, Formación y Cultura de Seguridad de la Información

Cada una de estas políticas ha sido desarrollada para respaldar de forma directa uno o varios planes de acción, evitando redundancias normativas y garantizando coherencia metodológica entre el análisis de riesgos, la planificación de controles y la propuesta del SGSI. Su implementación permitiría a la EPAA-AA contar con un marco normativo claro, aplicable y alineado a buenas prácticas internacionales, fortaleciendo la protección de la información y la continuidad de los servicios institucionales.

4.8.1 Política de Gestión de Vulnerabilidades y Seguridad Operacional

a) Objetivo

Establecer los lineamientos institucionales para la identificación, gestión y mitigación de vulnerabilidades técnicas y operativas en los activos de información de la EPAA-AA, con el fin de reducir la probabilidad de incidentes de seguridad derivados de software desactualizado, errores en el desarrollo de sistemas y fallas de hardware, garantizando la confidencialidad, integridad y disponibilidad de la información.

b) Alcance

Esta política es de aplicación obligatoria para lo siguiente.

- Todos los sistemas de información institucionales
- Infraestructura tecnológica, incluyendo servidores, estaciones de trabajo, equipos de red y dispositivos críticos
- Personal técnico, administrativo y terceros que tengan responsabilidades en la operación, mantenimiento o desarrollo de sistemas
- Proveedores externos que realicen actividades de soporte, mantenimiento o desarrollo tecnológico para la EPAA-AA

c) Principios generales

La gestión de vulnerabilidades y operaciones de seguridad se regirá por los siguientes principios.

- **Prevención:** priorizar acciones que eviten la materialización de vulnerabilidades antes de que se conviertan en incidentes
- **Actualización continua:** mantener los sistemas, aplicaciones y equipos en condiciones seguras y actualizadas
- **Responsabilidad compartida:** cada área es responsable de cumplir los controles de seguridad asociados a los activos bajo su gestión
- **Mejora continua:** los controles deberán evaluarse y ajustarse periódicamente conforme a la evolución tecnológica y de riesgos

d) Lineamientos de la política

Gestión de actualizaciones y parches

- Todos los sistemas operativos, aplicaciones, firmware y componentes de red deberán mantenerse actualizados mediante mecanismos de actualización controlados
- Se prohíbe el uso de software no autorizado o sin soporte oficial
- Se deberá mantener un inventario actualizado de los activos de software y su estado de actualización

Gestión de vulnerabilidades técnicas

- Se deberán implementar herramientas de escaneo junto con monitoreo que permitan identificar vulnerabilidades conocidas
- Las vulnerabilidades críticas deberán ser tratadas dentro de plazos definidos según su nivel de riesgo
- Los resultados de los análisis de vulnerabilidades deberán ser documentados y revisados periódicamente

Desarrollo y mantenimiento seguro de sistemas

- Todo desarrollo o modificación de sistemas deberá cumplir procedimientos formales de pruebas y validación

- Se deberán utilizar entornos separados para desarrollo, pruebas y producción
- El código fuente de los sistemas críticos será objeto de revisiones periódicas orientadas a detectar errores y debilidades de seguridad

e) Mantenimiento y operación de hardware

- Los equipos críticos deberán contar con un plan de mantenimiento preventivo documentado
- Se deberán implementar mecanismos de monitoreo que permitan detectar fallas de hardware de forma temprana
- La sustitución o renovación de equipos deberá planificarse considerando su criticidad y ciclo de vida

f) Roles y responsabilidades

- **Dirección Técnica:** aprobar y supervisar el cumplimiento de la presente política
- **Responsable de Seguridad de la Información:** coordinar la gestión de vulnerabilidades y verificar la aplicación de los controles definidos
- **Área de Tecnología / Infraestructura:** implementar los controles técnicos de actualización, monitoreo y mantenimiento
- **Talento Humano:** coordinar procesos de capacitación relacionados con buenas prácticas operativas y de seguridad
- **Proveedores externos:** cumplir con los lineamientos de seguridad establecidos en esta política y en los contratos respectivos

g) Cumplimiento y seguimiento

El cumplimiento de esta política será verificado mediante las siguientes acciones.

- Auditorías internas de seguridad de la información
- Indicadores de desempeño definidos en los planes de acción asociados
- Revisiones periódicas del estado de vulnerabilidades, actualizaciones y mantenimiento

h) Sanciones por incumplimiento

El incumplimiento de esta política podrá dar lugar a:

- Medidas administrativas conforme a la normativa interna de la EPAA-AA

- Restricción o revocación de accesos a sistemas institucionales
- Aplicación de sanciones disciplinarias de acuerdo con la gravedad del incumplimiento
- En el caso de proveedores, la aplicación de penalizaciones contractuales o la terminación del contrato, según corresponda

i) Relación con los planes de acción

La presente política respalda directamente los siguientes planes de acción:

- **4.9.1** Evitar riesgo de malware por falta de actualizaciones de seguridad
- **4.9.3** Reducción del riesgo por errores en el código
- **4.9.5** Prevención de fallas de hardware

j) Vigencia y revisión

La política entrará en vigencia a partir de su aprobación por la autoridad competente y deberá ser revisada al menos una vez al año o cuando se produzcan cambios significativos en el entorno tecnológico o en los riesgos de la organización.

4.8.2 Política de Control de Accesos y Gestión de Identidades

a) Objetivo

Establecer los lineamientos institucionales para la gestión segura de identidades, credenciales, usuarios y roles de acceso a los sistemas de información de la EPAA-AA, con el fin de prevenir accesos no autorizados, reducir el uso indebido de privilegios y garantizar que el acceso a la información se otorgue únicamente conforme a las funciones y responsabilidades asignadas.

b) Alcance

La presente política aplica a:

- Todos los sistemas de información, aplicaciones, bases de datos y plataformas tecnológicas de la EPAA-AA
- Usuarios administrativos, operativos y técnicos, incluyendo personal interno y terceros autorizados

- Procesos de creación, modificación, revisión y revocación de cuentas de usuario
- Mecanismos de autenticación, autorización y monitoreo de accesos

c) Principios generales

La gestión de accesos e identidades se regirá por los siguientes principios:

- **Mínimo privilegio:** cada usuario contará únicamente con los accesos estrictamente necesarios para el desempeño de sus funciones
- **Segregación de funciones:** se evitará la concentración de privilegios incompatibles en una misma cuenta de usuario
- **Autenticación robusta:** el acceso a sistemas críticos deberá protegerse mediante mecanismos de autenticación reforzada
- **Trazabilidad:** todas las acciones relevantes realizadas por los usuarios deberán ser registradas y auditables
- **Revisión periódica:** los accesos otorgados deberán evaluarse de forma regular para asegurar su vigencia y pertinencia

d) Lineamientos de la política

Gestión de usuarios y roles

- Se deberá mantener un inventario actualizado de todas las cuentas de usuario y sus roles asignados
- Los roles de acceso deberán definirse formalmente y alinearse a las funciones organizacionales
- La creación, modificación o eliminación de cuentas deberá estar debidamente autorizada y documentada

Gestión de credenciales y contraseñas

- Las contraseñas deberán cumplir criterios de complejidad, longitud mínima y caducidad periódica
- Se prohíbe el uso de credenciales compartidas entre usuarios
- Las credenciales comprometidas o sospechosas deberán ser revocadas de forma inmediata

Autenticación segura

- Los sistemas críticos deberán implementar mecanismos de autenticación multifactor (MFA)
- Se priorizará el uso de soluciones de autenticación compatibles con los sistemas existentes, incluidos aquellos de carácter operativo como SCADA y facturación
- Los intentos de acceso fallidos deberán ser monitoreados y gestionados conforme a procedimientos establecidos

Revisión y control de accesos

- Se deberán realizar revisiones periódicas de los privilegios asignados a los usuarios
- Las cuentas inactivas o asociadas a personal que haya cambiado de funciones deberán ser deshabilitadas o eliminadas
- Se deberán configurar alertas ante accesos no autorizados o comportamientos anómalos

e) Roles y responsabilidades

- **Responsable de Seguridad de la Información:** definir, supervisar y evaluar el cumplimiento de esta política
- **Administradores de Sistemas:** implementar los controles técnicos de autenticación, autorización y monitoreo
- **Talento Humano:** notificar oportunamente cambios de rol, ingreso o salida de personal que afecten los accesos
- **Auditoría Interna:** verificar periódicamente la correcta aplicación de los controles de acceso
- **Usuarios:** utilizar sus credenciales de forma responsable y conforme a los lineamientos establecidos

f) Cumplimiento y seguimiento

El cumplimiento de esta política será evaluado mediante:

- Auditorías internas de accesos y privilegios
- Revisión de registros de autenticación y uso de sistemas
- Indicadores de desempeño definidos en los planes de acción asociados

g) Sanciones por incumplimiento

El incumplimiento de esta política podrá derivar en lo siguiente

- Suspensión temporal o definitiva de accesos a los sistemas institucionales
- Aplicación de sanciones administrativas o disciplinarias conforme a la normativa interna
- Responsabilidades contractuales en el caso de terceros o proveedores
- Acciones legales cuando el incumplimiento derive en afectaciones graves a la organización

h) Relación con los planes de acción

La presente política respalda directamente los siguientes planes de acción:

- **4.9.2** Reducción del riesgo de accesos no autorizados por gestión deficiente de contraseñas
- **4.9.6** Prevención de accesos no autorizados por falta de autenticación segura
- **4.9.18** Reducción de accesos no autorizados por gestión inadecuada de usuarios y roles

i) Vigencia y revisión

La política entrará en vigencia una vez aprobada por la autoridad competente y deberá revisarse de manera anual o cuando se produzcan cambios relevantes en la estructura organizacional, tecnológica o en los riesgos identificados.

4.8.3 Política de Seguridad Física y del Entorno

a) Objetivo

Establecer los lineamientos institucionales para la protección física de las instalaciones, infraestructuras y activos de información de la EPAA-AA, con el fin de prevenir accesos físicos no autorizados, robos, daños, sabotajes o pérdidas que

puedan afectar la confidencialidad, integridad o disponibilidad de la información y de los servicios esenciales

b) Alcance

La presente política aplica para lo siguiente.

- Todas las instalaciones físicas de la EPAA-AA, incluyendo oficinas administrativas, centros de atención, centros de control, salas de servidores, estaciones de bombeo y áreas de archivo
- Equipos tecnológicos, dispositivos informáticos y medios físicos que contengan información institucional
- Personal interno, contratistas, proveedores y visitantes que accedan a las instalaciones
- Sistemas de control de acceso físico, vigilancia, monitoreo y protección del entorno

c) Principios generales

La seguridad física y del entorno se regirá por los siguientes principios

- **Protección por zonas:** las instalaciones deberán clasificarse según su nivel de criticidad y riesgo
- **Control de accesos físicos:** el ingreso a áreas sensibles deberá estar restringido y monitoreado
- **Prevención y disuasión:** se priorizará la implementación de controles que reduzcan la probabilidad de incidentes físicos
- **Trazabilidad:** los accesos y eventos relevantes deberán ser registrables y auditables
- **Concienciación:** el personal deberá conocer y respetar las normas de seguridad física establecidas

d) Lineamientos de la política

Protección de instalaciones

- Las áreas críticas deberán contar con mecanismos de control de acceso físico acordes a su nivel de riesgo
- Se deberán implementar sistemas de vigilancia y monitoreo en zonas sensibles
- Las áreas de almacenamiento de información física deberán mantenerse bajo condiciones de seguridad adecuadas

Protección de equipos y dispositivos

- Los equipos informáticos deberán contar con mecanismos de protección física contra robo o manipulación no autorizada
- Se deberá mantener un inventario actualizado de los activos tecnológicos
- El traslado de equipos fuera de las instalaciones deberá estar debidamente autorizado y documentado

Gestión de visitantes

- El acceso de visitantes a las instalaciones deberá estar controlado, registrado y limitado a las áreas autorizada
- Los visitantes deberán estar acompañados cuando ingresen a zonas restringida
- Se deberán definir procedimientos claros para el ingreso de proveedores y personal externo

Concienciación en seguridad física

- El personal deberá recibir capacitación periódica sobre prácticas seguras relacionadas con la protección física de los activos
- Se deberán difundir normas claras sobre el uso adecuado de instalaciones y equipo
- Cualquier incidente o situación irregular deberá ser reportada de manera inmediata.

e) Roles y responsabilidades

- **Dirección Administrativa:** garantizar la disponibilidad de recursos para la implementación de controles físicos

- **Responsable de Seguridad de la Información:** coordinar la integración de la seguridad física con el SGSI
- **Seguridad Física / Infraestructura:** implementar y mantener los controles de acceso, vigilancia y protección
- **Talento Humano:** apoyar los procesos de concienciación y capacitación del personal
- **Usuarios:** cumplir los lineamientos establecidos y reportar incidentes de seguridad física

f) Cumplimiento y seguimiento

El cumplimiento de esta política será verificado mediante:

- Inspecciones periódicas de las instalaciones
- Revisión de registros de acceso físico y eventos de seguridad
- Evaluación de indicadores definidos en los planes de acción asociados

g) Sanciones por incumplimiento

El incumplimiento de la presente política podrá conllevar:

- Restricción o revocación de accesos físicos
- Aplicación de sanciones administrativas conforme a la normativa interna
- Responsabilidades contractuales para terceros o proveedores
- Acciones legales cuando se generen daños a los activos o a la información institucional

h) Relación con los planes de acción

La presente política respalda directamente los siguientes planes de acción:

- **4.9.4** Prevención de robo o pérdida de dispositivos
- **4.9.5** Prevención de fallas de hardware por mantenimiento inadecuado
- **4.9.8** Prevención de pérdida de documentos físicos por ausencia de controles
- **4.9.10** Prevención de intrusión física.

i) Vigencia y revisión

Esta política entrará en vigencia una vez aprobada por la autoridad competente y deberá revisarse de forma anual o cuando se produzcan cambios relevantes en la infraestructura física, en el entorno operativo o en los riesgos identificados.

4.8.4 Política de Continuidad del Servicio y Respaldo de la Información

a) Objetivo

Establecer los lineamientos institucionales para garantizar la continuidad de los servicios tecnológicos y la protección de la información de la EPAA-AA frente a incidentes que puedan afectar la disponibilidad, integridad y confiabilidad de los datos, mediante la implementación de mecanismos adecuados de respaldo, redundancia y recuperación.

b) Alcance

La presente política aplica para lo siguiente.

- Todos los sistemas de información críticos de la EPAA-AA, incluyendo facturación, contabilidad, gestión documental, plataformas operativas y sistemas SCADA
- Las bases de datos que almacenan información financiera, operativa, técnica y de usuarios
- Infraestructura tecnológica asociada a la prestación continua de los servicios
- Personal técnico, administrativo y proveedores que gestionen o administren información institucional

c) Principios generales

La continuidad del servicio y el respaldo de la información se regirán por los siguientes principios:

- **Disponibilidad permanente:** los servicios críticos deben mantenerse operativos dentro de niveles aceptables

- **Integridad de la información:** los datos deben conservar su exactitud y consistencia ante fallas o incidentes
- **Prevención y preparación:** se prioriza la anticipación frente a la reacción
- **Recuperabilidad:** la información debe poder restaurarse de forma confiable y oportuna
- **Responsabilidad compartida:** la continuidad del servicio involucra a áreas técnicas, administrativas y de gestión

d) Lineamientos de la política

Respaldo de la información

- Todos los sistemas críticos deberán contar con mecanismos automáticos y periódicos de respaldo
- Los respaldos deberán almacenarse en ubicaciones seguras, separadas de los sistemas productivos
- Se deberán realizar pruebas periódicas de restauración para verificar la efectividad de los respaldos
- Los procedimientos de respaldo y recuperación deberán estar documentados y actualizados

Integridad de los datos

- Se deberán implementar controles que garanticen la integridad de los datos durante su almacenamiento y procesamiento
- Los accesos y modificaciones a bases de datos deberán ser trazables y auditables
- Se deberán realizar auditorías periódicas a las configuraciones y registros de las bases de datos

Continuidad del servicio

- Los servicios críticos deberán contar con mecanismos de redundancia acordes a su nivel de criticidad
- Se deberán definir tiempos objetivos de recuperación para los sistemas prioritarios

- Los procedimientos de recuperación ante incidentes deberán ser conocidos por el personal responsable
- La continuidad operativa deberá evaluarse periódicamente mediante pruebas controladas

Capacitación y concienciación

- El personal involucrado en la gestión de sistemas críticos deberá recibir capacitación específica sobre respaldo, recuperación y continuidad
- Se deberán difundir buenas prácticas relacionadas con la protección de la información y la continuidad del servicio

e) Roles y responsabilidades

- **Dirección Técnica:** aprobar los lineamientos de continuidad y asignar recursos necesarios
- **Responsable de Seguridad de la Información:** coordinar la integración de esta política con el SGSI
- **Área de Sistemas / Tecnología:** implementar y mantener los mecanismos de respaldo, redundancia y recuperación
- **Talento Humano:** apoyar los procesos de capacitación relacionados con esta política
- **Usuarios:** cumplir los procedimientos establecidos y reportar incidentes que afecten la continuidad del servicio

f) Cumplimiento y seguimiento

El cumplimiento de esta política será evaluado mediante:

- Revisión de registros de respaldo y restauración
- Resultados de pruebas de continuidad y recuperación
- Seguimiento de indicadores definidos en los planes de acción asociados
- Auditorías internas de seguridad de la información

g) Sanciones por incumplimiento

El incumplimiento de la presente política podrá dar lugar a lo siguiente.

- Aplicación de sanciones administrativas conforme a la normativa interna

- Restricción de responsabilidades técnicas en la gestión de sistemas críticos
- Acciones contractuales frente a proveedores o terceros
- Medidas correctivas cuando se comprometa la continuidad del servicio o la integridad de la información

h) Relación con los planes de acción

La presente política respalda directamente los siguientes planes de acción:

- **4.9.11** Prevención de intercepción de datos
- **4.9.16** Evitar la pérdida de integridad de los datos
- **4.9.17** Reducir la interrupción de los servicios

i) Vigencia y revisión

Esta política entrará en vigencia una vez aprobada por la autoridad competente y deberá revisarse de forma anual o cuando se presenten cambios relevantes en la infraestructura tecnológica, en los servicios críticos o en el análisis de riesgos del SGSI.

4.8.5 Política de Seguridad en Comunicaciones y Redes

a) Objetivo

Establecer los lineamientos institucionales para proteger la confidencialidad, integridad y disponibilidad de la información que se transmite o procesa a través de las redes de comunicación de la EPAA-AA, mediante la implementación de controles técnicos, administrativos y organizativos que prevengan accesos no autorizados, interceptación de datos y configuraciones inseguras.

b) Alcance

La presente política aplica a:

- Todas las redes de datos de la EPAA-AA, tanto internas como externas.
- Infraestructura de red que incluye routers, switches, firewalls, enlaces de comunicación y redes inalámbricas
- Sistemas de información que transmiten datos sensibles o críticos, incluyendo plataformas administrativas, operativas y SCADA

- Accesos remotos, enlaces entre sedes y comunicaciones con proveedores externos
- Personal técnico, administrativo y terceros que gestionen, operen o utilicen los recursos de red institucionales

c) Principios generales

La seguridad en las comunicaciones y redes se rige por los siguientes principios:

- **Defensa en profundidad:** implementación de múltiples capas de protección
- **Acceso controlado:** solo usuarios y dispositivos autorizados pueden acceder a la red
- **Cifrado obligatorio:** la información sensible debe transmitirse de forma segura
- **Segmentación:** separación lógica de redes para reducir el impacto de incidentes
- **Monitoreo continuo:** detección temprana de accesos o comportamientos anómalos

d) Lineamientos de la política

Protección de las comunicaciones

- Toda comunicación que involucre información sensible o crítica deberá utilizar mecanismos de cifrado robustos
- Se deberán emplear protocolos seguros para la transmisión de datos internos y externos
- Las configuraciones de cifrado deberán revisarse periódicamente para garantizar su vigencia y efectividad

Seguridad de la infraestructura de red

- Los dispositivos de red deberán configurarse siguiendo principios de seguridad por defecto
- Se deberá restringir el acceso administrativo a los equipos de red únicamente a personal autorizado
- Las configuraciones de red deberán documentarse y mantenerse actualizadas

Control de accesos a la red

- El acceso a la red deberá estar basado en autenticación y autorización adecuadas
- Se deberá implementar segmentación de red para aislar sistemas críticos y redes operativas
- Las redes de invitados deberán mantenerse separadas de las redes internas y operativas

Monitoreo y detección

- Se deberán implementar mecanismos de registro y monitoreo del tráfico de red
- Los eventos de seguridad detectados deberán ser analizados y atendidos oportunamente
- Se deberán generar alertas ante intentos de acceso no autorizado o actividades anómalas

Concienciación y buenas prácticas

- El personal deberá ser capacitado en el uso seguro de redes y comunicaciones
- Se deberán difundir lineamientos sobre el manejo seguro de información transmitida por medios digitales
- El uso de redes institucionales deberá limitarse exclusivamente a fines autorizados.

e) Roles y responsabilidades

- **Dirección Técnica:** aprobar y respaldar los controles de seguridad de red
- **Área de Tecnología / Redes:** implementar, administrar y monitorear la infraestructura de comunicaciones
- **Responsable de Seguridad de la Información:** supervisar el cumplimiento de esta política dentro del SGSI
- **Talento Humano:** coordinar acciones de capacitación relacionadas con seguridad en redes

- **Usuarios:** cumplir las disposiciones establecidas y reportar incidentes de seguridad

f) Cumplimiento y seguimiento

El cumplimiento de esta política se verificará mediante:

- Auditorías a configuraciones de red y dispositivos de seguridad
- Revisión de registros y alertas de tráfico
- Seguimiento de los indicadores definidos en los planes de acción asociados
- Evaluaciones periódicas de vulnerabilidades en la red

g) Sanciones por incumplimiento

El incumplimiento de la presente política podrá conllevar:

- Medidas administrativas conforme a la normativa institucional
- Suspensión o restricción de accesos a la red institucional
- Aplicación de sanciones contractuales a proveedores o terceros
- Acciones correctivas cuando se comprometa la seguridad de las comunicaciones

h) Relación con los planes de acción

La presente política respalda directamente los siguientes planes de acción:

- **4.9.11** Prevención de intercepción de datos
- **4.9.12** Reducción del acceso no autorizado a la red

i) Vigencia y revisión

Esta política entrará en vigencia tras su aprobación formal y deberá revisarse al menos una vez al año, o cuando se produzcan cambios relevantes en la infraestructura de red, tecnologías de comunicación o en el análisis de riesgos del SGSI.

4.8.6 Política de Gestión de Proveedores y Servicios Externos

a) Objetivo

Establecer los lineamientos institucionales para gestionar de manera segura la relación con proveedores y terceros que tengan acceso a información, sistemas o servicios críticos de la EPAA-AA, garantizando que los riesgos asociados a la dependencia externa, confidencialidad de la información y continuidad del servicio sean adecuadamente controlados, reducidos o transferidos conforme a los principios del SGSI.

b) Alcance

La presente política aplica a lo siguiente.

- Todos los proveedores externos que suministren servicios tecnológicos, operativos o de soporte a la EPAA-AA
- Contratos relacionados con conectividad, hosting, soporte de sistemas, infraestructura tecnológica, SCADA, software y servicios críticos
- Personal interno involucrado en procesos de contratación, supervisión y gestión de proveedores
- Proveedores que tengan acceso directo o indirecto a información sensible, infraestructura tecnológica o servicios esenciales

c) Principios generales

La gestión de proveedores se fundamenta en los siguientes principios:

- **Responsabilidad compartida:** la seguridad de la información debe ser garantizada tanto por la EPAA-AA como por los proveedores
- **Gestión contractual del riesgo:** los riesgos asociados a terceros deben ser tratados mediante acuerdos formales
- **Confidencialidad obligatoria:** la información institucional debe protegerse durante toda la relación contractual
- **Continuidad del servicio:** los servicios críticos deben contar con compromisos claros de disponibilidad
- **Supervisión continua:** el cumplimiento de los acuerdos debe ser verificado periódicamente.

d) Lineamientos de la política

Evaluación y selección de proveedores

- Antes de la contratación, se deberá evaluar el impacto que el proveedor tendrá sobre la seguridad de la información y la continuidad operativa
- Se priorizarán proveedores que demuestren capacidad técnica, experiencia y compromiso con la seguridad de la información
- Los proveedores críticos deberán identificarse y mantenerse actualizados en un inventario institucional

Cláusulas contractuales de seguridad

- Todos los contratos con proveedores que accedan a información sensible deberán incluir cláusulas de confidencialidad
- Los contratos deberán establecer responsabilidades claras sobre el manejo, protección y uso de la información
- Se deberán definir penalizaciones en caso de incumplimiento de las obligaciones de seguridad

Acuerdos de nivel de servicio (SLA)

- Los servicios críticos deberán contar con acuerdos de nivel de servicio formalmente establecidos
- Los SLA deberán definir, como mínimo, niveles de disponibilidad, tiempos de respuesta, mecanismos de soporte y penalizaciones
- Los acuerdos deberán revisarse y actualizarse periódicamente según la criticidad del servicio

Gestión de la continuidad y respaldo

- Se deberán identificar alternativas de respaldo para proveedores considerados críticos
- La dependencia de un proveedor único deberá ser analizada y, de ser posible, mitigada
- Los proveedores deberán informar oportunamente cualquier evento que pueda afectar la continuidad del servicio

Supervisión y seguimiento

- Se deberá realizar un seguimiento periódico del cumplimiento de los contratos y SLA
- El desempeño de los proveedores críticos deberá evaluarse mediante indicadores definidos
- Los incumplimientos deberán documentarse y gestionarse conforme a los procedimientos institucionales

e) Roles y responsabilidades

- **Dirección Administrativa Financiera:** supervisar la contratación y gestión de proveedores
- **Asesoría Legal:** revisar y validar cláusulas contractuales de seguridad y confidencialidad
- **Responsable del SGSI:** verificar que los riesgos asociados a proveedores estén debidamente tratados
- **Área Técnica / TI:** monitorear el cumplimiento técnico de los servicios contratados
- **Proveedores:** cumplir las obligaciones contractuales y de seguridad establecidas

f) Cumplimiento y seguimiento

El cumplimiento de esta política se verificará mediante:

- Revisión periódica de contratos y SLA vigentes
- Evaluación del desempeño de proveedores críticos
- Auditorías documentales relacionadas con seguridad de la información
- Seguimiento de indicadores definidos en los planes de acción asociados

g) Sanciones por incumplimiento

El incumplimiento de esta política podrá dar lugar a lo siguiente.

- Aplicación de penalizaciones contractuales
- Suspensión o terminación de contratos
- Restricción de accesos a información o sistemas institucionales

- Acciones legales conforme a la normativa vigente

h) Relación con los planes de acción

La presente política respalda directamente los siguientes planes de acción:

- **4.9.13** Transferir el fallo de los proveedores
- **4.9.14** Reducción del acceso a información sensible por terceros
- **4.9.15** Transferir la interrupción del servicio mediante SLA

i) Vigencia y revisión

Esta política entrará en vigencia una vez aprobada por la autoridad competente y deberá revisarse al menos una vez al año, o cuando se produzcan cambios relevantes en los proveedores, contratos, servicios críticos o en el análisis de riesgos del SGSI.

4.8.7 Política de Clasificación y Protección de la Información

a) Objetivo

Establecer los lineamientos institucionales para la correcta clasificación, manejo, almacenamiento, protección y divulgación de la información de la EPAA-AA, con el fin de prevenir la pérdida, el acceso no autorizado y la divulgación accidental de información, garantizando la confidencialidad, integridad y disponibilidad de los activos de información.

b) Alcance

La presente política aplica a:

- Toda la información generada, procesada, almacenada o transmitida por la EPAA-AA, independientemente de su formato (físico o digital)
- Documentos administrativos, legales, financieros, técnicos, operativos y de usuarios
- Personal directivo, administrativo, técnico, operativo y contratistas
- Sistemas de información, repositorios documentales, archivos físicos y digitales

c) Principios generales

La clasificación y protección de la información se rige por los siguientes principios:

- **Necesidad de conocer:** el acceso a la información se limita según funciones y responsabilidades
- **Protección proporcional:** el nivel de protección se ajusta a la criticidad de la información
- **Responsabilidad compartida:** todo el personal es responsable del manejo adecuado de la información
- **Trazabilidad:** las actividades sobre la información deben poder ser identificadas y auditadas
- **Cumplimiento normativo:** el manejo de la información se ajusta a la normativa legal y regulatoria vigente

d) Clasificación de la información

La EPAA-AA clasifica la información en los siguientes niveles:

- **Información Pública:** información que puede ser divulgada sin restricciones
- **Información de Uso Interno:** información destinada únicamente al personal autorizado
- **Información Confidencial:** información sensible cuya divulgación no autorizada puede causar impactos operativos, legales o reputacionales
- **Información Crítica:** información esencial para la continuidad del servicio y el cumplimiento legal

Cada tipo de información deberá ser identificado, etiquetado y tratado conforme a su nivel de clasificación.

e) Lineamientos de protección

Protección de información física

- Los documentos físicos clasificados deberán almacenarse en archivadores o gabinetes con cerradura

- Las áreas de archivo deberán contar con controles de acceso físico
- Se deberá mantener un inventario actualizado de documentos críticos
- El acceso a archivos físicos estará limitado al personal autorizado

Protección de información digital

- La información digital clasificada deberá almacenarse en sistemas con controles de acceso y respaldo
- Se deberán aplicar políticas de respaldo periódico para documentos críticos
- Los repositorios digitales deberán contar con mecanismos de autenticación y registro de accesos
- La digitalización de documentos deberá realizarse en repositorios institucionales seguros

Prevención de divulgación accidental

- Se deberán establecer y difundir políticas de confidencialidad claras
- El personal deberá recibir capacitación periódica sobre el manejo seguro de la información
- Se deberán incorporar cláusulas de confidencialidad en contratos laborales y acuerdos internos
- El uso de dispositivos externos y medios removibles deberá estar regulado

f) Roles y responsabilidades

- **Dirección Administrativa:** supervisar la correcta gestión documental institucional
- **Gestión Documental / Archivo:** garantizar el almacenamiento seguro y ordenado de los documentos
- **Responsable del SGSI:** verificar la correcta clasificación y protección de la información
- **Talento Humano:** coordinar procesos de capacitación y concienciación
- **Todo el personal:** cumplir los lineamientos establecidos en esta política

g) Cumplimiento y seguimiento

El cumplimiento de esta política se verificará mediante.

- Auditorías documentales periódicas
- Revisiones de accesos a información clasificada
- Seguimiento de incidentes relacionados con pérdida o divulgación de información
- Evaluación de indicadores definidos en los planes de acción asociados

h) Sanciones por incumplimiento

El incumplimiento de esta política podrá dar lugar a lo siguiente.

- Llamados de atención administrativos
- Aplicación de sanciones disciplinarias conforme a la normativa interna
- Restricción o revocación de accesos a la información
- Acciones legales en caso de afectación grave a la institución

i) Relación con los planes de acción

La presente política respalda directamente los siguientes planes de acción:

- **4.9.7** Prevención de pérdida de documentos por almacenamiento inseguro
- **4.9.8** Prevención de pérdida de documentos físicos por ausencia de controles
- **4.9.9** Reducción del riesgo de divulgación accidental de información

j) Vigencia y revisión

Esta política entrará en vigencia una vez aprobada por la autoridad competente y deberá revisarse al menos una vez al año, o cuando se produzcan cambios en los procesos documentales, el análisis de riesgos o la normativa aplicable.

4.8.8 Política de Concienciación, Formación y Cultura de Seguridad de la Información

a) Objetivo

Establecer los lineamientos institucionales para la concienciación, formación continua y fortalecimiento de la cultura organizacional en materia de seguridad de

la información en la EPAA-AA, con el fin de reducir los riesgos asociados a errores humanos, prácticas inseguras y desconocimiento de los controles de seguridad, promoviendo el cumplimiento del SGSI y de la norma ISO/IEC 27001:2022.

b) Alcance

La presente política aplica a:

- Todo el personal de la EPAA-AA, independientemente de su nivel jerárquico o tipo de vinculación
- Personal técnico, administrativo, operativo y directivo
- Contratistas, proveedores y terceros que tengan acceso a información o sistemas institucionales
- Usuarios que participen en procesos críticos relacionados con la información

c) Principios generales

La concienciación y formación en seguridad de la información se rige por los siguientes principios:

- **Responsabilidad individual:** cada persona es responsable de proteger la información que utiliza
- **Prevención:** la formación reduce incidentes antes de que ocurra
- **Mejora continua:** el conocimiento en seguridad debe actualizarse de forma permanente.
- **Enfoque práctico:** la capacitación debe ser comprensible y aplicable al contexto real de la EPAA-AA
- **Cultura organizacional:** la seguridad de la información es parte integral del trabajo diario

d) Lineamientos de concienciación y formación

Programas de concienciación

- Se deberán implementar campañas periódicas de concienciación en seguridad de la información

- Las campañas deberán abordar temas como: contraseñas seguras, manejo de información confidencial, malware, phishing, accesos no autorizados y buenas prácticas digitales
- La concienciación deberá adaptarse a los diferentes perfiles del personal

Formación continua

- El personal deberá recibir capacitación inicial y periódica en seguridad de la información
- Las capacitaciones deberán alinearse con los riesgos identificados en el SGSI
- El personal técnico deberá recibir formación especializada según sus funcione
- La participación en actividades de formación deberá quedar registrada.

Integración en procesos institucionales

- La seguridad de la información deberá incorporarse en los procesos de inducción de nuevo personal
- Los cambios de rol o responsabilidades deberán incluir capacitación específica
- La cultura de seguridad deberá reforzarse en evaluaciones internas y comunicaciones institucionales

e) Roles y responsabilidades

- **Talento Humano:** coordinar y gestionar los programas de capacitación y concienciación
- **Responsable del SGSI:** definir contenidos, evaluar efectividad y proponer mejoras
- **Direcciones y jefaturas:** asegurar la participación del personal a su cargo
- **Todo el personal:** cumplir con las disposiciones y aplicar las buenas prácticas aprendidas

f) Medición y seguimiento

La efectividad de esta política se evaluará mediante:

- Indicadores de participación en capacitaciones
- Evaluaciones periódicas de conocimiento
- Análisis de incidentes relacionados con errores humanos
- Resultados de auditorías internas del SGSI

g) Sanciones por incumplimiento

El incumplimiento de las disposiciones establecidas en esta política podrá dar lugar a:

- Llamados de atención administrativos
- Requerimientos obligatorios de capacitación adicional
- Restricción de accesos a sistemas o información
- Aplicación de sanciones conforme a la normativa interna vigente

h) Relación con los planes de acción

La presente política respalda directamente los siguientes planes de acción:

- **4.9.1** Evitar riesgo de malware por falta de actualizaciones de seguridad
- **4.9.2** Reducción del riesgo de accesos no autorizados
- **4.9.3** Reducción del riesgo por errores en el código
- **4.9.6** Prevención de accesos no autorizados por falta de autenticación segura
- **4.9.9** Reducción del riesgo de divulgación accidental de información
- **4.9.17** Reducción de la interrupción de los servicios
- **4.9.18** Reducción de accesos no autorizados por gestión inadecuada de usuarios y roles

i) Vigencia y revisión

Esta política entrará en vigencia una vez aprobada por la máxima autoridad institucional y será revisada anualmente o cuando se produzcan cambios relevantes en el análisis de riesgos, el SGSI o la normativa aplicable.

4.9 Plan de acción

La presente sección desarrolla los planes de acción propuestos para el tratamiento de los riesgos de seguridad de la información identificados como prioritarios en la etapa de evaluación (TABLA 19),

estos planes representan una propuesta técnica orientada a definir de manera estructurada, las intervenciones necesarias para la mitigación de los riesgos que requieren tratamiento activo dentro del futuro Sistema de Gestión de la Seguridad de la Información (SGSI) de la EPAA-AA. La implementación efectiva dependería, en una fase posterior, del compromiso formal de la alta dirección, la asignación de recursos y su adecuación a la dinámica operativa de la entidad.

Cada plan de acción responde de forma directa a un riesgo específico clasificado con tratamiento "Evitar", "Reducir" o "Transferir". De los veintiún riesgos analizados, dieciocho fueron considerados como requirentes de intervención mediante planes específicos, mientras que los riesgos CT-04.2, CT-04.3 y CT-05.2 fueron tratados bajo el criterio de "Aceptar", dado que su nivel residual se encuentra alineado con el apetito de riesgo institucional de la EPAA-AA. La relación entre los planes propuestos y los procesos críticos de la organización se documenta en la Matriz de Trazabilidad de Controles con Impacto Empresarial (Anexo 6), evidenciando cómo la aplicación de los controles de la norma ISO/IEC 27001 contribuye a la protección de procesos esenciales para la continuidad del servicio de agua potable.

En coherencia con el marco normativo interno del SGSI definido en la sección 4.8, los planes de acción presentados en esta sección representan la materialización operativa de las políticas de seguridad de la información propuestas. Cada plan se encuentra respaldado normativamente por una o más de las políticas marco establecidas, garantizando que las acciones planteadas cuenten con sustento institucional, lo cual evita la aplicación de medidas aisladas o sin lineamientos formales. Con este enfoque se asegura la trazabilidad entre riesgos, políticas, controles, así como acciones, fortaleciendo la coherencia metodológica de la propuesta de SGSI.

El diseño junto con la organización de los planes de acción se fundamentaron en criterios técnicos que garantizan una implementación tanto lógica como coherente, entre estos criterios se consideran la criticidad del riesgo determinada en la matriz de calor, las dependencias existentes entre planes priorizando la definición de políticas con los lineamientos antes de la aplicación de controles técnicos, por último una estimación temporal realista. Para cada acción se estableció un plazo técnico junto con un plazo estimado ajustado al contexto institucional de la EPAA-AA, incorporando los procesos tanto de aprobación como gestión propios de una empresa pública.

Cada plan de acción incorpora indicadores clave de desempeño (KPIs) diseñados para permitir la medición objetiva de su efectividad, estos indicadores se derivan directamente de los controles

aplicables del Anexo A de la norma ISO/IEC 27001:2022 y consideran fórmulas de cálculo, metas alcanzables, junto con frecuencias de medición acordes con la capacidad operativa de la EPAA-AA. La inclusión de estos indicadores tiene un doble propósito, por una parte la validación técnica de la propuesta planteada, por otra parte en cambio servir como referencia para una futura planificación del monitoreo del SGSI, reconociendo que los valores definidos deberán ser ajustados durante una eventual etapa de implementación.

Para asegurar la coherencia junto con claridad del análisis, todos los planes de acción siguen una estructura uniforme que incluye la descripción del contexto del riesgo, el objetivo del tratamiento, los controles normativos aplicables, las acciones específicas con responsables y con plazos estimados, los resultados esperados, los indicadores de medición, junto a las consideraciones prácticas relevantes para la EPAA-AA.

La ejecución conjunta de los 18 planes propuestos, considerando sus interrelaciones junto a los requerimientos de recursos, se representa de manera consolidada en el Diagrama de Gantt incluido en el Anexo 5, el cual demuestra la viabilidad de una implementación progresiva en un horizonte aproximado de doce meses.

4.9.1 Evitar riesgo de malware por falta de actualizaciones de seguridad

Descripción	
Amenaza	Malware o software malicioso que puede comprometer la confidencialidad, integridad y disponibilidad de la información
Vulnerabilidad	Falta de actualizaciones de seguridad en sistemas operativos, software de aplicaciones, firmware y componentes de red
Nivel de riesgo	Muy alto, debido a la alta probabilidad de ocurrencia y al impacto crítico sobre los activos de información
Objetivo	Evitar el riesgo mediante la implementación de mecanismos que aseguren la actualización oportuna y automática de todos los sistemas, cerrando así la brecha de vulnerabilidad que permitiría la ejecución de malware

Política de respaldo	Política de Gestión de Vulnerabilidades y Seguridad Operacional, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-01.1 - Malware por falta de actualizaciones - Tratamiento: EVITAR (Riesgo: 20 - MA - Muy Alto)

Controles ISO/IEC 27001:2022 aplicables

- A.5.23 - Gestión de parches de software
- A.5.9 - Inventario de información y otros activos
- A.5.10 - Aceptación, uso y eliminación de activos
- A.5.15 - Restricción de instalación de software
- A.5.28 - Pruebas de seguridad de TI
- A.6.3 - Concientización, educación y capacitación

Acciones específicas y responsables

N°	**Acción**	**Responsable**	**Plazo**	**Plazo estimado EPAA-AA**
1	Establecer una política institucional para la actualización automática y obligatoria de software	Dirección Técnica / Seguridad de la Información	2 semana	3-4 semanas
2	Implementar mecanismos automáticos de actualización de software y sistemas	Área de Infraestructura y Soporte Técnico	4 semanas	6-7 semanas
3	Realizar un inventario actualizado de todos los activos de software y	Seguridad de la Información	2 semana	3-4 semanas

	verificar su estado de actualización			
4	Instalar herramientas de escaneo de vulnerabilidades que alerten sobre software desactualizado	Seguridad de la Información / TIC	4 semanas	6-8 semanas
5	Limitar la instalación de software no autorizado en equipos institucionales	Dirección Técnica / Administración de TI	2 semana	2-3 semanas
6	Capacitar al personal sobre los riesgos del malware y la importancia de mantener los sistemas actualizados	Talento Humano / Seguridad de la Información	6 semanas	9-12 semanas

Resultados esperados

- Reducción significativa del riesgo de infección por malware asociado a software obsoleto
- Eliminación de la vulnerabilidad crítica mediante actualizaciones automáticas y monitoreo constante
- Mayor cumplimiento de los requisitos del SGSI conforme a ISO/IEC 27001:2022
- Sensibilización y participación activa del personal en la protección del entorno digital

Mejora de la postura general de seguridad de la empresa frente a ataques cibernéticos

KPIs (Indicadores de Medición)

Indicador	Objetivo	Fórmula	Meta	Frecuencia
1.1 Cobertura sistema de parches	Medir implementación control A.8.6 (Gestión vulnerabilidades técnicas)	% = (Equipos en sistema centralizado ÷ Total equipos) × 100	100% (6 meses)	Mensual

1.2 Vulnerabilidades críticas pendientes	Evaluar efectividad remediación vulnerabilidades	# = Número de equipos con vulnerabilidades críticas >30 días	0	Trimestral

NOTA

- Este plan mitiga el riesgo CT-01.1 (Malware por falta de actualizaciones), identificado como de criticidad "Muy Alta". La actividad de mayor duración es la capacitación masiva (6 semanas técnicas, 9-12 semanas EPAA-AA), que debe coordinarse con todas las áreas sin interrumpir la operación de servicios críticos. Para EPAA-AA, los plazos se extienden por: 1) Procesos de aprobación gerencial de políticas, 2) Logística para inventariar todo el parque tecnológico, 3) Coordinación de capacitación para personal en diferentes turnos y ubicaciones.

4.9.2 Reducción del riesgo de accesos no autorizados

Descripción	
Amenaza	Accesos no autorizados a sistemas o datos confidenciales, que pueden comprometer la integridad y confidencialidad de la información
Vulnerabilidad	Gestión deficiente de contraseñas, como uso de claves débiles, repetidas o sin renovación periódica
Nivel de riesgo	Medio, debido a una probabilidad moderada y al impacto considerable sobre los activos de información
Objetivo	Reducir el riesgo mediante el fortalecimiento de la gestión de credenciales de acceso y la implementación de políticas seguras de autenticación
Política de respaldo	Política de Control de Accesos y Gestión de Identidades, definida en la sección 4.8 del Marco Normativo Interno del SGSI

Correspondencia con análisis de riesgos:	CT-01.2 - Accesos no autorizados por gestión deficiente de contraseñas - Tratamiento: REDUCIR (Riesgo: 12 - M - Moderado)

Controles ISO/IEC 27001:2022 aplicables

- A.5.17 - Gestión de identidad y autenticación de la información
- A.5.18 - Uso de contraseñas seguras
- A.5.15 - Restricción de instalación de software
- A.5.21 - Control de acceso a redes y servicios
- A.6.3- Concientización, educación y capacitación

Acciones específicas y responsables

N°	Acción	Responsable	Plazo	Plazo estimado EPAA-AA
1	Diseñar y aprobar una política institucional de gestión segura de contraseñas	Seguridad de la Información / Dirección Técnica	3 semanas	5-6 semanas
2	Implementar mecanismos para exigir contraseñas complejas y caducidad periódica	Infraestructura TI / Soporte Técnico	4 semanas	6-7 semanas
3	Auditar las credenciales de acceso actuales y forzar renovación de contraseñas inseguras	Seguridad de la Información	2 semana	3-4 semanas
4	Desplegar autenticación de	Administración de TI	5 semanas	8-10 semanas

	múltiples factores en los sistemas críticos			
5	Capacitar al personal en la creación y gestión segura de contraseñas	Talento Humano / Seguridad de la Información	6 semanas	9-12 semanas

Resultados esperados

- Mejora en la seguridad de las credenciales utilizadas en los sistemas institucionales
- Reducción significativa del riesgo de accesos no autorizados
- Cumplimiento con los controles de seguridad definidos por la norma ISO/IEC 27001

Aumento en la conciencia del personal sobre la importancia de la gestión segura de contraseñas

KPIs (Indicadores de Medición)

Indicador	Objetivo	Fórmula	Meta	Frecuencia
2.1 Cumplimiento política de contraseñas	Implementar control A.5.17 (Información de autenticación)	% = (Cuentas con contraseñas que cumplen política de complejidad y no están expiradas ÷ Total cuentas activas) × 100	95% (mes 6)	Mensual

NOTA

- Dirigido al riesgo CT-01.2 (Accesos no autorizados). La implementación de autenticación multifactor (MFA) en sistemas críticos (acción 4) es técnicamente compleja y requiere evaluación de soluciones compatibles con SCADA y facturación. Para EPAA-AA, la auditoría de credenciales (acción 3) puede revelar necesidad de reestructurar perfiles de acceso existentes. La capacitación (acción 5) debe adaptarse a diferentes niveles de conocimiento tecnológico del personal.

4.9.3 Reducción del riesgo por errores en el código

Descripción

Amenaza	Errores en el código fuente de los sistemas que pueden derivar en fallos de seguridad, pérdida de datos o interrupciones del servicio
Vulnerabilidad	Falta de pruebas y validaciones formales durante el ciclo de desarrollo de software, lo que incrementa el riesgo de errores no detectados
Nivel de riesgo	Medio, dado que los errores en el código pueden ser explotados si no son identificados y corregidos oportunamente
Objetivo	Reducir el riesgo mediante la implementación de controles que fortalezcan el aseguramiento de la calidad del código y validación en ambientes de prueba controlados
Política de respaldo	Política de Gestión de Vulnerabilidades y Seguridad Operacional, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-01.3 - Errores en el código por falta de pruebas - Tratamiento: REDUCIR (Riesgo: 12 - M - Moderado)

Controles ISO/IEC 27001:2022 aplicables

- A.8.25 - Pruebas de seguridad en el desarrollo y aceptación
- A.8.26 - Protección del código fuente
- A.8.27 - Ambientes de prueba seguros
- A.5.32 - Validación de insumos y salidas de datos
- A.6.3 - Concientización, educación y capacitación

Acciones específicas y responsables

N°	Acción	Responsable	Plazo	Plazo estimado EPAA-AA
1	Establecer procedimientos formales de pruebas	Equipo de Desarrollo / Dirección Técnica	5 semanas	7-8 semanas

	unitarias, integrales y de aceptación			
2	Implementar herramientas automáticas de revisión de código (linting, escaneo de vulnerabilidades)	TI / Seguridad de la Información	4 semanas	6-7 semanas
3	Capacitar al personal de desarrollo en buenas prácticas de codificación segura	Talento Humano / Seguridad de la Información	6 semanas	9-12 semanas
4	Establecer entornos separados para pruebas y producción con acceso controlado	TI / Infraestructura	4 semanas	6-8 semanas
5	Realizar auditorías periódicas al código fuente crítico de los sistemas	Auditoría Interna / Seguridad de la Información	Mensual	Mensual

Resultados esperados

- Reducción de errores en producción derivados de problemas de codificación
- Aumento de la calidad y seguridad del software institucional
- Disminución del riesgo de explotación por vulnerabilidades en el código
- Mejora continua en los procesos de desarrollo seguro

KPIs (Indicadores de Medición)

Indicador	Objetivo	Fórmula	Meta	Frecuencia
3.1 Cobertura pruebas de código	Implementar control A.8.25 (Ciclo de vida del desarrollo seguro)	% = (Líneas de código con pruebas ÷ Total líneas críticas) × 100	80% (mes 9)	Trimestral

3.2 Vulnerabilidades en código producción	Medir calidad codificación segura	# = Número de vulnerabilidades críticas detectadas en producción	≤2 por año	Semestral
NOTA				
• Para el riesgo CT-01.3 (Errores en código). EPAA-AA actualmente no cuenta con procedimientos formales de desarrollo seguro, por lo que la acción 1 (establecer procedimientos) es fundacional. La acción 3 (capacitación) probablemente requerirá consultoría externa especializada. La acción 4 puede necesitar inversión en infraestructura adicional para entornos de prueba segregados, especialmente para sistemas críticos como facturación.				

4.9.4 Prevención de robo o pérdida de dispositivos

Descripción	
Amenaza	Robo o pérdida de dispositivos electrónicos como laptops, computadoras y otros equipos informáticos
Vulnerabilidad	Ausencia de sistemas de bloqueo físico y medidas de protección antirrobo en las instalaciones
Nivel de riesgo	Alto, ya que la pérdida de dispositivos puede conllevar la exposición de información confidencial o crítica
Objetivo	Evitar incidentes relacionados con el robo o pérdida de dispositivos mediante controles preventivos físicos, técnicos y organizativos que garanticen su protección
Política de respaldo	Política de Seguridad Física y del Entorno, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-02.1 - Robo o pérdida de dispositivos - Tratamiento: EVITAR (Riesgo: 20 - A - Alto).
Controles ISO/IEC 27001:2022 aplicables	

- A.7.3 - Seguridad física y ambiental
- A.7.7 - Seguridad de los activos fuera del sitio
- A.7.9 - Protección contra robo
- A.8.10 - Registro y control de activos
- A.5.10 - Política de uso aceptable de activos

Acciones específicas y responsables

N°	Acción	Responsable	Plazo	Plazo estimado EPAA-AA
1	Instalar mecanismos de bloqueo físico en estaciones de trabajo y gabinetes	Dirección Técnica / Infraestructura	4 semanas	6-8 semanas
2	Implementar dispositivos antirrobo (candados, anclajes de seguridad, etc.)	Seguridad Física / TI	8 semanas	12-16 semanas
3	Actualizar políticas sobre el uso y traslado de equipos fuera del sitio	Asesoría Legal / Seguridad de la Información	3 semanas	5-6 semanas
4	Sensibilizar al personal sobre los riesgos y buenas prácticas para proteger los dispositivos	Talento Humano / Seguridad de la Información	4 semanas	6-8 semanas
5	Actualizar y revisar periódicamente el inventario de activos informáticos	Jefatura de Tecnología / Auditoría Interna	Mensual	Mensual

Resultados esperados

- Disminución del riesgo de robo o extravío de dispositivos informáticos

- Mayor control y trazabilidad de los equipos
- Concienciación del personal sobre la importancia del resguardo físico
- Mejora en la seguridad física y organizacional de los activos de información

KPIs (Indicadores de Medición)

Indicador	Objetivo	Fórmula	Meta	Frecuencia
4.1 Equipos con bloqueo físico	Implementar control A.7.1 (Perímetro de seguridad física)	% = (Equipos con sistemas antirrobo ÷ Total equipos) × 100	100% (mes 4)	Mensual
4.2 Incidentes robo/pérdida	Medir efectividad controles físicos	# = Número de incidentes reportados	0	Trimestral

NOTA

- Mitiga el riesgo CT-02.1 (Robo/pérdida dispositivos). La acción 2 (dispositivos antirrobo) puede requerir proceso de compra pública si supera umbrales establecidos. Especial atención a equipos portátiles y dispositivos en áreas de acceso público. La sensibilización (acción 4) debe enfocarse en personal de campo que transporta equipos fuera de instalaciones.

4.9.5 Prevención de fallas de Hardware

Descripción	
Amenaza	Fallas de hardware en equipos críticos como servidores, routers y estaciones de trabajo
Vulnerabilidad	Mantenimiento inadecuado, inexistente o no periódico de los componentes físicos
Nivel de riesgo	Alto, debido a la posibilidad de interrupciones en los servicios, pérdida de datos o fallos operacionales
Objetivo	Evitar las fallas de hardware mediante la implementación de controles técnicos y organizativos que garanticen el

	mantenimiento preventivo, monitoreo y reemplazo oportuno de los equipos
Política de respaldo	Política de Seguridad Física y del Entorno, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-02.2 - Fallas de hardware por mantenimiento inadecuado - Tratamiento: EVITAR (Riesgo: 16 - A - Alto)

Controles ISO/IEC 27001:2022 aplicables

- A.7.5 - Mantenimiento de equipos
- A.8.9 - Gestión de la configuración
- A.5.23 - Gestión de cambios
- A.7.4 - Protección contra amenazas físicas y ambientales

Acciones específicas y responsables

N°	Acción	Responsable	Plazo	Plazo estimado EPAA-AA
1	Establecer un cronograma de mantenimiento preventivo para equipos críticos	Dirección Técnica / Área de Infraestructura	6 semanas	9-12 semanas
2	Implementar un sistema de monitoreo de hardware para detectar fallos tempranos	Jefatura de Tecnología / Soporte Técnico	16 semanas	24-32 semanas
3	Actualizar y documentar procedimientos de mantenimiento físico y lógico	Seguridad de la Información / Gestión de Calidad	6 semanas	9-12 semanas

4	Capacitar al personal técnico en buenas prácticas de mantenimiento	Talento Humano / Jefatura Técnica	8 semanas	12-16 semanas
5	Evaluar contratos con proveedores externos de soporte y mantenimiento	Dirección Administrativa / Compras	3 semanas	5-6 semanas

Resultados esperados

- Reducción significativa en la ocurrencia de fallas de hardware
- Disponibilidad continua de servicios tecnológicos
- Mantenimiento documentado y ejecutado según cronograma
- Mejor capacidad de respuesta ante posibles incidentes técnicos relacionados con hardware

KPIs (Indicadores de Medición)

Indicador	Objetivo	Fórmula	Meta	Frecuencia
5.1 Mantenimiento preventivo cumplido	Implementar control A.7.9 (Mantenimiento de equipos)	% = (Equipos con mantenimiento al día ÷ Total equipos críticos) × 100	100%	Mensual
5.2 Prevención de fallas hardware	Medir efectividad mantenimiento preventivo	% = (Equipos sin fallas críticas en el último trimestre ÷ Total equipos críticos) × 100	≥95%	Trimestral

NOTA

- Para el riesgo CT-02.2 (Fallos hardware). Este es uno de los planes más largos debido a la acción 2 (sistema monitoreo), que es inversión significativa posiblemente sujeta a licitación. Crítico para mantener operativos sistemas como SCADA y servidores de facturación. La capacitación (acción 4) debe ser especializada, posiblemente con consultoría externa.

4.9.6 Prevención de accesos no autorizados por falta de autenticación segura

Descripción	
Amenaza	Acceso no autorizado a sistemas o información sensible
Vulnerabilidad	Falta de mecanismos robustos de autenticación segura (por ejemplo, contraseñas débiles, ausencia de autenticación multifactor)
Nivel de riesgo	Medio, con posibles impactos en la confidencialidad y la integridad de la información
Objetivo	Reducir el riesgo de accesos no autorizados mediante la implementación de controles técnicos y administrativos de autenticación segura
Política de respaldo	Política de Control de Accesos y Gestión de Identidades, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-02.3 - Acceso no autorizado por falta de autenticación segura - Tratamiento: REDUCIR (Riesgo: 12 - M - Moderado)

Controles ISO/IEC 27001:2022 aplicables

- A.5.15 - Seguridad de la autenticación
- A.8.2 - Gestión de identidades
- A.8.3 - Gestión de credenciales de autenticación
- A.5.17 - Gestión de acceso a información

Acciones específicas y responsables

N°	Acción	Responsable	Plazo	Plazo estimado EPAA-AA
1	Implementar autenticación multifactor (MFA) en sistemas críticos.	Área de Tecnología / Seguridad de la Información	16 semanas	20-24 semanas
2	Establecer políticas de complejidad de contraseñas y caducidad.	Seguridad de la Información / Talento Humano	6 semanas	9-12 semanas

3	Realizar auditoría de credenciales actuales y revocar accesos innecesarios.	Jefatura de Tecnología	6 semanas	9-12 semanas
4	Capacitar al personal sobre buenas prácticas de autenticación segura.	Talento Humano / Seguridad de la Información	6 semanas	9-12 semanas

Resultados esperados

- Disminución de la probabilidad de accesos no autorizados
- Fortalecimiento de los controles de acceso en la organización
- Reducción del riesgo asociado a credenciales comprometidas o débiles
- Mayor concienciación del personal sobre seguridad de acceso

KPIs (Indicadores de Medición)

Indicador	Objetivo	Fórmula	Meta	Frecuencia
6.1 Sistemas críticos con MFA	Implementar control A.8.5 (Autenticación segura)	% = (Sistemas críticos con MFA ÷ Total sistemas críticos) × 100	100% (mes 12)	Trimestral

NOTA

- Aborda el riesgo CT-02.3. La acción 1 (MFA) es técnicamente compleja y debe integrarse cuidadosamente con sistemas críticos existentes. Requiere evaluación de soluciones compatibles y posible inversión en licencias. La auditoría (acción 3) puede revelar necesidad de reestructurar completamente perfiles de acceso heredados. Priorizar MFA en sistemas con datos sensibles de usuarios.

4.9.7 Prevención de pérdida de documentos por almacenamiento inseguro

Descripción	
Amenaza	Pérdida de documentos físicos o digitales relevantes para la operación institucional

Vulnerabilidad	Almacenamiento inseguro de documentos, ya sea en espacios físicos sin control o en medios digitales sin respaldo ni control de acceso
Nivel de riesgo	Alto, debido al posible impacto en la continuidad operativa y en el cumplimiento normativo
Objetivo	Evitar la pérdida de documentos mediante controles adecuados de almacenamiento y respaldo
Política de respaldo	Política de Clasificación y Protección de la Información, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-03.1 - Pérdida de documentos por almacenamiento inseguro - Tratamiento: EVITAR (Riesgo: 16 - A - Alto)

Controles ISO/IEC 27001:2022 aplicables

- A.7.9 - Almacenamiento seguro de activos
- A.8.12 - Respaldo de información
- A.5.10 - Gestión de documentos de la organización
- A.5.15 - Seguridad de la autenticación

Acciones Específicas y Responsables

N°	Acción	Responsable	Plazo	Plazo estimado EPAA-AA
1	Implementar gabinetes con cerradura para archivo físico de documentos	Dirección Administrativa / Infraestructura	8 semanas	12-16 semanas
2	Configurar políticas de respaldo automático para los sistemas que almacenan documentos críticos	Área de Tecnología	16 semanas	20-24 semanas

3	Digitalizar documentos físicos importantes y almacenarlos en repositorios seguros	Archivo / Dirección Técnica	24 semanas	36-48 semanas
4	Establecer y difundir políticas de conservación y manejo de documentos institucionales	Gestión Documental / Legal	6 semanas	9-12 semanas

Resultados esperados

- Disminución del riesgo de pérdida de documentos físicos y digitales
- Mayor control y seguridad sobre el almacenamiento de la información institucional
- Cumplimiento de normativas internas y externas en la gestión documental
- Mejora en la eficiencia y disponibilidad de la información crítica para los procesos organizacionales

KPIs (Indicadores de Medición)

Indicador	Objetivo	Fórmula	Meta	Frecuencia
7.1 Documentos críticos respaldados	Implementar control A.8.13 (Protección de respaldo de información)	% = (Documentos críticos con respaldo ÷ Total documentos críticos) × 100	100%	Mensual
7.2 Documentos con almacenamiento seguro	Verificar clasificación y ubicación segura	% = (Documentos críticos almacenados en ubicaciones seguras verificadas ÷ Total documentos críticos) × 100	100%	Mensual

NOTA

- Para riesgo CT-03.1. La acción 3 (digitalización) es un proyecto masivo que probablemente requerirá contratación externa especializada. Representa la mayor inversión en tiempo y recursos de este plan. La acción 1 puede involucrar mobiliario especializado sujeto a procesos de compra. Priorizar digitalización de documentos legales, contractuales y operativos críticos.

4.9.8 Prevención de pérdida de documentos físicos por ausencia de controles

Descripción	
Amenaza	Acceso no autorizado
Vulnerabilidad	Ausencia de controles físicos
Nivel de riesgo	Muy Alto, ya que podría comprometer la continuidad operativa, la trazabilidad documental y el cumplimiento legal
Objetivo	Evitar la pérdida de documentos físicos mediante la implementación de medidas de seguridad física y organizacional
Política de respaldo	Política de Seguridad Física y del Entorno, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-03.2 - Acceso no autorizado a documentos por ausencia de controles físicos - Tratamiento: EVITAR (Riesgo: 25 - MA - Muy Alto)

Controles ISO/IEC 27001:2022 aplicables

- A.7.4 - Zonas seguras
- A.7.9 - Almacenamiento seguro de activos
- A.5.10 - Gestión de documentos de la organización
- A.5.15 - Seguridad de la autenticación

Acciones específicas y responsables

N°	**Acción**	**Responsable**	**Plazo**	**Plazo estimado EPAA-AA**

1	Instalar gabinetes de seguridad con cerradura para documentos clasificados	Infraestructura / Archivo	8 semanas	12-16 semanas
2	Establecer controles de acceso físico a las áreas de archivo documental	Dirección Administrativa / Seguridad	8 semanas	12-16 semanas
3	Implementar sistemas de monitoreo (cámaras) en zonas donde se almacenen documentos críticos	Tecnología / Infraestructura	16 semanas	24-32 semanas
4	Elaborar y divulgar políticas de gestión documental con énfasis en seguridad física	Asesoría Legal / Gestión Documental	6 semanas	9-12 semanas

Resultados esperados

- Mitigación del riesgo de pérdida de documentos físicos clave para la operación institucional
- Fortalecimiento de la infraestructura de seguridad física documental
- Establecimiento de normas claras sobre manejo y conservación de documentos
- Mejora de la trazabilidad y acceso controlado a la documentación crítica

KPIs (Indicadores de Medición)

Indicador	Objetivo	Fórmula	Meta	Frecuencia
8.1 Áreas críticas con control acceso	Implementar control A.7.3 (Protección de oficinas, salas e instalaciones)	% = (Áreas críticas con controles ÷ Total áreas críticas) × 100	100% (mes 6)	Mensual
8.2 Intrusiones	Medir efectividad controles acceso físico	# = Número de intrusiones detectadas	0	Mensual

físicas detectadas				
NOTA				
• Mitiga riesgo CT-03.2 (criticidad "Muy Alta"). Junto con el plan 2.8.10, representa la mayor inversión en infraestructura física. La acción 3 (videovigilancia) requiere diseño técnico, posible licitación, instalación y configuración. Priorizar áreas con documentos legales, registros de usuarios y datos financieros. La acción 4 debe alinearse con normativa de archivo y gestión documental pública.				

4.9.9 Reducción del riesgo de divulgación accidental de información

Descripción	
Amenaza	Divulgación accidental de información confidencial por parte del personal
Vulnerabilidad	Falta de políticas de confidencialidad claras y accesibles para todos los miembros de la organización
Nivel de riesgo	Bajo, pero con implicaciones significativas si afecta datos sensibles o estratégicos
Objetivo	Reducir el riesgo de divulgación accidental mediante el establecimiento de directrices claras de confidencialidad y capacitación continua
Política de respaldo	Política de Clasificación y Protección de la Información, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-03.3 - Divulgación accidental por falta de políticas de confidencialidad - Tratamiento: REDUCIR (Riesgo: 9 - B - Bajo)
Controles ISO/IEC 27001:2022 aplicables	

- A.5.12 - Políticas para la seguridad de la información
- A.6.1 - Responsabilidades de seguridad de la información
- A.6.3 - Concienciación, educación y formación en seguridad de la información
- A.5.10 - Gestión de documentos de la organización

Acciones específicas y responsables

N°	**Acción**	**Responsable**	**Plazo**	**Plazo estimado EPAA-AA**
1	Elaborar e implementar una política de confidencialidad institucional	Asesoría Legal / Dirección Administrativa	6 semanas	9-12 semanas
2	Difundir las políticas entre todos los colaboradores mediante comunicados internos y sesiones informativas	Talento Humano / Comunicaciones	3 semanas	5-6 semanas
3	Realizar capacitaciones semestrales sobre buenas prácticas de manejo de información	Talento Humano / Seguridad Informática	6 semanas	9-12 semanas
4	Incorporar cláusulas de confidencialidad en contratos laborales y acuerdos internos	Asesoría Legal	6 semanas	9-12 semanas

<table>
<tr><th colspan="5">Resultados Esperados</th></tr>
<tr><td colspan="5">• Mayor conocimiento y cumplimiento de las políticas de confidencialidad por parte del personal
• Reducción del riesgo de exposición accidental de datos
• Refuerzo de la cultura organizacional orientada a la protección de la información
• Implementación formal de políticas internas de confidencialidad en toda la institución</td></tr>
<tr><th colspan="5">KPIs (Indicadores de Medición)</th></tr>
<tr><th>Indicador</th><th>Objetivo</th><th>Fórmula</th><th>Meta</th><th>Frecuencia</th></tr>
<tr><td>9.1 Personal capacitado en confidencialidad</td><td>Implementar control A.6.3 (Concientización, educación y formación)</td><td>% = (Personal que ha completado capacitación en confidencialidad ÷ Total personal activo) × 100</td><td>80% (mes 6), 100% (mes 12)</td><td>Semestral</td></tr>
<tr><th colspan="5">NOTA</th></tr>
<tr><td colspan="5">• Para riesgo CT-03.3. Plan principalmente administrativo y de formación. La acción 4 requiere revisar y actualizar progresivamente todos los contratos vigentes, proceso que puede extenderse según cantidad. La capacitación (acción 3) debe ser continua, no puntual, e incluir ejemplos específicos del sector agua (datos de usuarios, información técnica de redes). La política (acción 1) debe definir claramente qué información es confidencial en EPAA-AA.</td></tr>
</table>

4.9.10 Prevención de intrusión física

Descripción	
Amenaza	Intrusión física a las instalaciones
Vulnerabilidad	Sistemas de vigilancia insuficientes en áreas críticas
Nivel de riesgo	Alto, debido al potencial acceso no autorizado a activos sensibles

Objetivo	Evitar la ocurrencia de intrusiones físicas mediante la implementación de controles físicos efectivos y medidas preventivas adecuadas
Política de respaldo	Política de Seguridad Física y del Entorno, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-04.1 - Intrusión física por sistemas de vigilancia insuficientes - Tratamiento: EVITAR (Riesgo: 20 - A - Alto)

Controles ISO/IEC 27001:2022 aplicables

- A.7.1 - Seguridad física y ambiental
- A.7.4 - Seguridad de las oficinas, salas y equipos
- A.7.7 - Protección contra amenazas físicas y del entorno
- A.7.8 - Trabajar en áreas seguras

Acciones específicas y responsables

N°	Acción	Responsable	Plazo	Plazo estimado EPAA-AA
1	Realizar un análisis de riesgo de las áreas críticas de la institución	Dirección Técnica / Seguridad Física	6 semanas	9-12 semanas
2	Diseñar e implementar un sistema de videovigilancia adecuado en las zonas vulnerables	Dirección Administrativa / Proveedores Externos	16 semanas	24-32 semanas
3	Establecer controles de acceso físico con tarjetas o biometría	Dirección Técnica / Sistemas	16 semanas	24-32 semanas
4	Capacitar al personal sobre protocolos de ingreso y seguridad física	Talento Humano / Seguridad	8 semanas	12-16 semanas

Resultados Esperados

- Reducción significativa de intentos de acceso físico no autorizado
- Mayor protección de los activos ubicados en áreas críticas
- Conciencia institucional reforzada sobre medidas de seguridad física
- Cumplimiento con los requisitos de seguridad física establecidos por la norma ISO/IEC 27001

KPIs (Indicadores de Medición)

Indicador	Objetivo	Fórmula	Meta	Frecuencia
10.1 Cobertura videovigilancia	Implementar control A.7.13 (Monitorización de la seguridad física)	% = (Áreas críticas con videovigilancia ÷ Total áreas críticas) × 100	100% (mes 12)	Trimestral
10.2 Puntos de acceso físico controlados	Implementar control A.7.3 (Protección de oficinas, salas e instalaciones)	% = (Puntos de acceso físico con controles validados ÷ Total puntos de acceso) × 100	100% (mes 9)	Trimestral

NOTA

- Aborda riesgo CT-04.1. La acción 1 debe priorizar: centro de control, sala de servidores, áreas con documentación crítica, estaciones de bombeo remotas. Las acciones 2 y 3 son inversiones significativas que requieren diseño especializado, posible licitación pública, instalación técnica y capacitación de usuarios. Implementar por fases, comenzando por las áreas más críticas identificadas en acción 1.

4.9.11 Prevención de Intercepción de Datos

Descripción	
Amenaza	Intercepción de datos durante su transmisión o almacenamiento
Vulnerabilidad	Cifrado inadecuado o ausente en la comunicación de datos sensibles
Nivel de riesgo	Alto, debido al posible acceso no autorizado a información crítica

Objetivo	Evitar la intercepción de datos mediante la implementación de mecanismos de cifrado robustos y buenas prácticas de seguridad
Política de respaldo	Política de Seguridad en Comunicaciones y Redes, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-05.1 - Intercepción de datos por cifrado inadecuado - Tratamiento: EVITAR (Riesgo: 15 - A - Alto)

Controles ISO/IEC 27001:2022 aplicables

- A.10.1 - Cifrado de la información
- A.13.1 - Protección de la información en tránsito
- A.13.2 - Protección de aplicaciones en red

Acciones específicas y responsables

N°	Acción	Responsable	Plazo	Plazo estimado EPAA-AA
1	Revisar los protocolos de cifrado actuales utilizados en la institución	Equipo de Seguridad Informática	3 semanas	5-6 semanas
2	Implementar cifrado de extremo a extremo en los canales de comunicación	Departamento de Sistemas / Proveedor de TI	7 semanas	10-12 semanas
3	Actualizar políticas internas de seguridad para el uso obligatorio de cifrado	Dirección Técnica / Seguridad Informática	6 semanas	9-12 semanas
4	Capacitar al personal sobre prácticas seguras	Talento Humano / Seguridad Informática	8 semanas	12-16 semanas

	de transmisión de información			
Resultados esperados				
• Reducción de riesgos de interceptación de datos por terceros • Mayor protección de la confidencialidad y privacidad de la información institucional • Cumplimiento con los estándares de cifrado exigidos por ISO/IEC 27001 • Personal capacitado y consciente de la importancia del cifrado de la información				
KPIs (Indicadores de medición)				
Indicador	**Objetivo**	**Fórmula**	**Meta**	**Frecuencia**
11.1 Comunicaciones críticas cifradas	Implementar control A.8.24 (Uso de criptografía)	% = (Comunicaciones críticas cifradas ÷ Total comunicaciones críticas) × 100	100% (mes 9)	Mensual
11.2 Incidentes de intercepción	Medir efectividad controles de cifrado	# = Número de incidentes reportados	0	Trimestral
NOTA				
• Para riesgo CT-05.1. Crítico para: 1) Comunicaciones con estaciones de bombeo remotas, 2) Transmisión datos sensibles de usuarios, 3) Acceso remoto administrativo. La acción 2 puede requerir actualización de sistemas o adquisición de herramientas de cifrado. Priorizar cifrado en comunicaciones SCADA y sistemas de facturación. La capacitación (acción 4) debe incluir personal técnico y administrativo que maneje datos sensibles.				

4.9.12 Reducción del acceso no autorizado a la red

Descripción	
Amenaza	Acceso no autorizado a la red institucional, lo que puede comprometer la confidencialidad, integridad y disponibilidad de la información
Vulnerabilidad	Configuraciones inseguras de red que permiten accesos sin las debidas restricciones

Nivel de riesgo	Medio, dado que, si bien el acceso no autorizado puede ser detectado, aún representa una amenaza relevante
Objetivo	Reducir el riesgo de accesos no autorizados mediante la implementación de controles técnicos y administrativos en la red
Política de respaldo	Política de Seguridad en Comunicaciones y Redes, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-05.3 - Acceso no autorizado a la red por configuraciones inseguras - Tratamiento: REDUCIR (Riesgo: 16 - M - Moderado)

Controles ISO/IEC 27001:2022 aplicables

- A.9.1.2 - Acceso a la red
- A.13.1.1 - Controles de red
- A.13.1.3 - Segmentación de redes
- A.14.1.2 - Seguridad de servicios en red

Acciones específicas y responsables

N°	Acción	Responsable	Plazo	Plazo estimado EPAA-AA
1	Auditar la red actual para identificar configuraciones inseguras	Equipo de Seguridad Informática	3 semanas	5-6 semanas
2	Actualizar la configuración de los dispositivos de red (routers, switches, firewalls)	Departamento de Sistemas	5 semanas	8-10 semanas
3	Aplicar segmentación de red para limitar el acceso a recursos sensibles	Equipo de Infraestructura	7 semanas	11-14 semanas

4	Implementar autenticación y registros de acceso a la red	Administrador de Red	7 semanas	11-14 semanas

Resultados esperados

- Configuración segura de dispositivos de red institucional
- Disminución significativa de accesos no autorizados a la red
- Implementación de políticas de acceso robustas
- Mejora en la protección de la información y los servicios institucionales

KPIs (Indicadores de Medición)

Indicador	Objetivo	Fórmula	Meta	Frecuencia
12.1 Segmentación de red implementada	Implementar control A.8.22 (Seguridad de redes)	% = (Redes críticas segmentadas ÷ Total redes críticas) × 100	100% (mes 12)	Trimestral
12.2 Accesos no autorizados detectados	Medir efectividad controles de red	# = Número de incidentes de acceso no autorizado	≤2 por mes	Mensual

NOTA

- Mitiga riesgo CT-05.3. La segmentación (acción 3) es técnicamente compleja, especialmente en redes existentes. Requiere planificación cuidadosa para no interrumpir servicios críticos. Recomendado: 1) Separar red administrativa de operacional (SCADA), 2) Aislar redes de invitados, 3) Segmentar por áreas funcionales. La acción 4 debe integrarse con directorio de usuarios existente. Ejecutar en etapas, con ventanas de mantenimiento programadas.

4.9.13 Transferir el fallo de los proveedores

Descripción

Amenaza	Fallo del proveedor que puede comprometer la continuidad de los servicios contratados
Vulnerabilidad	Dependencia crítica sin respaldo o plan alternativo para el servicio.
Nivel de riesgo	Bajo, debido a una baja probabilidad y a un impacto limitado, pero que requiere tratamiento
Objetivo	Transferir el riesgo al proveedor externo mediante cláusulas contractuales y acuerdos de nivel de servicio (SLA)
Política de respaldo	Política de Gestión de Proveedores y Servicios Externos, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-06.1 - Fallo del proveedor por dependencia crítica sin respaldo - Tratamiento: TRANSFERIR (Riesgo: 9 - B - Bajo)

Controles ISO/IEC 27001:2022 aplicables

- A.15.1.1 - Política de seguridad de la información para relaciones con proveedores
- A.15.2.1 - Supervisión y revisión de servicios de proveedores
- A.17.1.2 - Implementación de la continuidad de la información

Acciones específicas y responsables

N°	Acción	Responsable	Plazo	Plazo estimado EPAA-AA
1	Revisar contratos actuales para identificar cláusulas de respaldo y continuidad	Unidad Jurídica	3 semanas	5-6 semanas
2	Establecer acuerdos de nivel de servicio (SLA) con los proveedores clave	Dirección Administrativa Financiera	5 semanas	7-8 semanas
3	Evaluar alternativas de respaldo con otros proveedores	Unidad de Adquisiciones	6 semanas	9-12 semanas

4	Implementar supervisión periódica del cumplimiento de los SLA	Unidad Técnica	Continuo	Implementación: 8-12 semanas

Resultados esperados

- Reducción de la dependencia crítica mediante planes de respaldo
- Establecimiento de acuerdos de nivel de servicio claros con los proveedores
- Transferencia formal del riesgo mediante cláusulas contractuales
- Mejora en la gestión de continuidad operativa frente a fallas de proveedores

KPIs (Indicadores de Medición)

Indicador	Objetivo	Fórmula	Meta	Frecuencia
13.1 Proveedores críticos con SLA	Implementar control A.5.22 (Supervisión, revisión y evaluación de servicios del proveedor)	% = (Proveedores críticos con SLA ÷ Total proveedores críticos) × 100	100% (mes 9)	Trimestral

NOTA

- Para riesgo CT-06.1. Plan principalmente contractual-administrativo. Priorizar proveedores de: 1) Conectividad internet, 2) Hosting sistemas críticos, 3) Soporte SCADA, 4) Mantenimiento infraestructura. La acción 2 (SLA) requiere negociación caso por caso. La acción 3 es crucial para servicios sin alternativas actuales (ej: proveedor único). La supervisión (acción 4) necesita mecanismos formales de monitoreo y reporte.

4.9.14 Reducir el acceso a información sensible

Descripción	
Amenaza	Acceso a información sensible
Vulnerabilidad	Contratos con proveedores externos sin cláusulas de confidencialidad
Nivel de riesgo	Bajo

Objetivo	Garantizar la protección de la información sensible estableciendo cláusulas contractuales de confidencialidad con proveedores externos
Política de respaldo	Política de Gestión de Proveedores y Servicios Externos, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-06.2 - Acceso a información sensible por contratos sin cláusulas de confidencialidad - Tratamiento: REDUCIR (Riesgo: 6 - B - Bajo).

Controles ISO/IEC 27001:2022 aplicables

- A.13.2.4 - Acuerdos de confidencialidad
- A.15.1.1 - Políticas de seguridad de la información para relaciones con proveedores
- A.15.2.2 - Monitoreo y revisión de servicios de proveedores

Acciones específicas y responsables

N°	Acción	Responsable	Plazo	Plazo estimado EPAA-AA
1	Revisar todos los contratos vigentes con proveedores externos	Asesoría Legal	6 semanas	9-12 semanas
2	Incluir cláusulas de confidencialidad en los nuevos contratos o al renovar los existentes	Asesoría Legal / Dirección Administrativa Financiera	9 semanas	14-18 semanas
3	Capacitar al personal involucrado en la contratación sobre la importancia de la protección de información sensible	Unidad de Talento Humano / Seguridad de la Información	16 semanas	20-24 semanas

4	Monitorear periódicamente el cumplimiento de las cláusulas contractuales relacionadas con la seguridad de la información	Responsable del SGSI	Trimestral	Implementación: 8-12 semanas

Resultados esperados

- Todos los contratos con proveedores externos contarán con cláusulas de confidencialidad adecuadas
- Reducción del riesgo de acceso no autorizado a información sensible
- Mayor conciencia institucional sobre la importancia de la seguridad en relaciones contractuales

KPIs (Indicadores de Medición)

Indicador	Objetivo	Fórmula	Meta	Frecuencia
14.1 Contratos con cláusulas confidencialidad	Implementar control A.5.20 (Inclusión de la seguridad de la información en los acuerdos con proveedores)	% = (Contratos con cláusulas ÷ Total contratos vigentes) × 100	100% (mes 12)	Semestral

NOTA

- Aborda riesgo CT-06.2. La acción 1 puede ser extensa si existen muchos contratos vigentes. La acción 3 es fundamental para asegurar que nuevas contrataciones incluyan desde el inicio cláusulas adecuadas. Requiere coordinación estrecha con áreas de Talento Humano y Compras. Priorizar proveedores con acceso a: datos de usuarios, información financiera, planos técnicos de infraestructura, datos operativos SCADA.

4.9.15 Transferir la interrupción del servicio

Descripción	
Amenaza	Interrupción del servicio
Vulnerabilidad	Falta de acuerdos de nivel de servicio (SLA)
Nivel de riesgo	Bajo, por lo que el tratamiento recomendado es transferir el riesgo al proveedor externo mediante la formalización de compromisos contractuales
Objetivo	Garantizar la continuidad operativa y reducir la exposición ante fallas del servicio, estableciendo acuerdos claros que definan los tiempos de respuesta, niveles de disponibilidad y penalizaciones aplicables
Política de respaldo	Política de Gestión de Proveedores y Servicios Externos, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-06.3 - Interrupción del servicio por falta de acuerdos SLA - Tratamiento: TRANSFERIR (Riesgo: 6 - B - Bajo)

Controles ISO/IEC 27001:2022 aplicables

- A.15.1.1 - Políticas de seguridad de la información para relaciones con proveedores.
- A.15.2.1 - Supervisión y revisión de servicios del proveedor.
- A.17.1.1 - Planificación de la continuidad de la seguridad de la información.

Acciones específicas y responsables

N°	Acción	Responsable	Plazo	Plazo estimado EPAA-AA
1	Revisar los servicios contratados para identificar brechas contractuales	Dirección Administrativa	2 semana	3-4 semanas
2	Negociar y establecer acuerdos SLA con proveedores críticos	Gerencia General / Asesoría Legal	3 semanas	5-6 semanas

3	Documentar y firmar los SLA con cláusulas de disponibilidad y penalización	Asesoría Legal	3 semanas	5-6 semanas
4	Realizar seguimiento periódico al cumplimiento de los SLA establecidos	Responsable de TI	Mensual	Implementación: 4-6 semanas

Resultados esperados

- Disminución del impacto de la interrupción del servicio sobre los procesos críticos
- Formalización de acuerdos SLA con proveedores estratégicos
- Mejora de la supervisión de los servicios prestados por terceros
- Reducción del riesgo residual al transferir parte de la responsabilidad al proveedor

KPIs (Indicadores de Medición)

Indicador	Objetivo	Fórmula	Meta	Frecuencia
15.1 Proveedores con acuerdos de disponibilidad	Implementar control A.5.22 (Supervisión de proveedores)	% = (Proveedores críticos con SLA disponibilidad ÷ Total proveedores críticos) × 100	100% (mes 9)	Trimestral

NOTA

- Para riesgo CT-06.3. Plan focalizado en proveedores de servicios tecnológicos críticos. Priorizar: 1) Proveedor conectividad internet (afecta todos los sistemas), 2) Hosting de sistemas en línea, 3) Soporte especializado SCADA, 4) Proveedores de software crítico. La acción 2 requiere negociación específica por proveedor. La acción 4 necesita proceso formal de monitoreo con métricas claras (uptime, tiempo respuesta).

4.9.16 Evitar la pérdida de integridad de los datos

Descripción	
Amenaza	Pérdida de integridad de los datos
Vulnerabilidad	Errores en la gestión de la base de datos
Nivel de riesgo	Alto, debido a la posibilidad de generarse errores en el almacenamiento de información
Objetivo	Garantizar la integridad y confiabilidad de los datos institucionales mediante controles preventivos y correctivos
Política de respaldo	Política de Continuidad del Servicio y Respaldo de la Información, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-07.1 - Pérdida de integridad de datos por errores en gestión de bases de datos - Tratamiento: EVITAR (Riesgo: 16 - A - Alto)

Controles ISO/IEC 27001:2022 aplicables

- A.12.1.2 - Controles contra software malicioso
- A.14.2.4 - Protección de datos de prueba
- A.14.1.2 - Validación de entradas de datos
- A.9.4.1 - Restricciones en el acceso a la información
- A.12.4.1 - Registro y monitoreo de eventos

Acciones específicas y responsables

N°	Acción	Responsable	Plazo	Plazo estimado EPAA-AA
1	Implementar procedimientos de respaldo y restauración de bases de datos	Administrador de bases de datos	11 semanas	15-18 semanas
2	Capacitar al personal en buenas prácticas de gestión de datos	Unidad de Talento Humano	12 semanas	18-24 semanas

3	Establecer políticas de validación de datos al ingreso de información	Responsable de Desarrollo de Sistemas	9 semanas	14-18 semanas
4	Auditar registros y configuraciones de bases de datos periódicamente	Unidad de Seguridad de la Información	12 semanas	18-24 semanas

Resultados esperados

- Garantizar la integridad de los datos almacenados en las bases de datos institucionales
- Minimizar el riesgo de errores en la gestión de datos mediante la implementación de políticas y procedimientos claros
- Establecer controles técnicos que aseguren la integridad de la información
- Contar con personal capacitado en la gestión de bases de datos
- Reducir la probabilidad de pérdida de integridad por fallas humanas o técnicas

KPIs (Indicadores de Medición)

Indicador	Objetivo	Fórmula	Meta	Frecuencia
16.1 Backups de bases de datos críticas	Implementar control A.8.13 (Protección de respaldo)	% = (Backups exitosos ÷ Total backups programados) × 100	100%	Diaria
16.2 Integridad de transacciones críticas	Medir protección de integridad de datos	% = (Transacciones críticas con integridad verificada ÷ Total transacciones críticas) × 100	100%	Mensual

NOTA

- Mitiga riesgo CT-07.1. Crítico para sistemas: facturación, contabilidad, SCADA, gestión documental. La acción 1 debe incluir no solo configuración técnica, sino también pruebas periódicas de restauración (ej: trimestrales). La auditoría (acción 4) debe verificar: controles de acceso, integridad referencial, procedimientos de respaldo, logs de transacciones. Priorizar bases de datos con información financiera y operacional crítica.

4.9.17 Reducir la interrupción de los servicios

Descripción	
Amenaza	Interrupción del servicio
Vulnerabilidad	Falta de redundancia o backup
Nivel de riesgo	Media, debido a la posibilidad que los servicios se vena interrumpidos
Objetivo	Establecer mecanismos de respaldo y redundancia que aseguren la continuidad del servicio ante posibles interrupciones
Política de respaldo	Política de Continuidad del Servicio y Respaldo de la Información, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-07.2 - Interrupción del servicio por falta de redundancia o backup - Tratamiento: REDUCIR (Riesgo: 12 - M - Moderado)

Controles ISO/IEC 27001:2022 aplicables

- A.12.3.1 - Copias de seguridad de la información
- A.17.1.1 - Planificación de la continuidad de la seguridad de la información
- A.17.2.1 - Disponibilidad de servicios de TI

Acciones específicas y responsables

N°	Acción	Responsable	Plazo	Plazo estimado EPAA-AA
1	Diseñar e implementar un sistema de backup regular y automático	Área de Sistemas	11 semanas	15-18 semanas
2	Establecer redundancia en servicios críticos (servidores, redes)	Área Técnica	16 semanas	20-24 semanas
3	Realizar pruebas periódicas de restauración de backups	Área de Sistemas	Mensual	Implementación: 8-12 semanas
4	Documentar procedimientos de respaldo y recuperación	Responsable de Seguridad de la Información	6 semanas	9-12 semanas

5	Capacitar al personal sobre políticas de respaldo y recuperación	RRHH y Seguridad de la Información	16 semanas	20-24 semanas

Resultados esperados

- Reducción del riesgo de pérdida de servicio ante fallos técnicos o humanos
- Mejora de la disponibilidad de los sistemas críticos
- Establecimiento de procedimientos claros de respaldo y recuperación
- Capacitación efectiva del personal en medidas de contingencia
- Fortalecimiento de la continuidad operativa de la organización

KPIs (Indicadores de Medición)

Indicador	Objetivo	Fórmula	Meta	Frecuencia
17.1 Sistemas críticos con redundancia	Implementar control A.8.14 (Disponibilidad de los recursos de procesamiento de la información)	% = (Sistemas críticos con redundancia ÷ Total sistemas críticos) × 100	100% (mes 12)	Trimestral
17.2 Tiempo de recuperación de servicios críticos	Medir eficiencia continuidad operativa	Horas = Tiempo entre fallo y restauración completa del servicio (SCADA, Facturación, Contabilidad)	≤1 hora para sistemas TI; ≤4 horas para SCADA	Por evento

NOTA

- Para riesgo CT-07.2. Fundamental para continuidad operativa. La redundancia (acción 2) puede requerir inversión significativa en hardware adicional. Priorizar: servidores de facturación, sistemas SCADA, conectividad a estaciones remotas. Las pruebas de restauración (acción 3) deben programarse regularmente y documentarse. La

capacitación (acción 5) debe incluir personal técnico y usuarios clave de cada sistema crítico.

4.9.18 Reducir los accesos no autorizados

Descripción	
Amenaza	Acceso no autorizado
Vulnerabilidad	Gestión inadecuada de usuarios y roles
Nivel de riesgo	Bajo, debido a que puede generar una gestión inadecuada de usuarios y roles
Objetivo	Reducir los acceso no autorizados
Política de respaldo	Política de Control de Accesos y Gestión de Identidades, definida en la sección 4.8 del Marco Normativo Interno del SGSI
Correspondencia con análisis de riesgos:	CT-07.3 - Acceso no autorizado por gestión inadecuada de usuarios y roles - Tratamiento: REDUCIR (Riesgo: 9 - B - Bajo)

Controles ISO/IEC 27001:2022 aplicables

- A.9.1.2 Acceso de usuarios
- A.9.2.1 Registro de usuarios
- A.9.2.2 Gestión de privilegios
- A.9.4.1 Restricción del acceso a la información

Acciones específicas y responsables

N°	**Acción**	**Responsable**	**Plazo**	**Plazo estimado EPAA-AA**
1	Realizar un inventario actualizado de todos los usuarios y sus roles asignados	Administrador de Sistemas	6 semanas	9-12 semanas
2	Definir y documentar políticas de control de accesos basadas en roles	Responsable de Seguridad de la Información	6 semanas	4-6 semanas

3	Implementar revisiones periódicas de cuentas de usuario y privilegios	Auditor Interno	Trimestral	Implementación: 8-12 semanas
4	Capacitar al personal en prácticas seguras de gestión de accesos	Talento Humano	4 semanas	6-8 semanas
5	Configurar alertas para accesos no autorizados o inusuales	Administrador de Seguridad TI	7 semanas	11-14 semanas

Resultados esperados

- Control efectivo de accesos basado en roles claramente definidos
- Reducción del riesgo de accesos indebidos o privilegios excesivos
- Personal concienciado sobre la importancia del manejo seguro de credenciales
- Mejora en la trazabilidad de actividades realizadas por los usuarios
- Cumplimiento con los requisitos de seguridad de la norma ISO/IEC 27001

KPIs (Indicadores de Medición)

Indicador	Objetivo	Fórmula	Meta	Frecuencia
18.1 Revisiones de privilegios de acceso ejecutadas	Implementar control A.8.2 (Gestión de privilegios de acceso)	% = (Cuentas con revisión de privilegios en el último trimestre ÷ Total cuentas con acceso a sistemas críticos) × 100	100% (trimestral)	Trimestral
18.2 Alertas de acceso no autorizado atendidas	Medir efectividad de controles de acceso	% = (Alertas de acceso no autorizado investigadas en ≤30 minutos ÷ Total alertas generadas) × 100	≥95%	Mensual

NOTA
• Aborda riesgo CT-07.3. Completa el ciclo de gestión de identidades iniciado en planes 4.8.2 y 4.8.6. La acción 1 puede revelar cuentas obsoletas o privilegios excesivos heredados. Las revisiones periódicas (acción 3) deben institucionalizarse como proceso formal, posiblemente vinculado a evaluaciones de desempeño o cambios de rol. Las alertas (acción 5) ayudan a detección temprana de accesos sospechosos. Priorizar sistemas con datos sensibles.

4.10 Cronograma propuesto de implementación - diagrama de Gantt

El cronograma establece la planificación temporal para la ejecución de las 80 actividades derivadas de los 18 planes de acción definidos en la sección 4.9. La propuesta contempla un horizonte de 24 semanas en base a un calendario mientras organiza las actividades en una secuencia lógica determinada por dependencias técnicas, priorización según criticidad del riesgo, así como viabilidad operativa en el contexto de la EPAA-AA. La representación gráfica completa junto con el detalle técnico de actividades, duraciones y dependencias se presenta en el anexo 4.

4.10.1 Criterios de estructuración del cronograma

El cronograma fue elaborado con base en los siguientes criterios.

- **Duración total**: 24 semanas consecutivas, desde el inicio de actividades de preparación y definición normativa hasta la etapa de verificación y cierre
- **Identificación de actividades**: cada actividad cuenta con un código alfanumérico (por ejemplo, *1.1*, *10.1*), donde el primer número corresponde al plan de acción de origen y el segundo identifica la actividad dentro de dicho plan
- **Secuenciación por ejecución práctica**: en el Diagrama de Gantt (Anexo 5), las actividades se agrupan y ordenan según su lógica de implementación, priorizando acciones habilitantes (por ejemplo, definición de políticas, inventarios y análisis previos) antes de controles técnicos que dependen de ellas
- **Priorización por criticidad**: se prioriza la atención de riesgos clasificados como Muy Altos (MA) y Altos (A), conforme a los criterios establecidos en la matriz de calor

- **Consideraciones de recursos**: la calendarización incorpora la disponibilidad esperable de equipos técnicos y administrativos, evitando concentrar actividades altamente dependientes del mismo responsable en un mismo periodo cuando ello pudiera comprometer la continuidad operativa

El Anexo 5 utiliza una convención de colores para facilitar la lectura del cronograma según el nivel de criticidad del riesgo: rojo (MA), naranja (A), amarillo (M) y verde (B/MB).

4.10.2 Fases de ejecución propuestas

Para facilitar la gestión, monitoreo y comprensión del avance, las 24 semanas se organizan en tres fases consecutivas que agrupan actividades con objetivos afines, como se detalla en la ***Tabla 20***.

Tabla 20 Fases de Ejecución Propuestas

Fase	Rango semanal	Objetivo principal	Actividades representativas	Fundamento de la agrupación
Fase 1 Establecimiento de Bases Organizativas	Semanas 1-8	Definir lineamientos, levantar información base e iniciar acciones habilitantes	1.1, 4.1, 8.1, 10.1	Establece condiciones mínimas para controles técnicos posteriores
Fase 2 Implementación de Controles Prioritarios	Semanas 9-16	Implementar controles técnicos/organizativos de mayor impacto	2.4, 7.2, 12.2, 16.1	Materializa tratamientos de riesgos con mayor criticidad
Fase 3 Consolidación y Verificación	Semanas 17-24	Capacitación, cierre de implementaciones y verificación	6.1, 10.2, 16.4, 18.3	Refuerza sostenibilidad y valida funcionamiento de controles

4.10.3 Puntos críticos de coordinación

El cronograma identifica periodos que demandan mayor coordinación interáreas debido a la concurrencia de actividades y a la sensibilidad de los activos involucrados. En particular:

1. **Inicio de actividades sensibles:** (por ejemplo, digitalización documental y auditorías técnicas), que requieren coordinación previa con las áreas propietarias de la información y definición de ventanas de trabajo.

2. **Periodo de mayor concentración operativa:** (fase intermedia), donde coinciden actividades técnicas que pueden requerir ventanas de mantenimiento y acceso a sistemas críticos, por lo que se recomienda calendarización coordinada y control de cambios.
3. **Transición hacia capacitación y verificación**: implica gestionar agendas del personal sin afectar la continuidad del servicio.

4.10.4 Actividades de larga duración (camino crítico)

Las siguientes actividades presentan la mayor duración individual dentro del cronograma. La finalización determina la duración mínima total de 24 semanas, que corresponde al "camino crítico" del plan. Cualquier tipo de retraso en cualquiera de ellas retrasaría proporcionalmente la finalización de todo el cronograma, como se detalla en la ***Tabla 21***.

Tabla 21: Actividades de Larga Duración

ID	Descripción	Duración	Rango	Nivel de riesgo	Complejidad y justificación de la duración
7.3	Digitalización documentos críticos	15 semanas	10-24	MA (CT-03.2)	Alto volumen documental y necesidad de clasificación y validación
5.2	Monitoreo hardware servidores/SCADA	11 semanas	14-24	A (CT-02.2)	Evaluación, adquisición, instalación, configuración y puesta en marcha
10.2	Videovigilancia áreas críticas	10 semanas	15-24	MA (CT-04.1)	Diseño, instalación multiubicación y configuración de monitoreo
6.1	MFA sistemas SCADA/facturación	10 semanas	15-24	A (CT-02.3)	Integración con sistemas existentes y despliegue gradual con pruebas

4.10.5 Supuestos de cronograma propuesto

La ejecución de la planificación propuesta considera los siguientes supuestos:

1. Disponibilidad del personal asignado, con autorización para dedicar tiempo a actividades del SGSI sin comprometer funciones operativas esenciales.
2. Respeto de dependencias técnicas, evitando iniciar actividades cuya ejecución requiere entregables previos (por ejemplo, políticas y lineamientos antes de controles técnicos).

3. Agilidad razonable en aprobaciones y adquisiciones, dentro de plazos compatibles con la calendarización propuesta, especialmente en actividades que requieren contratación o compra.
4. Estabilidad operativa, asumiendo que no ocurran contingencias mayores que obliguen a suspender actividades por periodos prolongados.

4.10.6 Relación con el anexo técnico

Para la comprensión integral del cronograma se debe consultar el Anexo 5, que contiene lo siguiente.

- Listado completo de las 80 actividades con responsables sugeridos y duración
- Representación visual del Gantt con solapamientos, secuencia y periodos de mayor concentración
- Mapa de dependencias entre actividades
- Identificación del camino crítico

4.11 Revisión y mantenimiento

La sostenibilidad del SGSI a lo largo del tiempo no depende únicamente de su implementación inicial al contrario depende de un proceso cíclico y sistemático de mejora continua, el cual se alinea con el modelo Planificar-Hacer-Verificar-Actuar (PHVA) establecido por la norma ISO/IEC 27001:2022, que garantiza que el SGSI se adapte de forma dinámica a los cambios en el contexto organizacional, el panorama de amenazas, en conjunto con los requisitos de la empresa.

La Figura 13 ilustra cómo las actividades de revisión con mantenimiento propuestas cierran el ciclo del SGSI, alimentando la fase de "Verificar" y "Actuar" para generar nuevos insumos en la "Planificación" de cada ciclo.

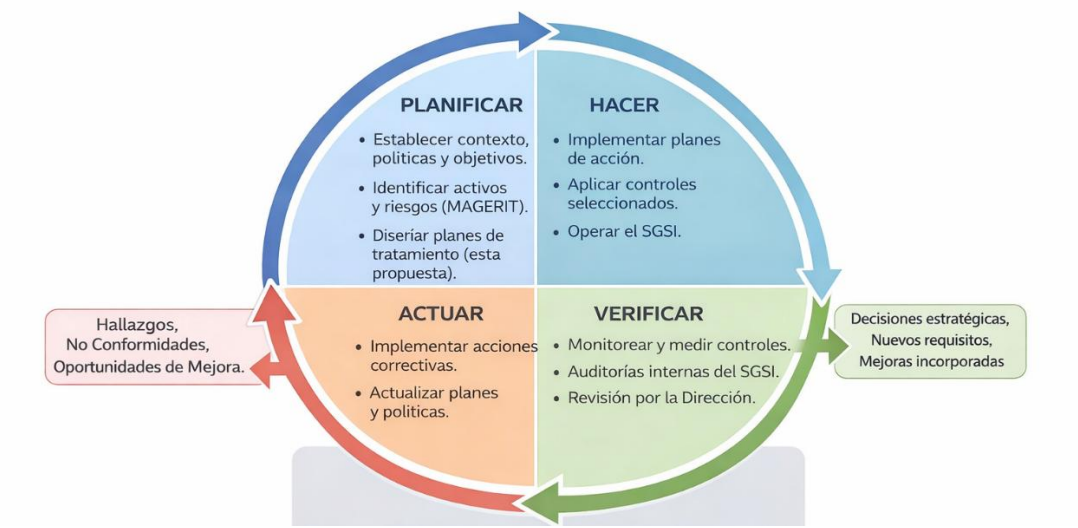

Figura 13: *Integración de la Revisión y Mantenimiento (PHVA).*

4.11.1 Actividades claves de rendimiento y mantenimiento

A continuación, se describen las actividades propuestas para evaluar el desempeño del SGSI y mantenerlo vigente en la EPAA-AA, de acuerdo con los lineamientos de ISO/IEC 27001. Estas actividades se ejecutarán con una frecuencia mínima y también de forma extraordinaria cuando existan cambios relevantes (por ejemplo: cambios tecnológicos, incidentes, nuevos procesos o requisitos normativos):

- **Revisión periódica de la Política de Seguridad de la Información:** se revisará al menos una vez al año o cuando ocurran cambios significativos en el entorno organizacional, tecnológico o normativo, para asegurar su vigencia y aplicabilidad

- **Evaluación y actualización de riesgos:** se mantendrá un proceso cíclico de identificación, análisis, evaluación y tratamiento de riesgos. Como mínimo, se revisará anual y adicionalmente cuando surjan nuevos activos, amenazas, vulnerabilidades o cambios relevantes en procesos institucionales

- **Actualización del inventario de activos:** el inventario se actualizará semestralmente, verificando estado, criticidad, responsables (propietarios) y relación con procesos

institucionales, con el fin de mantener el control sobre los activos de información y la infraestructura crítica

- **Auditorías internas del SGSI:** se planificarán auditorías internas al menos una vez al año para verificar el grado de conformidad del SGSI con ISO/IEC 27001. Sus resultados permitirán identificar no conformidades, observaciones y oportunidades de mejora

- **Monitoreo y verificación de controles:** se aplicará un plan de monitoreo para evaluar la eficacia de los controles técnicos, físicos y administrativos definidos en la propuesta. Este seguimiento permitirá detectar debilidades y priorizar acciones de mejora

- **Revisión por la Dirección:** la Dirección revisará periódicamente el desempeño del SGSI considerando, como mínimo: resultados de auditorías, incidentes de seguridad relevantes, cumplimiento de objetivos, estado del tratamiento de riesgos y necesidades de recurso

- **Actualización del Plan de Tratamiento de Riesgos:** el plan se revisará semestralmente (o cuando existan cambios críticos) incorporando hallazgos de auditorías, incidentes, nuevas brechas o riesgos identificados, asegurando que los controles necesarios se mantengan priorizados y actualizados

- **Capacitación y concienciación continua:** se desarrollarán acciones periódicas de capacitación para el personal sobre buenas prácticas de seguridad, gestión de incidentes, uso adecuado de la información y cumplimiento de políticas internas, reforzando el componente humano del SGSI

4.11.2 Mecanismos para el cierre del ciclo del PHVA

El Para que estas actividades se conviertan en **mejora real** y no queden solo como documentación, se establecen mecanismos formales que aseguran el cierre del ciclo PHVA:

- **Documentación de decisiones y resultados:** las conclusiones de auditorías, revisiones y revisiones por la Dirección se registrarán mediante actas e informes, dejando evidencia de lo analizado y de lo decidido

- **Asignación de responsables y plazos:** cada acción correctiva o de mejora identificada se asignará a un responsable y a un plazo definido, asegurando trazabilidad y control de avance.
- **Seguimiento sistemático:** el Responsable del SGSI (o el Comité de Seguridad de la Información) realizará seguimiento al cumplimiento de acciones, integrándolas al Plan de Tratamiento de Riesgos y a la planificación del SGS
- **Verificación de efectividad:** una vez ejecutadas las acciones, se verificará si resolvieron la causa de la no conformidad o mejoraron el control, dejando constancia del resultado y cerrando formalmente el ciclo

La revisión junto con el mantenimiento actúan como el componente que mantiene actualizado el SGSI, permitiendo que la EPAA-AA fortalezca de forma sostenida la protección de su información crítica frente a un entorno cambiante.

4.12 Validación de la propuesta

Para validar la propuesta del Sistema de Gestión de la Seguridad de la Información (SGSI) desarrollada para la Empresa Pública de Agua Potable y Alcantarillado de Antonio Ante (EPAA-AA), se definió un enfoque de evaluación acorde con la naturaleza y el alcance de la investigación. El trabajo representa una propuesta técnica de diseño más no contempla la implementación ni la operación del sistema, por lo tanto la validación no se orienta a la medición de resultados empíricos u operativos, sino a la evaluación de la solidez conceptual del planteamiento desarrollado.

Se aplicó una validación teórica del diseño, entendida como un método de análisis que permite la verificación de la coherencia interna, integridad, completitud, en conjunto con la alineación normativa de una propuesta antes de su ejecución. La validación de este tipo es coherente con los objetivos del estudio, cuyo propósito es diseñar un SGSI alineado a la norma ISO/IEC 27001:2022, sustentado en un diagnóstico institucional como también en un análisis sistemático de riesgos sin evaluar su desempeño operativo en un entorno real.

Con la validación teórica se comprueba si la estructura propuesta responde de manera lógica y sistemática a las brechas, riesgos, o necesidades identificadas durante las fases previas de

diagnóstico junto con análisis, proporcionando evidencia de que el diseño del SGSI es conceptualmente viable como hoja de ruta para una futura implementación en la EPAA-AA.

4.12.1 Metodología de validación teórica

La validación teórica de la propuesta se realizó mediante una lista de verificación estructurada, cuyo objetivo fue contrastar los resultados del diagnóstico inicial con las soluciones planteadas en el diseño del SGSI. En particular, se analizaron los 67 controles del Anexo A de la norma ISO/IEC 27001:2022 identificados como no implementados durante el diagnóstico institucional, comparándolos con las acciones definidas en los 18 planes de acción desarrollados en la propuesta.

Para cada control no implementado, se evaluó la existencia de correspondencia con al menos una acción propuesta, aplicando criterios de cobertura conceptual, los cuales permitieron valorar la coherencia del diseño sin necesidad de una ejecución práctica. Los criterios utilizados fueron los siguientes:

1. **Relevancia temática:** la acción propuesta debe abordar de manera directa el objetivo del control de seguridad establecido en la norma ISO/IEC 27001:2022.
2. **Viabilidad contextual:** las medidas planteadas deben ser técnicamente aplicables y organizativamente posibles dentro del contexto institucional, operativo y normativo de la EPAA-AA.
3. **Capacidad teórica de mitigación:** el conjunto de acciones asociadas a cada control debe demostrar, desde una perspectiva conceptual, la capacidad de reducir o tratar los riesgos identificados en el análisis realizado.

Con estos criterios se verifica que la propuesta no se limita a una cobertura formal de controles, sino que plantea respuestas coherentes y contextualizadas frente a las brechas de seguridad detectadas.

4.12.2 Resultados de la validación de diseño

Los resultados de la validación teórica se presentan de forma resumida en la TABLA 22, la cual muestra la correspondencia entre los controles no implementados identificados en el diagnóstico y los controles cubiertos conceptualmente por los planes de acción propuestos.

En la tabla se observa que los 18 planes de acción desarrollados cubren conceptualmente el 100% de los 67 controles no implementados del Anexo A de la norma ISO/IEC 27001:2022, esto indica que desde la perspectiva del diseño, la propuesta del SGSI proporciona una respuesta estructurada y a la vez planificada para cada brecha de seguridad identificada en la EPAA-AA.

El porcentaje de cobertura observado no implica la efectividad operativa de los controles ni su grado de madurez, solo evidencia que el diseño del SGSI es integral y exhaustivo, para lo que establece que una base completa al ser ejecutada en el futuro permitiría a la organización avanzar de manera ordenada hacia la implementación de los requisitos de la norma de referencia.

TABLA 22
Resultados de la lista de verificación

Sección	Subsección	Controles no implementados (Diagnóstico)	Controles cubiertos por la propuesta	%Cobertura
A.5 Controles Organizativos	Clasificación y manejo de la información	3	3	100%
A.5 Controles Organizativos	Control de acceso organizativo	2	2	100%
A.5 Controles Organizativos	Cumplimiento y requisitos legales	4	4	100%
A.5 Controles Organizativos	Gestión de activos	3	3	100%
A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5	5	100%
A.5 Controles Organizativos	Políticas, organización y relaciones	5	5	100%
A.5 Controles Organizativos	Relaciones con proveedores	5	5	100%
A.5 Controles Organizativos	Revisiones y operaciones organizativas	3	3	100%

Sección	Subsección	Controles no implementados (Diagnóstico)	Controles cubiertos por la propuesta	%Cobertura
A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	5	5	100%
A.7 Controles Físicos	Controles Físicos	9	9	100%
A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	10	10	100%
A.8 Controles Tecnológicos	Disponibilidad y registros	2	2	100%
A.8 Controles Tecnológicos	Gestión de la capacidad, vulnerabilidades y configuración	4	4	100%
A.8 Controles Tecnológicos	Protección de datos	4	4	100%
A.8 Controles Tecnológicos	Seguridad de dispositivos y acceso	2	2	100%
A.8 Controles Tecnológicos	Uso seguro de herramientas y software	1	1	100%
Total		**67**	**67**	**100%**

Este resultado confirma que la propuesta cumple con el requisito fundamental de integralidad en su alcance, al contemplar de manera sistemática todos los controles necesarios para cerrar las brechas de seguridad identificadas durante el diagnóstico institucional.

4.12.3 Alcance y limitaciones de la validación realizada

Con el fin de evitar interpretaciones erróneas sobre los resultados obtenidos, es necesario precisar el alcance y las limitaciones de la validación teórica realizada:

- **Si valida**

  La validación confirma la integridad, coherencia y completitud del diseño del SGSI propuesto, verificando que todas las brechas y necesidades de seguridad identificadas cuentan con acciones planificadas y alineadas a la norma ISO/IEC 27001:2022.

- **No valida**

  Esta validación no evalúa la eficacia operativa de los controles, no garantiza el éxito de una futura implementación, ni sustituye las evaluaciones prácticas que deberán realizarse durante una eventual ejecución del SGSI. Aspectos como la disponibilidad de recursos, la aceptación por parte del personal, la correcta configuración técnica de los controles y la gestión del cambio organizacional exceden el alcance de este análisis y deberán ser considerados en fases posteriores.

La validación teórica demuestra que la propuesta de SGSI desarrollada para la EPAA-AA es conceptualmente coherente, completa, así como también alineada con los requisitos de la norma ISO/IEC 27001:2022, constituyéndose en un documento base sólido bien fundamentado que puede servir como punto de partida para la planificación estratégica de la seguridad de la información en la organización.

4.13 Consideraciones para la planificación presupuestaria futura

La eventual implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) requiere una adecuada planificación de recursos humanos, tecnológicos y financieros. No obstante, dado que el presente trabajo constituye una propuesta técnica de diseño y no contempla la ejecución del sistema, esta sección no incluye presupuestos detallados ni cotizaciones formales.

La finalidad de este apartado es la proporción de un marco referencial que permita a la EPAA-AA la identificación de manera preliminar de los principales componentes de costo que deberían considerarse en caso de decidir avanzar con la implementación del SGSI, apoyando de esta manera la toma de decisiones estratégicas a nivel institucional.

4.13.1 Componentes generales de costo a considerar

De forma referencial, y en concordancia con la estructura del SGSI propuesto y los requisitos de la norma ISO/IEC 27001, se identifican los siguientes componentes generales de costo que podrían ser considerados en una futura planificación presupuestaria.

1. **Recursos humanos internos:** dedicación parcial del personal de la empresa para participar en actividades de gestión del SGSI, tales como comités de seguridad, revisión de políticas, ejecución de auditorías internas y procesos de capacitación.
2. **Desarrollo y mantenimiento de documentación:** elaboración, actualización y gestión de políticas, procedimientos, registros y planes requeridos por el SGSI.
3. **Capacitación y concienciación:** programas de formación orientados a fortalecer la cultura de seguridad de la información y el cumplimiento de las políticas internas por parte del personal.
4. **Controles tecnológicos:** posibles inversiones asociadas a la incorporación o fortalecimiento de herramientas de seguridad de la información, tales como mecanismos de protección, respaldo, control de accesos y monitoreo.
5. **Infraestructura física:** adecuaciones relacionadas con controles de acceso físico, protección de áreas críticas y condiciones ambientales para la infraestructura tecnológica.
6. **Asesoría especializada:** eventual contratación de apoyo externo para actividades específicas, como acompañamiento técnico, auditorías internas o asesoría en etapas iniciales de implementación.
7. **Certificación (opcional):** en caso de que la EPAA-AA decida, en una etapa posterior, optar por una certificación formal en ISO/IEC 27001, se deberán considerar los costos asociados a auditorías externas de certificación.

4.13.2 Metodología sugerida para estimación presupuestaria

En el momento en que la EPAA-AA defina el alcance junto con la decisión institucional de implementar el SGSI, se sugiere la implementación de una metodología de estimación presupuestaria que considere como mínimo los siguientes lineamientos.

1. Realizar estudios detallados de costos mediante procesos formales de cotización con proveedores calificados
2. Priorizar la implementación por fases, enfocándose inicialmente en los controles asociados a los riesgos de criticidad “Muy Alta” identificados en esta propuesta
3. Diferenciar los costos de inversión inicial de los costos recurrentes de operación, mantenimiento y mejora continua del SGSI
4. Alinear los procesos de adquisición y contratación con lo establecido en la Ley Orgánica del Sistema Nacional de Contratación Pública y demás normativa aplicable al sector público

4.13.3 Planificación gradual

La estructura de los 18 planes de acción definidos en la propuesta del SGSI permite una implementación gradual y progresiva en el tiempo, lo que facilitaría la distribución de los costos en distintos ejercicios presupuestarios. Desde una perspectiva estratégica, se sugiere iniciar con los componentes de carácter organizativo, tales como la formalización de políticas, procedimientos y actividades de capacitación, los cuales presentan menores requerimientos de inversión financiera directa y generan una base sólida para etapas posteriores.

Los costos específicos asociados a cada fase deberán determinarse mediante procesos formales de análisis junto con cotización, una vez que se defina con precisión el alcance de la implementación. La sección por lo tanto cumple exclusivamente una función tanto orientativa como estratégica, sin constituir un compromiso presupuestario ni un plan de ejecución.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

A nivel general, se desarrolló una propuesta sólida y contextualizada de un Sistema de Gestión de la Seguridad de la Información para la Empresa Pública de Agua Potable y Alcantarillado de Antonio Ante, alineada con los requisitos de la norma ISO/IEC 27001, la cual permite establecer mecanismos de protección, control y mejora continua en el tratamiento de los activos de información institucionales, aportando a la reducción de riesgos, al cumplimiento normativo y a la sostenibilidad operativa de la organización.

Con respecto al primer objetivo específico se construyó un marco teórico integral sobre los fundamentos de la seguridad de la información junto con los principios de la norma ISO/IEC 27001, considerando tanto su evolución, estructura, controles del Anexo A, así como metodologías complementarias como MAGERIT, OCTAVE y NIST RM, que permitieron contextualizar la importancia de implementar un SGSI en instituciones públicas.

Se verificó de forma exhaustiva el nivel de adopción de los 93 controles establecidos en el Anexo A de la norma ISO/IEC 27001, esto permitió la identificación de aquellos que se encuentran implementados, documentados o revisados periódicamente dentro de la EPAA-AA, a partir de eso se determinó el nivel real de madurez en seguridad de la información de la institución, así como la línea base desde la cual se planteó el diseño del SGSI.

Se diseñó una propuesta estructurada del SGSI a través de un plan de acción detallado basado en los riesgos más relevantes que contempla también acciones de seguimiento, auditoría, junto a mejora continua, asegurando su alineación con los principios de gobernanza institucional, lo que garantiza tanto su viabilidad como la sostenibilidad en el contexto organizacional de la EPAA-AA.

Recomendaciones

- Socializar y capacitar al personal de la EPAA-AA sobre las políticas, procedimientos y buenas prácticas de seguridad de la información, con el fin de fortalecer la cultura organizacional y minimizar errores humanos.
- Designar formalmente un Comité de Seguridad de la Información, encargado de coordinar, supervisar y dar seguimiento a las actividades relacionadas con la implementación y mantenimiento del SGSI.
- Establecer un cronograma de auditorías internas junto con revisiones periódicas del SGSI, para que de esta manera se garantice su mejora continua conforme al Ciclo PHVA (Planificar, Hacer, Verificar, Actuar), y exista adaptación a nuevas amenazas o cambios organizacionales.
- Integrar cláusulas de seguridad de la información en los contratos con proveedores externos, para que exista completa seguridad del cumplimiento de requisitos de confidencialidad, disponibilidad y protección de datos ante eventuales incidentes.
- Implementar recursos tecnológicos y humanos adecuados para la gestión del SGSI, que incluyan herramientas de monitoreo, sistemas de respaldo, plataformas de cifrado y personal especializado en seguridad informática.
- Revisar el inventario de activos de información junto con su clasificación, valoración y protección, para mantenerlo alineado con los cambios operativos, tecnológicos y legales de la organización.

Referencias

[1] M. M. .. Minaya, R. W. .. Minaya, M. L. .. Intriago y J. A. Intriago, «Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática,» *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS,* vol. 5, nº 4, pp. 584-599, 2023.

[2] ESET, «Security report latinoamérica 2023,» 2023. [En línea]. Available: [Online]. Available: https://web-assets.esetstatic.com/wls/es/articulos/reportes/eset-security-report-latam2023.pdf. [Último acceso: 27 Mayo 2024].

[3] Naciones Unidas, «La Agenda 2030 y los Objetivos de Desarrollo Sostenible: una oportunidad para América Latina y el Caribe,» 2023. [En línea]. Available: [Online]. Available: https://repositorio.cepal.org/server/api/core/bitstreams/cb30a4de-7d87-4e79-8e7a-ad5279038718/content. [Último acceso: 24 Abril 2024].

[4] Secretaría Nacional de Planificación, «Plan de Creación de Oportunidades 2021-2025,» 2021. [En línea]. Available: [Online]. Available: https://www.planificacion.gob.ec/wp-content/uploads/2021/09/Plan-de-Creacio%CC%81n-de-Oportunidades-2021-2025-Aprobado.pdf. [Último acceso: 24 Abril 2024].

[5] W. Apaza, «Propuesta de un plan de seguridad de la información para incrementar la fiabilidad de datos en una financiera,» *Innovación y Software,* vol. 2, nº 2, pp. 27-43, 2021.

[6] G. De La Cruz, A. Méndez y R. Méndez, «Seguridad de la información en el comercio electrónico basado en ISO 27001 : Una revisión sistemática,» *Innovación y Software,* vol. 4, nº 1, pp. 219-236, 2023.

[7] R. D. Estrada, J. L. Unás y O. Flórez, «Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá,» *Revista Logos Ciencia & Tecnología,* vol. 13, nº 3, pp. 98-110, 2021.

[8] J. Rueda, N. Gallego, E. Estanlings, J. Tello y V. García, «Identificación de variables relacionadas a la seguridad informática a partir de tendencias investigativas de la tecnología blockchain,» *Revista Politécnica,* vol. 20, nº 40, pp. 9-29, 2024.

[9] O. Bustillos y J. Rojas, «Cómo promueven los estados la ciberseguridad de las pymes,» *Interfases,* nº 17, pp. 21-37, 2023.

[10] R. G. Ramos Mamami, R. R. Llanqui Argollo y R. Cahuaya Ancco, «Política informática y la gestión de la seguridad de la información en base a la norma ISO 27001,» *Innovación y Software,* vol. 4, nº 1, pp. 96-106, 2023.

[11] ISO Tools, «ISO 27001: Origen y evolución,» 2025. [En línea]. Available: https://pe.isotools.us/iso-27001-origen-y-evolucion/.

[12] Secuframe, «Una breve historia de ISO 27001,» 2025. [En línea]. Available: https://secureframe.com/es-es/hub/iso-27001/history.

[13] S. Bustamante, M. Valles, I. Cuellar y D. Lévano, «Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú,» *Enfoque UTE,* vol. 12, nº 2, pp. 69-79, 2021.

[14] M. Barrueto y O. Marchena, «Impacto de los costos estratégicos en la sostenibilidad empresarial de las PYMEs mediante una revisión bibliográfica,» *Revista científica En Ciencias Sociales,* pp. 1-11, 2024.

[15] D. Donoso, C. Calahorrano y S. Donoso, «Aplicación del SGSI ISO 27001 en el sistema de rehabilitación social de Ecuador,» *Revista Universidad y Sociedad,* vol. 15, nº 2, pp. 274-284, 2023.

[16] J. A. Panaqué, Y. G. Lizárraga y A. Mendoza De los Santos, «Efectos de la implementación de un SGSI basado en la norma ISO 27001 para las organizaciones,» *Perfiles De Ingeniería,* vol. 18, nº 18, pp. 67-74, 2022.

[17] J. Salazar, N. Mora, W. Romero y J. Ollague, «Diagnóstico de la aplicación del ciclo PHVA según la ISO 27001,» *Universidad Tecnica de Machala,* 2023.

[18] L. Fonseca, «Propuesta de un Sistema de Gestión de Seguridad y Salud en el Trabajo basado en la Norma INTE/ISO 45001:2018, para la planta de producción de la Corporación Manza Té de C.A.S.A,» 2022. [En línea]. Available: https://repositorio.una.ac.cr/items/35d2e135-6252-4032-9464-1e7c9c4006ef.

[19] K. Franco y L. Zambrano, «Análisis documental para la creación de un equipo de respuestas a incidentes informáticos orientado a pequeñas y medianas empresas del sector económico colombiano,» 2020. [En línea]. Available: https://repository.unad.edu.co/handle/10596/42683.

[20] J. Miranda, «Mapeo sistemático de metodologías de Seguridad de la Información para el control de la gestión de riesgos informáticos,» 2021. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/20966/4/UPS-GT003401.pdf.

[21] J. Llanos, F. Lópe y M. Mejía, «Implementación de un sistema de seguridad de la información en empresa del sector salud,» *SUMMA,* vol. 5, pp. 1-14, 2023.

[22] M. Diaz, «Repositorio institucional de la Universidad Nacional de Ingeniería,» 2021. [En línea]. Available: https://ribuni.uni.edu.ni/3951/1/95597.pdf.

[23] T. Flores y R. Wherrems, «Auditoria de seguridad de la información utilizando ISO/IEC 27001 en una compañía del sector bancario,» 2023. [En línea]. Available: https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/670787/Flores_CT.pdf?sequence=1&isAllowed=y.

[24] A. Pacheco, L. Suarez y J. González, «Aplicar la Metodología OCTAVE de Identificación de Amenazas y Vulnerabilidades en una Entidad Bancaria.,» *Universidad de los Andes,* pp. 1-13, 2022.

[25] E. Linares, L. Balverdi y I. Cuellar, «Políticas de seguridad de la información y metodología Magerit en la empresa Induamerica Chiclayo S.A.C,» *Pakamuros,* vol. 10, nº 2, 2023.

[26] J. Pinguil, «Propuesta para la gestión de continuidad del negocio en el ámbito de TI para EMMAIPC-EP del cantón Cañar,» 2024. [En línea]. Available: https://dspace.ucacue.edu.ec/items/f2d263a1-c588-497a-af61-6f9cc2ee211a.

[27] IBM, «Enterprise IT security,» IBM, 2024. [En línea]. Available: https://www.ibm.com/trust/security.

[28] Microsoft, «Microsoft Copilot for Security obtiene las certificaciones ISO 27001,,» Microsoft, 2024. [En línea]. Available: https://techcommunity.microsoft.com/blog/securitycopilotblog/microsoft-copilot-for-security-attains-iso-27001-27017-and-27018-certifications/4161758?utm_source=chatgpt.com.

[29] Telefónica, «Seguridad,» Telefónica, 2023. [En línea]. Available: https://www.telefonica.com/es/centro-global-de-transparencia/seguridad.

[30] Google, «ISO 27001 Certification,» Google, 2023. [En línea]. Available: https://support.google.com/analytics/answer/3407084.

[31] EPAA-AA, «Empresa Pública de Agua Potable y Alcantarillado EPAA-AA,» EPAA-AA, 2025. [En línea]. Available: https://epaa.gob.ec/wp55/.

[32] EAPAA-AA, «Empresa Pública de Agua Potable y Alcantarillado,» EAPAA-AA, 2025. [En línea]. Available: https://epaa.gob.ec/wp55/?page_id=2.

[33] C. Benites, «Implementación de un Sistema de Gestión de Seguridad de la Información-Norma ISO 27001 para la Fábrica Radiadores Fortaleza,» 2019. [En línea]. Available: [Online]. Available: https://hdl.handle.net/20.500.12867/1933. [Último acceso: 27 Abril 2024].

ANEXOS

Anexo 1: Anexo A de la Norma ISO/IEC 27001:2022

Sección	Subsección	Control
A.5 Controles Organizativos	Políticas, organización y relaciones	5.1 Políticas para la seguridad de la información
A.5 Controles Organizativos	Políticas, organización y relaciones	5.2 Roles y responsabilidades en seguridad de la información
A.5 Controles Organizativos	Políticas, organización y relaciones	5.3 Segregación de funciones
A.5 Controles Organizativos	Políticas, organización y relaciones	5.4 Responsabilidades de la dirección
A.5 Controles Organizativos	Políticas, organización y relaciones	5.5 Contacto con las autoridades
A.5 Controles Organizativos	Políticas, organización y relaciones	5.6 Contacto con grupos de interés especiales
A.5 Controles Organizativos	Políticas, organización y relaciones	5.7 Inteligencia sobre amenazas
A.5 Controles Organizativos	Políticas, organización y relaciones	5.8 Seguridad de la información en la gestión de proyectos
A.5 Controles Organizativos	Gestión de activos	5.9 Inventario de la información y otros activos asociados
A.5 Controles Organizativos	Gestión de activos	5.10 Uso aceptable de la información y otros activos asociados
A.5 Controles Organizativos	Gestión de activos	5.11 Devolución de activos
A.5 Controles Organizativos	Clasificación y manejo de la información	5.12 Clasificación de la información
A.5 Controles Organizativos	Clasificación y manejo de la información	5.13 Etiquetado de la información
A.5 Controles Organizativos	Clasificación y manejo de la información	5.14 Transferencia de la información

Sección	Subsección	Control
A.5 Controles Organizativos	Control de acceso organizativo	5.15 Control de acceso
A.5 Controles Organizativos	Control de acceso organizativo	5.16 Gestión de la identidad
A.5 Controles Organizativos	Control de acceso organizativo	5.17 Información de autenticación
A.5 Controles Organizativos	Control de acceso organizativo	5.18 Derechos de acceso
A.5 Controles Organizativos	Relaciones con proveedores	5.19 Seguridad de la información en las relaciones con proveedores
A.5 Controles Organizativos	Relaciones con proveedores	5.20 Inclusión de la seguridad de la información en los acuerdos con proveedores
A.5 Controles Organizativos	Relaciones con proveedores	5.21 Gestión de la seguridad de la información en la cadena de suministro de TIC
A.5 Controles Organizativos	Relaciones con proveedores	5.22 Supervisión, revisión y evaluación de servicios del proveedor
A.5 Controles Organizativos	Relaciones con proveedores	5.23 Seguridad de la información para el uso de servicios en la nube
A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.24 Notificación de eventos de seguridad de la información
A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.25 Evaluación y decisión sobre eventos de seguridad de la información
A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.26 Respuesta a incidentes de seguridad de la información
A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.27 Lecciones aprendidas de incidentes de seguridad de la información
A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.28 Recopilación de evidencia
A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.29 Planificación de la continuidad del negocio
A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.30 Preparación de las TIC para la continuidad del negocio

Sección	Subsección	Control
A.5 Controles Organizativos	Cumplimiento y requisitos legales	5.31 Cumplimiento de requisitos legales, reglamentarios y contractuales
A.5 Controles Organizativos	Cumplimiento y requisitos legales	5.32 Derechos de propiedad intelectual
A.5 Controles Organizativos	Cumplimiento y requisitos legales	5.33 Protección de registros
A.5 Controles Organizativos	Cumplimiento y requisitos legales	5.34 Privacidad y protección de información de identificación personal (PII)
A.5 Controles Organizativos	Revisiones y operaciones organizativas	5.35 Revisión independiente de la seguridad de la información
A.5 Controles Organizativos	Revisiones y operaciones organizativas	5.36 Procedimientos operativos documentados
A.5 Controles Organizativos	Revisiones y operaciones organizativas	5.37 Gestión de cambios
A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.1 Verificación de antecedentes (Screening)
A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.2 Términos y condiciones de empleo
A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.3 Concientización, educación y formación en seguridad de la información
A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.4 Proceso disciplinario
A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.5 Responsabilidades tras la terminación o cambio de empleo
A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.6 Acuerdos de confidencialidad o no divulgación
A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.7 Trabajo remoto

Sección	Subsección	Control
A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.8 Capacitación en desarrollo seguro
A.7 Controles Físicos	Controles Físicos	7.1 Perímetro de seguridad física
A.7 Controles Físicos	Controles Físicos	7.2 Control de entrada física
A.7 Controles Físicos	Controles Físicos	7.3 Protección de oficinas, salas e instalaciones
A.7 Controles Físicos	Controles Físicos	7.4 Protección contra amenazas físicas
A.7 Controles Físicos	Controles Físicos	7.5 Trabajo en áreas seguras
A.7 Controles Físicos	Controles Físicos	7.6 Áreas de entrega y carga
A.7 Controles Físicos	Controles Físicos	7.7 Ubicación y protección de equipos
A.7 Controles Físicos	Controles Físicos	7.8 Seguridad del cableado
A.7 Controles Físicos	Controles Físicos	7.9 Mantenimiento
A.7 Controles Físicos	Controles Físicos	7.10 Eliminación o reutilización segura de equipos
A.7 Controles Físicos	Controles Físicos	7.11 Retirada de activos
A.7 Controles Físicos	Controles Físicos	7.12 Escritorio limpio y pantalla limpia
A.7 Controles Físicos	Controles Físicos	7.13 Monitorización de la seguridad física
A.7 Controles Físicos	Controles Físicos	7.14 Protección contra amenazas externas y ambientales
A.8 Controles Tecnológicos	Seguridad de dispositivos y acceso	8.1 Dispositivos de punto final del usuario
A.8 Controles Tecnológicos	Seguridad de dispositivos y acceso	8.2 Derechos de acceso privilegiado

Sección	Subsección	Control
A.8 Controles Tecnológicos	Seguridad de dispositivos y acceso	8.3 Restricción de acceso a la información
A.8 Controles Tecnológicos	Seguridad de dispositivos y acceso	8.4 Acceso al código fuente
A.8 Controles Tecnológicos	Seguridad de dispositivos y acceso	8.5 Autenticación segura
A.8 Controles Tecnológicos	Gestión de la capacidad, vulnerabilidades y configuración	8.6 Gestión de la capacidad
A.8 Controles Tecnológicos	Gestión de la capacidad, vulnerabilidades y configuración	8.7 Protección contra malware
A.8 Controles Tecnológicos	Gestión de la capacidad, vulnerabilidades y configuración	8.8 Gestión de vulnerabilidades técnicas
A.8 Controles Tecnológicos	Gestión de la capacidad, vulnerabilidades y configuración	8.9 Gestión de la configuración
A.8 Controles Tecnológicos	Protección de datos	8.10 Eliminación de la información
A.8 Controles Tecnológicos	Protección de datos	8.11 Enmascaramiento de datos
A.8 Controles Tecnológicos	Protección de datos	8.12 Prevención de fuga de datos
A.8 Controles Tecnológicos	Protección de datos	8.13 Copia de seguridad de la información
A.8 Controles Tecnológicos	Disponibilidad y registros	8.14 Redundancia de las instalaciones de procesamiento de la información
A.8 Controles Tecnológicos	Disponibilidad y registros	8.15 Registro (logging)
A.8 Controles Tecnológicos	Disponibilidad y registros	8.16 Monitorización de actividades
A.8 Controles Tecnológicos	Disponibilidad y registros	8.17 Sincronización del reloj
A.8 Controles Tecnológicos	Uso seguro de herramientas y software	8.18 Uso de programas utilitarios con privilegios

Sección	Subsección	Control
A.8 Controles Tecnológicos	Uso seguro de herramientas y software	8.19 Instalación de software en sistemas operativos en producción
A.8 Controles Tecnológicos	Seguridad de la red y servicios asociados	8.20 Seguridad de la red
A.8 Controles Tecnológicos	Seguridad de la red y servicios asociados	8.21 Seguridad de los servicios de red
A.8 Controles Tecnológicos	Seguridad de la red y servicios asociados	8.22 Segmentación de redes
A.8 Controles Tecnológicos	Seguridad de la red y servicios asociados	8.23 Filtrado web
A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.24 Uso de criptografía
A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.25 Ciclo de vida de desarrollo seguro
A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.26 Requisitos de seguridad de las aplicaciones
A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.27 Principios de ingeniería de sistemas seguros
A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.28 Entorno de desarrollo seguro
A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.29 Codificación segura
A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.30 Desarrollo externalizado
A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.31 Pruebas seguras
A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.32 Gestión de la seguridad de la información en entornos de prueba
A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.33 Seguridad de la información en procesos de desarrollo y soporte
A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.34 Revisión de la seguridad de la información tras cambios en el entorno operativo

Anexo 2: Validación del instrumento para el levantamiento del diagnóstico

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN SOFTWARE

VALIDACIÓN DE INSTRUMENTO PARA EL DIAGNÓSTICO DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO/IEC 27001 EN LA EPAA-AA

Proyecto:	Propuesta de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la Empresa Pública de Agua Potable y Alcantarillado de Antonio Ante (EPAA-AA) en base a la normativa ISO/IEC 27001.
Autor:	Jonathan Segovia
Objetivo:	Evaluar el nivel de implementación de los controles de seguridad de la información en la EPAA-AA, como parte del diagnóstico requerido por el segundo objetivo específico de la tesis.

Fecha de envió para la evaluación del experto:	20/05/2025
Fecha de revisión del experto:	20/05/2025

En la siguiente matriz marque con una X el criterio de evaluación según corresponda en cada ítem. De ser necesario realice la observación en el apartado correspondiente.

INSTRUMENTO DE EVALUACIÓN CUALITATIVO			
ÍTEMS	**CIRTERIOS DE EVALUACIÓN**		
	MUCHO	**POCO**	**NADA**
Instrucción breve, clara y completa.	X		
Formulación clara de cada pregunta.	X		
Comprensión de cada pregunta.	X		
Coherencia de las preguntas en relación con el objetivo.	X		
Relevancia del contenido.	X		
Orden y secuencia de las preguntas.	X		
Número de preguntas óptimo.		X	

Observaciones:

En el encabezado del cuestionario se menciona que se busca evaluar el nivel de implementación de los controles de seguridad de la información basados en la norma ISO/IEC 27001:2022; no obstante, es propicio verificar que todas las preguntas estén correctamente enfocadas a este propósito. A continuación, algunas observaciones puntuales:

- ¿El objetivo del cuestionario es únicamente evaluar el cumplimiento técnico de los controles, o también se busca detectar problemas o debilidades en su aplicación práctica?
- El número de preguntas es bastante extenso para una sola aplicación del instrumento de investigación, esto podría generar fatiga y afectar la calidad de las respuestas. Sería factible elaborar una matriz de operacionalización de variables y consolidar por bloques las dimensiones e indicadores.
- Posiblemente sería útil considerar un modelo de madurez complementario (por ejemplo, un enfoque basado en niveles como el ciclo PHVA o COBIT) para reforzar la lógica de la escala utilizada.

A continuación, marque con una X en el criterio de evaluación según el análisis de cada pregunta que conforma el cuestionario, las cuales se encuentran representadas en el siguiente instrumento de evaluación como ítem. De ser necesario realice la observación en el casillero correspondiente.

INSTRUMENTO DE EVALUACIÓN CUANTITATIVO				
CRITERIOS DE EVALUACIÓN				**OBSERVACIONES**
Ítem	**Dejar**	**Modificar**	**Eliminar**	
1	X			
2	X			
3	X			
4	X			
5	X			
6	X			
7		X		Eliminar la palabra "fuente", se repite 2 veces.
8	X			
9	X			
10	X			
11	X			
12		X		El verbo debe ser en singular "incluya".
13	X			
14	X			
15	X			
16	X			
17	X			
18	X			
19	X			
20	X			

21		X		Quitar la palabra "todos", se vuelve redundante el enunciado.
22	X			
23		X		Corregir la palabra "evaló", lo correcto sería "evaluó".
24	X			
25		X		Corregir la palabra "eprmita", lo correcto sería "permita".
26		X		La palabra debe ser en plural "aprobados".
27	X			
28		X		La palabra debe ser en singular "procedimiento".
29	X			
30		X		Reemplazar la palabra "para" por "de".
31	X			
32	X			
33	X			
34		X		Aclarar término técnico en la pregunta.
35	X			
36	X			
37	X			
38	X			
39	X			
40	X			
41	X			
42	X			
43	X			
44	X			
45	X			
46	X			
47	X			
48	X			
49	X			
50	X			
51	X			
52	X			
53	X			
54	X			
55	X			
56	X			
57	X			

58	X			
59	X			
60	X			
61	X			
62	X			
63	X			
64	X			
65		X		El verbo debe ser en singular "monitorea".
66	X			
67		X		Mejor sería redactarla así: ¿Existen informes sobre los resultados de los escaneos de vulnerabilidades del año 2024?
68	X			
69	X			
70	X			
71	X			
72	X			
73	X			
74	X			
75	X			
76	X			
77	X			
78	X			
79	X			
80	X			
81	X			
82	X			
83	X			
84	X			
85		X		Mejor sería redactarla así: ¿Se establecen requisitos de seguridad desde la fase de diseño hasta la de aplicación?
86		X		Se repite la misma pregunta 85. La pregunta debería ser formulada así: ¿Se aplican principios de seguridad en el diseño, desarrollo y mantenimiento de los sistemas?
87	X			
88	X			
89	X			
90	X			

91	X			
92	X			
93	X			

_____

Firma del evaluador

Apellidos y nombres completos	Paredes Andrade Diana Carolina
Título académico	*Ingeniera Comercial *Estudiante de posgrado MBA en Administración de Empresas
Institución de Educación Superior	*Universidad Técnica del Norte *Universidad Andina Simón Bolívar
Correo electrónico	dianacparedes97@gmail.com
Teléfono	0981238104

Anexo 3: Diagnóstico de la situación actual

#	Sección	Subsección	Control	Pregunta	Cumplido	Criterio
1	A.5 Controles Organizativos	Políticas, organización y relaciones	5.1 Políticas para la seguridad de la información	¿Existe una política de seguridad de la información formalmente aprobada?	SI	2. Implementado sin evidencia formal
2	A.5 Controles Organizativos	Políticas, organización y relaciones	5.2 Roles y responsabilidades en seguridad de la información	¿Se han documentado claramente los roles y responsabilidades de seguridad?	SI	2. Implementado sin evidencia formal
3	A.5 Controles Organizativos	Políticas, organización y relaciones	5.3 Segregación de funciones	¿Se han identificado y separado las funciones críticas para evitar conflictos de interés?	NO	1. No implementado
4	A.5 Controles Organizativos	Políticas, organización y relaciones	5.4 Responsabilidades de la dirección	¿La alta dirección demuestra compromiso con la seguridad de la información?	NO	1. No implementado
5	A.5 Controles Organizativos	Políticas, organización y relaciones	5.5 Contacto con las autoridades	¿Hay un canal establecido para contactar a las autoridades de TI en caso de incidentes?	SI	2. Implementado sin evidencia formal
6	A.5 Controles Organizativos	Políticas, organización y relaciones	5.6 Contacto con grupos de interés especiales	¿La organización participa en foros o grupos de seguridad especializados?	NO	1. No implementado
7	A.5 Controles Organizativos	Políticas, organización y relaciones	5.7 Inteligencia sobre amenazas	¿La organización mantiene suscripciones con fuente de inteligencia sobre nuevas amenazas?	NO	1. No implementado
8	A.5 Controles Organizativos	Políticas, organización y relaciones	5.8 Seguridad de la información en la gestión de proyectos	¿Se evalúan riesgos de seguridad antes de la implementación del proyecto?	NO	1. No implementado

#	Sección	Subsección	Control	Pregunta	Cumplido	Criterio
9	A.5 Controles Organizativos	Gestión de activos	5.9 Inventario de la información y otros activos asociados	¿Existe un inventario documentado y actualizado de los activos de información?	NO	1. No implementado
10	A.5 Controles Organizativos	Gestión de activos	5.10 Uso aceptable de la información y otros activos asociados	¿Se han definido políticas claras de uso aceptable de activos?	NO	1. No implementado
11	A.5 Controles Organizativos	Gestión de activos	5.11 Devolución de activos	¿Se verifica la devolución de activos (dispositivos, credenciales) al término de contratos o empleos?	NO	1. No implementado
12	A.5 Controles Organizativos	Clasificación y manejo de la información	5.12 Clasificación de la información	¿Existe una política aprobada que incluya los criterios para clasificar la información?	NO	1. No implementado
13	A.5 Controles Organizativos	Clasificación y manejo de la información	5.13 Etiquetado de la información	¿La información lleva etiquetas que indiquen su nivel de clasificación?	NO	1. No implementado
14	A.5 Controles Organizativos	Clasificación y manejo de la información	5.14 Transferencia de la información	¿Existen procedimientos aprobados que garanticen la seguridad para la transferencia de información?	NO	1. No implementado
15	A.5 Controles Organizativos	Control de acceso organizativo	5.15 Control de acceso	¿Se aplican controles de acceso basados en rol?	SI	3. Implementado y documentado
16	A.5 Controles Organizativos	Control de acceso organizativo	5.16 Gestión de la identidad	¿Se cuenta con un proceso aprobado que regule el alta, modificación y baja de identidades?	NO	1. No implementado
17	A.5 Controles Organizativos	Control de acceso organizativo	5.17 Información de autenticación	¿Se almacenan contraseñas cifradas y protegidas?	NO	1. No implementado

#	Sección	Subsección	Control	Pregunta	Cumplido	Criterio
18	A.5 Controles Organizativos	Control de acceso organizativo	5.18 Derechos de acceso	¿Se asignan privilegios mínimos necesarios para las tareas del usuario?	SI	2. Implementado sin evidencia formal
19	A.5 Controles Organizativos	Relaciones con proveedores	5.19 Seguridad de la información en las relaciones con proveedores	¿Se evalúa la seguridad de la información antes de contratar proveedores?	NO	1. No implementado
20	A.5 Controles Organizativos	Relaciones con proveedores	5.20 Inclusión de la seguridad de la información en los acuerdos con proveedores	¿Se incorporan cláusulas de seguridad de la información en los contratos con proveedores?	NO	1. No implementado
21	A.5 Controles Organizativos	Relaciones con proveedores	5.21 Gestión de la seguridad de la información en la cadena de suministro de TIC	¿En el año 2024 se evaluó la seguridad de toda la cadena de suministros de los dispositivos del parque informático?	NO	1. No implementado
22	A.5 Controles Organizativos	Relaciones con proveedores	5.22 Supervisión, revisión y evaluación de servicios del proveedor	¿Se llevan a cabo auditorías o revisiones periódicas a los proveedores en materia de seguridad?	NO	1. No implementado
23	A.5 Controles Organizativos	Relaciones con proveedores	5.23 Seguridad de la información para el uso de servicios en la nube	¿En el año 2024 se evaluó los riesgos asociados al uso de la nube?	NO	1. No implementado
24	A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.24 Notificación de eventos de seguridad de la información	¿Existe un canal definido para notificar eventos de seguridad?	SI	2. Implementado sin evidencia formal

#	Sección	Subsección	Control	Pregunta	Cumplido	Criterio
25	A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.25 Evaluación y decisión sobre eventos de seguridad de la información	¿Existen informes de evaluación sistemática de los eventos que permita clasificarlos como incidentes?	NO	1. No implementado
26	A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.26 Respuesta a incidentes de seguridad de la información	¿Existen protocolos aprobados que permita dar respuesta a los incidentes presentados?	SI	2. Implementado sin evidencia formal
27	A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.27 Lecciones aprendidas de incidentes de seguridad de la información	¿Existen informes que contengan información post-incidente para extraer lecciones aprendidas?	NO	1. No implementado
28	A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.28 Recopilación de evidencia	¿Existenten protocolos aprobados que regule el procedimiento para la recolección forense de datos?	NO	1. No implementado
29	A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.29 Planificación de la continuidad del negocio	¿Existen protocolos aprobados para la continuidad de los servicios?	NO	1. No implementado
30	A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.30 Preparación de las TIC para la continuidad del negocio	¿Existen protocolos de respaldo y recuperación para sistemas críticos?	NO	1. No implementado
31	A.5 Controles Organizativos	Cumplimiento y requisitos legales	5.31 Cumplimiento de requisitos legales, reglamentarios y contractuales	¿Se mantiene un registro de las normativas aplicables?	NO	1. No implementado

#	Sección	Subsección	Control	Pregunta	Cumplido	Criterio
32	A.5 Controles Organizativos	Cumplimiento y requisitos legales	5.32 Derechos de propiedad intelectual	¿Todos los computadores tienen software original?	NO	1. No implementado
33	A.5 Controles Organizativos	Cumplimiento y requisitos legales	5.33 Protección de registros	¿Se aplican controles para asegurar la integridad y disponibilidad de los registros?	NO	1. No implementado
34	A.5 Controles Organizativos	Cumplimiento y requisitos legales	5.34 Privacidad y protección de información de identificación personal (PII)	¿Se protege la PII mediante cifrado, acceso limitado y controles adicionales?	NO	1. No implementado
35	A.5 Controles Organizativos	Revisiones y operaciones organizativas	5.35 Revisión independiente de la seguridad de la información	¿Se llevan a cabo auditorías externas de seguridad de la información?	NO	1. No implementado
36	A.5 Controles Organizativos	Revisiones y operaciones organizativas	5.36 Procedimientos operativos documentados	¿Están los procedimientos de seguridad operativa claramente documentados?	NO	1. No implementado
37	A.5 Controles Organizativos	Revisiones y operaciones organizativas	5.37 Gestión de cambios	¿Existen protocolos aprobados que regulen el proceso para solicitar, evaluar y aprobar cambios en los sistemas de información?	NO	1. No implementado
38	A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.1 Verificación de antecedentes (Screening)	¿Se realizan verificaciones previas a la contratación según el nivel del puesto?	SI	2. Implementado sin evidencia formal

#	Sección	Subsección	Control	Pregunta	Cumplido	Criterio
39	A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.2 Términos y condiciones de empleo	¿Los contratos de empleo incluyen cláusulas de confidencialidad y seguridad?	SI	3. Implementado y documentado
40	A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.3 Concientización, educación y formación en seguridad de la información	¿Existen programas regulares de capacitación en seguridad de la información?	NO	1. No implementado
41	A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.4 Proceso disciplinario	¿Existen protocolos disciplinarios aprobados para abordar violaciones de seguridad?	NO	1. No implementado
42	A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.5 Responsabilidades tras la terminación o cambio de empleo	¿Se revocan accesos y devuelven activos tras la renuncia o despido de un empleado?	NO	1. No implementado
43	A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.6 Acuerdos de confidencialidad o no divulgación	¿Los trabajadores firman acuerdos de confidencialidad?	SI	4. Implementado, documentado y revisado periódicamente
44	A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.7 Trabajo remoto	¿Existen controles para proteger la información en entornos de trabajo remoto?	NO	1. No implementado
45	A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.8 Capacitación en desarrollo seguro	¿Los desarrolladores han recibido capacitaciones relacionadas con codificación segura?	NO	1. No implementado

#	Sección	Subsección	Control	Pregunta	Cumplido	Criterio
46	A.7 Controles Físicos	Controles Físicos	7.1 Perímetro de seguridad física	¿Se definen y protegen las fronteras físicas del edificio?	NO	1. No implementado
47	A.7 Controles Físicos	Controles Físicos	7.2 Control de entrada física	¿Se registran las entradas y salidas de personal y visitantes?	SI	3. Implementado y documentado
48	A.7 Controles Físicos	Controles Físicos	7.3 Protección de oficinas, salas e instalaciones	¿Se protegen las áreas críticas con cerraduras, alarmas o CCTV?	NO	1. No implementado
49	A.7 Controles Físicos	Controles Físicos	7.4 Protección contra amenazas físicas	¿Se cuenta con sistemas de detección y extinción de incendios?	NO	1. No implementado
50	A.7 Controles Físicos	Controles Físicos	7.5 Trabajo en áreas seguras	¿Se definen áreas seguras con controles de acceso adicionales?	NO	1. No implementado
51	A.7 Controles Físicos	Controles Físicos	7.6 Áreas de entrega y carga	¿Se monitorean las áreas de carga y descarga con cámaras o guardias?	SI	3. Implementado y documentado
52	A.7 Controles Físicos	Controles Físicos	7.7 Ubicación y protección de equipos	¿Se instalan equipos críticos en áreas con control climático y energía estable?	NO	1. No implementado
53	A.7 Controles Físicos	Controles Físicos	7.8 Seguridad del cableado	¿El cableado está en ductos protegidos o canaletas seguras?	NO	1. No implementado
54	A.7 Controles Físicos	Controles Físicos	7.9 Mantenimiento	¿Existen planes de mantenimiento preventivo?	NO	1. No implementado
55	A.7 Controles Físicos	Controles Físicos	7.10 Eliminación o reutilización segura de equipos	¿Existen protocolos aprobados para el borrado seguro de datos?	NO	1. No implementado
56	A.7 Controles Físicos	Controles Físicos	7.11 Retirada de activos	¿Se registra el destino final de los activos retirados?	SI	2. Implementado sin evidencia formal

#	Sección	Subsección	Control	Pregunta	Cumplido	Criterio
57	A.7 Controles Físicos	Controles Físicos	7.12 Escritorio limpio y pantalla limpia	¿Existen informes con información de la verificación que los usuarios no dejen información sensible en sus escritorios?	NO	1. No implementado
58	A.7 Controles Físicos	Controles Físicos	7.13 Monitorización de la seguridad física	¿Se emplea CCTV, guardias de seguridad u otros mecanismos de vigilancia?	SI	4. Implementado, documentado y revisado periódicamente
59	A.7 Controles Físicos	Controles Físicos	7.14 Protección contra amenazas externas y ambientales	¿Existen sistemas UPS y generadores para cortes de energía?	SI	3. Implementado y documentado
60	A.8 Controles Tecnológicos	Seguridad de dispositivos y acceso	8.1 Dispositivos de punto final del usuario	¿Se controla el software instalado en los dispositivos del usuario?	NO	1. No implementado
61	A.8 Controles Tecnológicos	Seguridad de dispositivos y acceso	8.2 Derechos de acceso privilegiado	¿Se asignan cuentas privilegiadas sólo a personal autorizado y capacitado?	SI	3. Implementado y documentado
62	A.8 Controles Tecnológicos	Seguridad de dispositivos y acceso	8.3 Restricción de acceso a la información	¿Se utilizan listas de control de acceso (ACL) o equivalentes?	SI	3. Implementado y documentado
63	A.8 Controles Tecnológicos	Seguridad de dispositivos y acceso	8.4 Acceso al código fuente	¿Se restringe el acceso al código fuente a personal autorizado?	SI	2. Implementado sin evidencia formal
64	A.8 Controles Tecnológicos	Seguridad de dispositivos y acceso	8.5 Autenticación segura	¿Se emplea autenticación multifactor donde corresponda?	NO	1. No implementado
65	A.8 Controles Tecnológicos	Gestión de la capacidad, vulnerabilidades y configuración	8.6 Gestión de la capacidad	¿Se monitorea el uso de CPU, memoria, ancho de banda y almacenamiento?	NO	1. No implementado

#	Sección	Subsección	Control	Pregunta	Cumplido	Criterio
66	A.8 Controles Tecnológicos	Gestión de la capacidad, vulnerabilidades y configuración	8.7 Protección contra malware	¿Todos los computadores cuentan con licencias de antivirus?	NO	1. No implementado
67	A.8 Controles Tecnológicos	Gestión de la capacidad, vulnerabilidades y configuración	8.8 Gestión de vulnerabilidades técnicas	¿Existen informes sobre los resultados de los escaneos de vulnerabilidades del año 2025?	NO	1. No implementado
68	A.8 Controles Tecnológicos	Gestión de la capacidad, vulnerabilidades y configuración	8.9 Gestión de la configuración	¿Existen estándares de configuración segura para sistemas críticos?	NO	1. No implementado
69	A.8 Controles Tecnológicos	Protección de datos	8.10 Eliminación de la información	¿Existen protocolos aprobados que regulen el borrado seguro antes de eliminar información?	NO	1. No implementado
70	A.8 Controles Tecnológicos	Protección de datos	8.11 Enmascaramiento de datos	¿Se emplean técnicas de enmascaramiento antes de compartir datos sensibles?	NO	1. No implementado
71	A.8 Controles Tecnológicos	Protección de datos	8.12 Prevención de fuga de datos	¿Se han implementado soluciones de DLP (Data Loss Prevention)?	NO	1. No implementado
72	A.8 Controles Tecnológicos	Protección de datos	8.13 Copia de seguridad de la información	¿Se efectúan respaldos regulares de los datos críticos?	NO	1. No implementado
73	A.8 Controles Tecnológicos	Disponibilidad y registros	8.14 Redundancia de las instalaciones de procesamiento de la información	¿Se dispone de centros de datos alternos o configuraciones de alta disponibilidad?	NO	1. No implementado
74	A.8 Controles Tecnológicos	Disponibilidad y registros	8.15 Registro (logging)	¿Se registran los eventos de seguridad clave (inicios de sesión, accesos, errores)?	SI	3. Implementado y documentado

#	Sección	Subsección	Control	Pregunta	Cumplido	Criterio
75	A.8 Controles Tecnológicos	Disponibilidad y registros	8.16 Monitorización de actividades	¿Se emplean sistemas de detección de intrusos o SIEM?	NO	1. No implementado
76	A.8 Controles Tecnológicos	Disponibilidad y registros	8.17 Sincronización del reloj	¿Se utilizan servidores NTP que garanticen la sincronización horaria?	SI	3. Implementado y documentado
77	A.8 Controles Tecnológicos	Uso seguro de herramientas y software	8.18 Uso de programas utilitarios con privilegios	¿Se mantiene un inventario de utilitarios con privilegios?	NO	1. No implementado
78	A.8 Controles Tecnológicos	Uso seguro de herramientas y software	8.19 Instalación de software en sistemas operativos en producción	¿Se requiere aprobación antes de instalar software en producción?	SI	4. Implementado, documentado y revisado periódicamente
79	A.8 Controles Tecnológicos	Seguridad de la red y servicios asociados	8.20 Seguridad de la red	¿Se utilizan firewalls y sistemas de detección de intrusos en la red?	SI	4. Implementado, documentado y revisado periódicamente
80	A.8 Controles Tecnológicos	Seguridad de la red y servicios asociados	8.21 Seguridad de los servicios de red	¿Se aplican controles de acceso a servicios como DNS, correo, FTP, etc.?	SI	2. Implementado sin evidencia formal
81	A.8 Controles Tecnológicos	Seguridad de la red y servicios asociados	8.22 Segmentación de redes	¿Se han definido segmentos separados para sistemas críticos y usuarios comunes?	SI	4. Implementado, documentado y revisado periódicamente
82	A.8 Controles Tecnológicos	Seguridad de la red y servicios asociados	8.23 Filtrado web	¿Se emplea filtrado web para bloquear sitios maliciosos?	SI	4. Implementado, documentado y revisado periódicamente
83	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.24 Uso de criptografía	¿Se utilizan algoritmos criptográficos aprobados?	NO	1. No implementado

#	Sección	Subsección	Control	Pregunta	Cumplido	Criterio
84	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.25 Ciclo de vida de desarrollo seguro	¿Se aplican metodologías de desarrollo seguro (por ejemplo, OWASP)?	NO	1. No implementado
85	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.26 Requisitos de seguridad de las aplicaciones	¿Se establecen requisitos de seguridad desde la fase de diseño hasta la de aplicación?	NO	1. No implementado
86	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.27 Principios de ingeniería de sistemas seguros	¿Se aplican principios de seguridad en el diseño, desarrollo y mantenimiento de los sistemas?	NO	1. No implementado
87	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.28 Entorno de desarrollo seguro	¿El entorno de desarrollo está separado del de producción?	SI	2. Implementado sin evidencia formal
88	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.29 Codificación segura	¿Se capacita a los desarrolladores en codificación segura?	NO	1. No implementado
89	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.30 Desarrollo externalizado	¿Se definen requisitos de seguridad en contratos con desarrolladores externos?	NO	1. No implementado
90	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.31 Pruebas seguras	¿Se realizan pruebas de penetración antes de la liberación de aplicaciones?	NO	1. No implementado
91	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.32 Gestión de la seguridad de la información en entornos de prueba	¿Se utilizan datos enmascarados en el entorno de prueba?	NO	1. No implementado
92	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.33 Seguridad de la información en procesos de desarrollo y soporte	¿Existen protocolos aprobados para el parcheo y actualización?	NO	1. No implementado

#	Sección	Subsección	Control	Pregunta	Cumplido	Criterio
93	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.34 Revisión de la seguridad de la información tras cambios en el entorno operativo	¿Se revisa la configuración de seguridad tras actualizaciones mayores?	NO	1. No implementado

Anexo 4: Priorización de brechas

#	Sección	Subsección	Control	Pregunta	Cumplido	Impacto	Urgencia	Criticidad	Tipo
1	A.5 Controles Organizativos	Políticas, organización y relaciones	5.3 Segregación de funciones	¿Se han identificado y separado las funciones críticas para evitar conflictos de interés?	NO	3	3	9	1. Alta

#	Sección	Subsección	Control	Pregunta	Cumplido	Impacto	Urgencia	Criticidad	Tipo
2	A.5 Controles Organizativos	Políticas, organización y relaciones	5.4 Responsabilidades de la dirección	¿La alta dirección demuestra compromiso con la seguridad de la información?	NO	3	3	9	1. Alta
3	A.5 Controles Organizativos	Políticas, organización y relaciones	5.6 Contacto con grupos de interés especiales	¿La organización participa en foros o grupos de seguridad especializados?	NO	3	2	6	2. Media
4	A.5 Controles Organizativos	Políticas, organización y relaciones	5.7 Inteligencia sobre amenazas	¿La organización mantiene suscripciones con fuente de inteligencia sobre nuevas amenazas?	NO	3	3	9	1. Alta
5	A.5 Controles Organizativos	Políticas, organización y relaciones	5.8 Seguridad de la información en la gestión de proyectos	¿Se evalúan riesgos de seguridad antes de la implementación del proyecto?	NO	3	2	6	2. Media
6	A.5 Controles Organizativos	Gestión de activos	5.9 Inventario de la información y otros activos asociados	¿Existe un inventario documentado y actualizado de los activos de información?	NO	3	3	9	1. Alta
7	A.5 Controles	Gestión de activos	5.10 Uso aceptable de la	¿Se han definido políticas claras de	NO	3	2	6	2. Media

#	Sección	Subsección	Control	Pregunta	Cumplido	Impacto	Urgencia	Criticidad	Tipo
	Organizativos		información y otros activos asociados	uso aceptable de activos?					
8	A.5 Controles Organizativos	Gestión de activos	5.11 Devolución de activos	¿Se verifica la devolución de activos (dispositivos, credenciales) al término de contratos o empleos?	NO	2	2	4	2. Media
9	A.5 Controles Organizativos	Clasificación y manejo de la información	5.12 Clasificación de la información	¿Existe una política aprobada que incluya los criterios para clasificar la información?	NO	3	2	6	2. Media
10	A.5 Controles Organizativos	Clasificación y manejo de la información	5.13 Etiquetado de la información	¿La información lleva etiquetas que indiquen su nivel de clasificación?	NO	2	2	4	2. Media
11	A.5 Controles Organizativos	Clasificación y manejo de la información	5.14 Transferencia de la información	¿Existen procedimientos aprobados que garanticen la seguridad para la transferencia de información?	NO	3	2	6	2. Media

#	Sección	Subsección	Control	Pregunta	Cumplido	Impacto	Urgencia	Criticidad	Tipo
12	A.5 Controles Organizativos	Control de acceso organizativo	5.16 Gestión de la identidad	¿Se cuenta con un proceso aprobado que regule el alta, modificación y baja de identidades?	NO	2	2	4	2. Media
13	A.5 Controles Organizativos	Control de acceso organizativo	5.17 Información de autenticación	¿Se almacenan contraseñas cifradas y protegidas?	NO	3	2	6	2. Media
14	A.5 Controles Organizativos	Relaciones con proveedores	5.19 Seguridad de la información en las relaciones con proveedores	¿Se evalúa la seguridad de la información antes de contratar proveedores?	NO	2	2	4	2. Media
15	A.5 Controles Organizativos	Relaciones con proveedores	5.20 Inclusión de la seguridad de la información en los acuerdos con proveedores	¿Se incorporan cláusulas de seguridad de la información en los contratos con proveedores?	NO	3	2	6	2. Media
16	A.5 Controles Organizativos	Relaciones con proveedores	5.21 Gestión de la seguridad de la información en la cadena de suministro de TIC	¿En el año 2024 se evaluó la seguridad de toda la cadena de suministros de los dispositivos del parque informático?	NO	3	2	6	2. Media

#	Sección	Subsección	Control	Pregunta	Cumplido	Impacto	Urgencia	Criticidad	Tipo
17	A.5 Controles Organizativos	Relaciones con proveedores	5.22 Supervisión, revisión y evaluación de servicios del proveedor	¿Se llevan a cabo auditorías o revisiones periódicas a los proveedores en materia de seguridad?	NO	2	2	4	2. Media
18	A.5 Controles Organizativos	Relaciones con proveedores	5.23 Seguridad de la información para el uso de servicios en la nube	¿En el año 2024 se evaluó los riesgos asociados al uso de la nube?	NO	2	1	2	3. Baja
19	A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.25 Evaluación y decisión sobre eventos de seguridad de la información	¿Existen informes de evaluación sistemática de los eventos que permita clasificarlos como incidentes?	NO	1	3	3	3. Baja
20	A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.27 Lecciones aprendidas de incidentes de seguridad de la información	¿Existen informes que contengan información post-incidente para extraer lecciones aprendidas?	NO	2	1	2	3. Baja
21	A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.28 Recopilación de evidencia	¿Existenten protocolos aprobados que regule el procedimiento para la	NO	1	3	3	3. Baja

#	Sección	Subsección	Control	Pregunta	Cumplido	Impacto	Urgencia	Criticidad	Tipo
				recolección forense de datos?					
22	A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.29 Planificación de la continuidad del negocio	¿Existen protocolos aprobados para la continuidad de los servicios?	NO	2	1	2	3. Baja
23	A.5 Controles Organizativos	Gestión de incidentes y continuidad del negocio	5.30 Preparación de las TIC para la continuidad del negocio	¿Existen protocolos de respaldo y recuperación para sistemas críticos?	NO	1	3	3	3. Baja
24	A.5 Controles Organizativos	Cumplimiento y requisitos legales	5.31 Cumplimiento de requisitos legales, reglamentarios y contractuales	¿Se mantiene un registro de las normativas aplicables?	NO	2	1	2	3. Baja
25	A.5 Controles Organizativos	Cumplimiento y requisitos legales	5.32 Derechos de propiedad intelectual	¿Todos los computadores tienen software original?	NO	1	3	3	3. Baja
26	A.5 Controles Organizativos	Cumplimiento y requisitos legales	5.33 Protección de registros	¿Se aplican controles para asegurar la integridad y disponibilidad de los registros?	NO	2	1	2	3. Baja
27	A.5 Controles	Cumplimiento y requisitos legales	5.34 Privacidad y protección de información de	¿Se protege la PII mediante cifrado, acceso limitado y	NO	2	1	2	3. Baja

#	Sección	Subsección	Control	Pregunta	Cumplido	Impacto	Urgencia	Criticidad	Tipo
	Organizativos		identificación personal (PII)	controles adicionales?					
28	A.5 Controles Organizativos	Revisiones y operaciones organizativas	5.35 Revisión independiente de la seguridad de la información	¿Se llevan a cabo auditorías externas de seguridad de la información?	NO	1	3	3	3. Baja
29	A.5 Controles Organizativos	Revisiones y operaciones organizativas	5.36 Procedimientos operativos documentados	¿Están los procedimientos de seguridad operativa claramente documentados?	NO	3	2	6	2. Media
30	A.5 Controles Organizativos	Revisiones y operaciones organizativas	5.37 Gestión de cambios	¿Existen protocolos aprobados que regulen el proceso para solicitar, evaluar y aprobar cambios en lo sistemas de información?	NO	3	2	6	2. Media
31	A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.3 Concientización, educación y formación en seguridad de la información	¿Existen programas regulares de capacitación en seguridad de la información?	NO	2	2	4	2. Media
32	A.6 Controles	Controles Relacionados	6.4 Proceso disciplinario	¿Existen protocolos	NO	1	3	3	3. Baja

#	Sección	Subsección	Control	Pregunta	Cumplido	Impacto	Urgencia	Criticidad	Tipo
	Relacionados con las Personas	con las Personas		disciplinarios aprobados para abordar violaciones de seguridad?					
33	A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.5 Responsabilidades tras la terminación o cambio de empleo	¿Se revocan accesos y devuelven activos tras la renuncia o despido de un empleado?	NO	2	1	2	3. Baja
34	A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.7 Trabajo remoto	¿Existen controles para proteger la información en entornos de trabajo remoto?	NO	3	2	9	2. Media
35	A.6 Controles Relacionados con las Personas	Controles Relacionados con las Personas	6.8 Capacitación en desarrollo seguro	¿Los desarrolladores han recibido capacitaciones relacionadas con codificación segura?	NO	3	3	9	1. Alta
36	A.7 Controles Físicos	Controles Físicos	7.1 Perímetro de seguridad física	¿Se definen y protegen las fronteras físicas del edificio?	NO	3	2	6	2. Media
37	A.7 Controles Físicos	Controles Físicos	7.3 Protección de oficinas, salas e instalaciones	¿Se protegen las áreas críticas con	NO	2	2	4	2. Media

#	Sección	Subsección	Control	Pregunta	Cumplido	Impacto	Urgencia	Criticidad	Tipo
				cerraduras, alarmas o CCTV?					
38	A.7 Controles Físicos	Controles Físicos	7.4 Protección contra amenazas físicas	¿Se cuenta con sistemas de detección y extinción de incendios?	NO	2	2	4	2. Media
39	A.7 Controles Físicos	Controles Físicos	7.5 Trabajo en áreas seguras	¿Se definen áreas seguras con controles de acceso adicionales?	NO	1	3	3	3. Baja
40	A.7 Controles Físicos	Controles Físicos	7.7 Ubicación y protección de equipos	¿Se instalan equipos críticos en áreas con control climático y energía estable?	NO	2	1	2	3. Baja
41	A.7 Controles Físicos	Controles Físicos	7.8 Seguridad del cableado	¿El cableado está en ductos protegidos o canaletas seguras?	NO	1	3	3	3. Baja
42	A.7 Controles Físicos	Controles Físicos	7.9 Mantenimiento	¿Existen planes de mantenimiento preventivo?	NO	3	3	9	1. Alta
43	A.7 Controles Físicos	Controles Físicos	7.10 Eliminación o reutilización segura de equipos	¿Existen protocolos aprobados para el borrado seguro de datos?	NO	3	3	9	1. Alta

#	Sección	Subsección	Control	Pregunta	Cumplido	Impacto	Urgencia	Criticidad	Tipo
44	A.7 Controles Físicos	Controles Físicos	7.12 Escritorio limpio y pantalla limpia	¿Existen informes con información de la verificación que los usuarios no dejen información sensible en sus escritorios?	NO	3	3	9	1. Alta
45	A.8 Controles Tecnológicos	Seguridad de dispositivos y acceso	8.1 Dispositivos de punto final del usuario	¿Se controla el software instalado en los dispositivos del usuario?	NO	3	3	9	1. Alta
46	A.8 Controles Tecnológicos	Seguridad de dispositivos y acceso	8.5 Autenticación segura	¿Se emplea autenticación multifactor donde corresponda?	NO	2	2	4	2. Media
47	A.8 Controles Tecnológicos	Gestión de la capacidad, vulnerabilidades y configuración	8.6 Gestión de la capacidad	¿Se monitorea el uso de CPU, memoria, ancho de banda y almacenamiento?	NO	3	3	9	1. Alta
48	A.8 Controles Tecnológicos	Gestión de la capacidad, vulnerabilidades y configuración	8.7 Protección contra malware	¿Todos los computadores cuentan con licencias de antivirus?	NO	3	2	6	2. Media
49	A.8 Controles Tecnológicos	Gestión de la capacidad, vulnerabilidade	8.8 Gestión de vulnerabilidades técnicas	¿Existen informes sobre los resultados de los escaneos de	NO	2	2	4	2. Media

#	Sección	Subsección	Control	Pregunta	Cumplido	Impacto	Urgencia	Criticidad	Tipo
		s y configuración		vulnerabilidades del año 2025?					
50	A.8 Controles Tecnológicos	Gestión de la capacidad, vulnerabilidades y configuración	8.9 Gestión de la configuración	¿Existen estándares de configuración segura para sistemas críticos?	NO	3	2	6	2. Media
51	A.8 Controles Tecnológicos	Protección de datos	8.10 Eliminación de la información	¿Existen protocolos aprobados que regulen el borrado seguro antes de eliminar información?	NO	2	2	4	2. Media
52	A.8 Controles Tecnológicos	Protección de datos	8.11 Enmascaramiento de datos	¿Se emplean técnicas de enmascaramiento antes de compartir datos sensibles?	NO	3	2	6	2. Media
53	A.8 Controles Tecnológicos	Protección de datos	8.12 Prevención de fuga de datos	¿Se han implementado soluciones de DLP (Data Loss Prevention)?	NO	2	2	4	2. Media
54	A.8 Controles Tecnológicos	Protección de datos	8.13 Copia de seguridad de la información	¿Se efectúan respaldos regulares de los datos críticos?	NO	2	1	2	3. Baja

#	Sección	Subsección	Control	Pregunta	Cumplido	Impacto	Urgencia	Criticidad	Tipo
55	A.8 Controles Tecnológicos	Disponibilidad y registros	8.14 Redundancia de las instalaciones de procesamiento de la información	¿Se dispone de centros de datos alternos o configuraciones de alta disponibilidad?	NO	1	3	3	3. Baja
56	A.8 Controles Tecnológicos	Disponibilidad y registros	8.16 Monitorización de actividades	¿Se emplean sistemas de detección de intrusos o SIEM?	NO	2	1	2	3. Baja
57	A.8 Controles Tecnológicos	Uso seguro de herramientas y software	8.18 Uso de programas utilitarios con privilegios	¿Se mantiene un inventario de utilitarios con privilegios?	NO	1	3	3	3. Baja
58	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.24 Uso de criptografía	¿Se utilizan algoritmos criptográficos aprobados?	NO	2	1	2	3. Baja
59	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.25 Ciclo de vida de desarrollo seguro	¿Se aplican metodologías de desarrollo seguro (por ejemplo, OWASP)?	NO	1	3	3	3. Baja
60	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.26 Requisitos de seguridad de las aplicaciones	¿Se establecen requisitos de seguridad desde la fase de diseño hasta la de aplicación?	NO	2	1	2	3. Baja

#	Sección	Subsección	Control	Pregunta	Cumplido	Impacto	Urgencia	Criticidad	Tipo
61	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.27 Principios de ingeniería de sistemas seguros	¿Se aplican principios de seguridad en el diseño, desarrollo y mantenimiento de los sistemas?	NO	2	1	2	3. Baja
62	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.29 Codificación segura	¿Se capacita a los desarrolladores en codificación segura?	NO	1	3	3	3. Baja
63	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.30 Desarrollo externalizado	¿Se definen requisitos de seguridad en contratos con desarrolladores externos?	NO	1	3	3	3. Baja
64	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.31 Pruebas seguras	¿Se realizan pruebas de penetración antes de la liberación de aplicaciones?	NO	3	3	9	1. Alta
65	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.32 Gestión de la seguridad de la información en entornos de prueba	¿Se utilizan datos enmascarados en el entorno de prueba?	NO	3	2	6	2. Media
66	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.33 Seguridad de la información en procesos de desarrollo y soporte	¿Existen protocolos aprobados para el parcheo y actualización?	NO	2	3	6	2. Media

#	Sección	Subsección	Control	Pregunta	Cumplido	Impacto	Urgencia	Criticidad	Tipo
67	A.8 Controles Tecnológicos	Criptografía, desarrollo y ciclo de vida	8.34 Revisión de la seguridad de la información tras cambios en el entorno operativo	¿Se revisa la configuración de seguridad tras actualizaciones mayores?	NO	3	2	6	2. Media

Anexo 5: Diagrama Técnico de Gantt (En semanas)

ID	Descripción	Prioridad	Responsable	Inicio	Fin	Duración	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24
1.1	Política actualizaciones	Critica	Dirección Técnica / S.I.	1	3	3																								
10.1	Análisis riesgos áreas	Critica	Dirección Técnica / Seguridad Física	1	3	3																								
4.1	Bloqueo físico estaciones	Critica	Dirección Técnica / Infraestructura	1	4	4																								
8.1	Gabinetes seguridad documentos	Critica	Infraestructura / Archivo	1	6	6																								
4.3	Políticas traslado equipos	Crítica	Asesoría Legal / S.I.	2	4	3																								
1.3	Inventario software	Crítica	Seguridad de la Información	2	3	2																								
2.1	Política gestión contraseñas	Alta	Seguridad Información / Dirección Técnica	3	6	4																								

ID	Descripción	Prioridad	Responsable	Inicio	Fin	Duración	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24
1.2	Mecanismos actualización automática	Crítica	Infraestructura / Soporte Técnico	4	7	4																								
1.5	Limitar software no autorizado	Crítica	Dirección Técnica / Admin. TI	5	7	3																								
8.2	Controles acceso físico archivo	Crítica	Dirección Admin. / Seguridad	6	11	6																								
4.2	Dispositivos antirrobo	Crítica	Seguridad Física / TI	6	11	6																								
2.2	Mecanismos contraseñas complejas	Alta	Infraestructura TI / Soporte Técnico	6	9	4																								
3.1	Procedimientos pruebas software	Media	Equipo Desarrollo / Dirección Técnica	4	8	5																								
1.4	Herramientas escaneo vulnerabilidades	Crítica	S.I. / TIC	8	11	4																								
2.3	Auditorías credenciales	Alta	Seguridad de la Información	9	11	3																								

ID	Descripción	Prioridad	Responsable	Inicio	Fin	Duración	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24
3.4	Entornos separados pruebas	Media	TI / Infraestructura	8	11	4																								
5.1	Cronograma mantenimiento preventivo	Alta	Dirección Técnica / Infraestructura	9	14	6																								
11.1	Revisión protocolos cifrado	Alta	Equipo Seguridad Informática	5	8	4																								
7.1	Gabinetes cerradura archivo	Alta	Dirección Admin. / Infraestructura	5	10	6																								
16.1	Respaldos bases de datos	Alta	Admin. bases de datos	6	13	8																								
1.6	Capacitación malware	Crítica	Talento Humano / S.I.	10	14	5																								
4.4	Sensibilización protección dispositivos	Crítica	Talento Humano / S.I.	9	12	4																								
2.4	Autenticación multifactor (MFA)	Alta	Administración de TI	11	16	6																								

ID	Descripción	Prioridad	Responsable	Inicio	Fin	Duración	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24
2.5	Capacitación contraseñas	Alta	Talento Humano / S.I.	13	17	5																								
3.2	Herramientas revisión código	Media	TI / Seguridad Información	10	13	4																								
5.2	Sistema monitoreo hardware	Alta	Jefatura Tecnología / Soporte	14	24	11																								
5.3	Procedimientos mantenimiento	Alta	S.I. / Gestión Calidad	17	22	6																								
6.1	Implementar MFA sistemas críticos	Media	Área Tecnología / S.I.	15	24	10																								
6.2	Políticas complejidad contraseñas	Media	S.I. / Talento Humano	7	12	6																								
6.3	Auditoría credenciales y accesos	Media	Jefatura de Tecnología	15	20	6																								
7.2	Respaldos automáticos documentos	Alta	Área de Tecnología	13	22	10																								

ID	Descripción	Prioridad	Responsable	Inicio	Fin	Duración	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24
8.3	Monitoreo cámaras documentos	Crítica	Tecnología / Infraestructura	15	24	10																								
8.4	Políticas gestión documental	Crítica	Asesoría Legal / Gestión Doc.	13	18	6																								
9.1	Política confidencialidad	Baja	Asesoría Legal / Dirección Admin.	8	13	6																								
10.2	Sistema videovigilancia	Crítica	Dirección Admin. / Proveedores	15	24	10																								
10.3	Controles acceso biométrico	Crítica	Dirección Técnica / Sistemas	15	24	10																								
10.4	Capacitación seguridad física	Crítica	Talento Humano / Seguridad	19	24	6																								
11.2	Cifrado extremo a extremo	Alta	Depto. Sistemas / Proveedor TI	10	15	6																								
11.3	Políticas uso cifrado	Alta	Dirección Técnica /	10	15	6																								

ID	Descripción	Prioridad	Responsable	Inicio	Fin	Duración	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24
			Seguridad Info.																											
12.1	Auditoría red	Media	Equipo Seguridad Informática	7	10	4																								
12.2	Actualización configuración red	Media	Departamento de Sistemas	11	15	5																								
5.4	Capacitación mantenimiento	Alta	Talento Humano / Jefatura Técnica	21	24	4																								
5.5	Evaluación contratos proveedores	Alta	Dirección Admin. / Compras	10	13	4																								
6.4	Capacitación autenticación	Media	Talento Humano / S.I.	18	22	5																								
7.3	Digitalización documentos	Alta	Archivo / Dirección Técnica	10	24	15																								
7.4	Políticas conservación documentos	Alta	Gestión Documental / Legal	8	13	6																								

ID	Descripción	Prioridad	Responsable	Inicio	Fin	Duración	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24
9.2	Difusión políticas confidencialidad	Baja	Talento Humano / Comunicaciones	14	17	4																								
9.3	Capacitaciones manejo información	Baja	Talento Humano / Seguridad Info.	16	20	5																								
11.4	Capacitación transmisión segura	Alta	Talento Humano / Seguridad Info.	15	20	6																								
12.3	Segmentación de red	Media	Equipo Infraestructura	14	19	6																								
12.4	Autenticación y registros red	Media	Administrador de Red	14	19	6																								
13.1	Revisión contratos proveedores	Baja	Unidad Jurídica	6	9	4																								
13.2	Establecer SLA con proveedores	Baja	Dirección Admin. Financiera	11	15	5																								
13.3	Evaluar alternativas proveedores	Baja	Unidad de Adquisiciones	12	17	6																								

ID	Descripción	Prioridad	Responsable	Inicio	Fin	Duración	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24
14.1	Revisión contratos confidencialidad	Baja	Asesoría Legal	8	15	8																								
14.2	Incluir cláusulas confidencialidad	Baja	Asesoría Legal / Dirección Admin.	16	23	8																								
14.3	Capacitación contratación	Baja	Unidad Talento Humano / S.I.	12	20	9																								
15.1	Revisión brechas contractuales	Baja	Dirección Administrativa	4	6	3																								
15.2	Negociar SLA críticos	Baja	Gerencia General / Asesoría Legal	7	10	4																								
15.3	Documentar y firmar SLA	Baja	Asesoría Legal	11	14	4																								
16.2	Capacitación gestión datos	Alta	Unidad Talento Humano	15	22	8																								
16.3	Políticas validación datos	Alta	Responsable Desarrollo Sistemas	15	20	6																								

ID	Descripción	Prioridad	Responsable	Inicio	Fin	Duración	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24
16.4	Auditorías bases de datos	Alta	Unidad Seguridad Información	10	19	10																								
17.1	Sistema backup automático	Media	Área de Sistemas	13	18	6																								
17.2	Redundancia servicios críticos	Media	Área Técnica	19	24	6																								
17.4	Documentar respaldo/recuperación	Media	Responsable S.I.	8	13	6																								
17.5	Capacitación respaldo/recuperación	Media	RRHH y S.I.	10	19	10																								
18.1	Inventario usuarios y roles	Baja	Administrador de Sistemas	13	18	6																								
18.2	Políticas control accesos por roles	Baja	Responsable S.I.	17	22	6																								
18.4	Capacitación gestión accesos	Baja	Talento Humano	22	24	3																								
18.5	Configurar alertas accesos	Baja	Administrador Seguridad TI	20	24	5																								

ID	Descripción	Prioridad	Responsable	Inicio	Fin	Duración	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24
9.4	Cláusulas confidencialidad contratos	Baja	Asesoría Legal	13	18	6																								
3.3	Capacitación codificación segura	Media	Talento Humano / S.I.	14	18	5																								
3.5	Auditorías código fuente	Media	Auditoría Interna / S.I.	20	20	1																								
4.5	Revisión inventario activos	Crítica	Jefatura Tecnología / Auditoría	18	18	1																								
13.4	Supervisión cumplimiento SLA	Baja	Unidad Técnica	19	19	1																								
15.4	Seguimiento cumplimiento SLA	Baja	Responsable de TI	19	19	1																								
17.3	Pruebas restauración backups	Media	Área de Sistemas	22	22	1																								
18.3	Revisiones cuentas usuario	Baja	Auditor Interno	23	23	1																								

Anexo 6: Trazabilidad de Controles con Impacto Empresarial

La siguiente tabla establece la relación directa entre los controles de seguridad propuestos y los riesgos empresariales específicos de la EPAA-AA. Esta trazabilidad demuestra que la implementación del SGSI no responde únicamente a requisitos normativos, sino que constituye una **inversión estratégica** en la protección de los procesos críticos que sustentan la prestación del servicio esencial de agua potable y alcantarillado.

Metodología aplicada:

1. Identificación de los controles ISO 27001 más relevantes para EPAA-AA
2. Análisis de riesgos empresariales asociados a cada control
3. Evaluación de impactos operativos concretos en servicios críticos
4. Vinculación con los planes de acción desarrollados en la propuesta

Uso de esta tabla:

- **Para priorización:** Identificar qué controles protegen procesos más críticos
- **Para justificación:** Comunicar el valor empresarial de cada inversión en seguridad

Para planificación: Alinear la implementación con objetivos estratégicos institucionales

Control ISO 27001	Descripción del Control	Riesgo Empresarial que Mitiga	Impacto en EPAA-AA si NO se Implementa	Plan de Acción Correspondiente
A.5.1	Políticas para la seguridad de la información	Falta de gobierno y coordinación en seguridad.	Decisiones descoordinadas, inversiones duplicadas o ineficientes, falta de alineación estratégica.	Plan 4.8.1 (Políticas generales)
A.5.9	Inventario de la información y otros activos	Desconocimiento de activos críticos.	No se protege lo importante, recursos mal asignados, incapacidad para priorizar inversiones.	Plan 4.8.4 (Protección dispositivos)
A.7.4	Seguridad de las oficinas, salas y equipos	Acceso físico no autorizado a áreas críticas	Intrusión en centro de control SCADA → interrupción servicio agua → afectación comunidad	Plan 4.8.10 (Intrusión física)
A.8.3	Gestión de la capacidad	Saturación o falla de sistemas críticos	Sistema de facturación colapsado → no se emiten facturas → sin ingresos → problemas financieros	Plan 4.8.17 (Redundancia servicios)
A.8.13	Información de respaldo	Pérdida de datos operativos	Pérdida registros de consumo → facturación incorrecta → reclamos masivos → daño reputacional	Plan 4.8.16 (Integridad datos)
A.8.19	Gestión de vulnerabilidades técnicas	Ataques cibernéticos a sistemas operativos	Infección malware en SCADA → interrupción distribución agua → emergencia sanitaria	Plan 4.8.1 (Actualizaciones seguridad)
A.8.23	Protección de datos	Exfiltración o robo de información	Robo datos de usuarios → violación privacidad → multas y sanciones legales	Plan 4.8.11 (Intercepción datos)

Control ISO 27001	Descripción del Control	Riesgo Empresarial que Mitiga	Impacto en EPAA-AA si NO se Implementa	Plan de Acción Correspondiente
A.5.14	Transferencia de la información	Intercepción de comunicaciones institucionales	Interceptación datos sensibles en tránsito → espionaje industrial → ventaja competidores	Plan 4.8.11 (Cifrado datos)
A.6.2	Términos y condiciones de empleo	Fugas de información por personal	Divulgación información estratégica → pérdida ventaja competitiva en licitaciones	Plan 4.8.9 (Divulgación accidental)
A.5.30	Preparación de las TIC para la continuidad del negocio	Interrupción prolongada de servicios	Corte prolongado sistema SCADA → suspensión servicio agua → emergencia pública	Plan 4.8.17 (Continuidad servicios
A.8.2	Privilegios de acceso	Accesos no autorizados a sistemas	Manipulación datos de facturación → fraudes → pérdidas económicas → investigaciones	Plan 4.8.2 (Accesos no autorizados)
A.5.15	Control de acceso organizativo	Accesos excesivos o inadecuados	Empleado con privilegios excesivos → errores o malas intenciones → daños sistemas críticos	Plan 4.8.18 (Gestión usuarios)
A.7.7	Protección contra amenazas físicas y del entorno	Daños por desastres naturales	Inundación sala servidores → pérdida total sistemas → suspensión operaciones por días/semanas	Plan 4.8.5 (Fallas hardware)
A.5.20	Inclusión de la seguridad de la información en los acuerdos con proveedores	Fallas en servicios tercerizados	Proveedor internet falla → sin conectividad → sistemas aislados → operación paralizada	Plan 4.8.13 (Fallo proveedores)

Control ISO 27001	Descripción del Control	Riesgo Empresarial que Mitiga	Impacto en EPAA-AA si NO se Implementa	Plan de Acción Correspondiente
A.8.12	Protección contra malware	Infecciones masivas en la red	Ransomware en red corporativa → cifrado todos los sistemas → operación detenida completamente	Plan 4.8.1 (Protección malware)
A.5.31	Cumplimiento de requisitos legales	Incumplimiento normativo	Multas por no proteger datos personales → sanciones de autoridades de control → daño reputacional	Plan 4.8.14 (Información sensible)
A.8.5	Gestión de credenciales de autenticación	Robo de identidades digitales	Suplantación administrador sistemas → control total por atacantes → sabotaje posible	Plan 4.8.6 (Autenticación segura)
A.8.10	Cifrado	Intercepción de comunicaciones	Interceptación datos SCADA en tránsito → conocimiento vulnerabilidades → ataques dirigidos	Plan 4.8.11 (Cifrado datos)

Anexo 7: Acta de Entrega – Recepción Técnica EPAA-AA

EPAA
ANTONIO ANTE

ACTA DE ENTREGA-RECEPCIÓN TÉCNICA

AREA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TICs) - EPAA-AA

En la ciudad de Atuntaqui, a los días 23 del mes de diciembre de 2025, se procede a realizar la entrega-recepción formal del material técnico derivado del Trabajo de Integración Curricular, bajo los siguientes términos:

1. INTERVINIENTES:

- **Entrega:** Sr. Jonathan David Segovia Chiza, estudiante de la Carrera de Software de la Universidad Técnica del Norte (UTN).
- **Recibe:** Ing. Marco Sarmiento, Especialista en Tecnología del Departamento de TICs de la EPAA-AA.

2. OBJETO: Certificar la entrega del documento técnico titulado: **"Propuesta de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la Empresa Pública de Agua Potable y Alcantarillado de Antonio Ante (EPAA-AA) en base a la normativa ISO/IEC 27001".**

3. DETALLE DE LO ENTREGADO: Se hace entrega de los siguientes insumos en formato digital y físico:

- Documento final de la Propuesta de SGSI (Informe técnico detallado).
- Matriz de Identificación y Valoración de Activos de Información.
- Análisis de Riesgos Institucionales bajo metodología MAGERIT v3.
- Plan de Tratamiento de Riesgos y Hoja de Ruta para la implementación de los 67 controles de seguridad identificados.

4. CONFORMIDAD: El Departamento de TICs de la EPAA-AA manifiesta haber recibido los productos antes mencionados, los cuales constituyen un insumo técnico de gran valor para la planificación de la seguridad informática y la mejora continua de los procesos tecnológicos de la institución.

MARCO ANTONIO SARMIENTO ROSERO

Ing. Marco Sarmiento
Especialista de Tecnologia
EPAA-AA

EMPRESA PUBLICA DE AGUA POTABLE Y ALCANTARILLADO
epaa
GERENCIA
ANTONIO ANTE
ECUADOR

Calle Bolívar y González Suárez esq. / Telf: (06)290-6823 Ext. 101.
www.epaa.gob.ec / Atuntaqui - Ecuador