**FACULTAD DE POSTGRADO**
**TRABAJO FINAL DE GRADUACIÓN**

# PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN ISO/IEC 27001:2022 EN LEYDE.

**SUSTENTADO POR:**

**DANILO JOSIMAR HERRERA ELVIR**
**NERY JESÚS MONJARÁS CARRANZA**

**PREVIA INVESTIDURA AL TÍTULO DE**

**MÁSTER EN**
**GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN**

**SAN PEDRO SULA, CORTÉS, HONDURAS, C.A.**

**AGOSTO, 2025**

**UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA**

**UNITEC**

**FACULTAD DE POSTGRADO**

**AUTORIDADES UNIVERSITARIAS**

**RECTORA**

**ROSALPINA RODRíGUEZ**

**VICERRECTOR ACADÉMICO NACIONAL**

**JAVIER ABRAHAM SALGADO LEZAMA**

**SECRETARIO GENERAL**

**ROGER MARTÍNEZ MIRALDA**

**DECANA FACULTAD DE POSTGRADO**

**ANA DEL CARMEN RETTALLY VARGAS**

# PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN ISO/IEC 27001:2022 EN LEYDE.

**TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE**

**MÁSTER EN**

**GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN**


**ASESOR METODOLÓGICO**

**JORGE RAÚL MARADIAGA CHIRINOS**

**MIEMBROS DE LA TERNA:**

**KEVIN EDUARDO FUNEZ FUNEZ**
**ALBA GABRIELA GARAY ROMERO**
**MANUEL SALVADOR GARCIA LACAYO**

# FACULTAD DE POSTGRADO

# PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN ISO/IEC 27001:2022 EN LEYDE

**Danilo Josimar Herrera Elvir**
**Nery Jesús Monjarás Carranza**

**Resumen**

La ciberseguridad es una prioridad global, pues las organizaciones enfrentan riesgos crecientes debido a la digitalización y las amenazas cibernéticas. En Honduras, aunque se han dado avances, aún existen desafíos en la adopción de prácticas robustas de seguridad. Este estudio evalúa la seguridad de la información en la empresa Leche y Derivados S.A (LEYDE) y su alineación con la norma ISO/IEC 27001:2022, identificando brechas y proponiendo un plan de acción basado en metodologías reconocidas. Se emplea el Ciclo de Deming (PDCA) para la mejora continua y la metodología OCTAVE para la gestión de riesgos de seguridad, con un enfoque en procesos, tecnología y el factor humano. A través de revisión documental, encuestas y entrevistas, se analizan las políticas actuales, vulnerabilidades y aceptación de nuevas estrategias de seguridad. Los hallazgos permitirán diseñar una hoja de ruta para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), fortaleciendo la protección de datos en LEYDE y asegurando su alineación con estándares internacionales.

**Palabras claves:** Ciberseguridad, Ciclo PDCA, Gestión de riesgos, ISO/IEC 27001:2022, Metodología OCTAVE, SGSI (Sistema de Gestión de Seguridad de la Información).

# GRADUATE SCHOOL

# PROPOSAL FOR THE IMPLEMENTATION OF AN INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) BASED ON ISO/IEC 27001:2022 IN LEYDE

**Danilo Josimar Herrara Elvir**
**Nery Jesús Monjarás Carranza**

**Abstract**

Cybersecurity is a global priority as organizations face increasing risks due to digitalization and cyber threats. In Honduras, despite progress, challenges remain in adopting robust security practices. This study evaluates information security at LEYDE and its alignment with the ISO/IEC 27001:2022 standard, identifying gaps and proposing an action plan based on recognized methodologies. The Deming Cycle (PDCA) is employed for continuous improvement, and the OCTAVE methodology is used for risk management, focusing on processes, technology, and the human factor. Through document review, surveys, and interviews, current policies, vulnerabilities, and the acceptance of new security strategies are analyzed. The findings will help design a roadmap for implementing an Information Security Management System (ISMS), strengthening data protection at LEYDE, and ensuring alignment with international standards.

**Keywords**: Cybersecurity, Deming Cycle (PDCA), ISMS (Information Security Management System), ISO/IEC 27001:2022, OCTAVE Methodology, Risk management.

# DEDICATORIA

A mis padres, quienes con su amor incondicional y esfuerzo han sido la base de mi crecimiento personal y académico. Su dedicación, sacrificio y apoyo constante me han permitido llegar hasta este punto, dándome las herramientas necesarias para enfrentar los desafíos con valentía y determinación. Gracias por enseñarme con su ejemplo el significado del trabajo arduo, la resiliencia y la integridad. Cada logro en mi vida es reflejo de sus enseñanzas y valores.

A mis hermanitos, mi fuente de inspiración y alegría. Su entusiasmo, su curiosidad y su manera de ver el mundo con ilusión me han recordado siempre la importancia de seguir adelante, sin perder la esperanza ni la pasión por aprender. Su presencia ha sido un motor en mi vida, llenándome de motivación para superar cada obstáculo y alcanzar mis metas.

Atentamente, Danilo Josimar Herrera Elvir

A mis padres, por ser mi guía y mi mayor ejemplo de esfuerzo, amor y dedicación. Su apoyo incondicional y sus enseñanzas han sido la base sobre la que he construido cada uno de mis logros.

A mis hermanos, por estar siempre a mi lado, apoyándome en cada paso de este camino.

A mi tía, por su cariño, consejos y por ser una fuente de inspiración y fortaleza.

A mi pareja, por su comprensión y por motivarme a seguir adelante incluso en los momentos más difíciles.

A mi hija, porque cada logro es también suyo.

Atentamente, Nery Jesús Monjarás Carranza

# AGRADECIMIENTO

A mis padres, por ser mi más grande apoyo en cada paso del camino. Gracias por su paciencia, sus palabras de aliento en los momentos difíciles y por creer en mí incluso cuando yo dudaba de mis propias capacidades. Su amor y confianza me han dado la fortaleza para superar cada reto. A mis hermanitos, por ser mi inspiración y mi mayor motivación. Su alegría, su cariño y sus ganas de aprender me han impulsado a seguir adelante con entusiasmo y determinación. A mis profesores y mentores, quienes con su guía y conocimientos me han ayudado a ampliar mis horizontes y a crecer académica y personalmente. Gracias por compartir su sabiduría y por impulsarme a dar siempre lo mejor de mí. A mis amigos y compañeros de estudio, por su compañía, su apoyo incondicional y por hacer de este proceso una experiencia más llevadera y enriquecedora. A todas aquellas personas que, de manera directa o indirecta, han sido parte de este camino, les agradezco profundamente por su apoyo y por contribuir a que este sueño hoy sea una realidad.

Atentamente, Danilo Josimar Herrera Elvir

Quiero expresar mi más sincero agradecimiento a todas las personas que han sido fundamentales en este proceso. A mis padres, por su apoyo y enseñanzas que han guiado mi camino; a mis hermanos, por su compañía y aliento constante; a mi tía, por su cariño y motivación; a mi pareja, por su paciencia, comprensión y apoyo en todo momento; y a mi hija, mi inspiración para seguir adelante. También agradezco a mis profesores y asesores, por su orientación y conocimientos que han sido esenciales en mi formación, así como a mis compañeros de estudio, por su apoyo, trabajo en equipo y amistad. Finalmente, extiendo mi gratitud a la Universidad Tecnológica Centroamericana (UNITEC) por brindarme las herramientas necesarias para mi desarrollo profesional.

Atentamente, Nery Jesús Monjarás Carranza

## TABLA DE CONTENIDO

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

## 1.1 INTRODUCCIÓN

La presente investigación se centra en analizar la necesidad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en Leche y Derivados S.A (LEYDE), fundamentado en la norma ISO/IEC 27001:2022, ante el creciente panorama de ciberataques y amenazas digitales. Ante incidentes como el gusano Morris y ataques de ransomware, que han generado importantes consecuencias económicas y operativas, la protección de datos sensibles se torna crucial para garantizar la continuidad del negocio.

La ausencia de un SGSI formalizado en LEYDE expone a la organización a riesgos que comprometen la confidencialidad, integridad y disponibilidad de la información. Por ello, se propone desarrollar una estrategia que integre controles internacionales y recursos adecuados, con el fin de fortalecer la seguridad y resiliencia ante amenazas cibernéticas.

El marco teórico aborda los fundamentos teóricos que sustentan la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en LEYDE. Se analiza el macroentorno, incluyendo la evolución de la ciberseguridad global, normativas internacionales como ISO/IEC 27001:2022 y modelos estratégicos para la gestión de riesgos. A nivel microentorno, se examina la situación actual de LEYDE en seguridad de la información y el impacto organizacional del SGSI.

Asimismo, se presentan teorías relevantes, metodologías aplicadas como PDCA y OCTAVE, y herramientas utilizadas en su ejecución. Finalmente, se detalla el marco legal aplicable, tanto internacional como en Honduras, proporcionando un contexto normativo esencial para el desarrollo del SGSI en la empresa.

En el Capítulo III se describe con detalle la metodología aplicada en esta investigación, incluyendo la identificación y operacionalización de las variables críticas para el SGSI, así como los instrumentos (cuestionarios, listas de verificación de controles ISO/IEC 27001:2022, entrevistas y matriz de análisis documental), los procedimientos de recolección de datos y las herramientas de procesamiento y validación de la información. Gracias a este diseño metodológico se obtuvo un conjunto de hallazgos cuantitativos y cualitativos presentados en el Capítulo IV que permiten diagnosticar con precisión el grado de alineamiento de LEYDE frente a los requisitos

normativos y las brechas existentes. A continuación, el Capítulo V ofrecerá las conclusiones derivadas de dichos resultados y formulará recomendaciones concretas para la implementación efectiva del SGSI conforme a ISO/IEC 27001:2022.

El Capítulo VI presenta la aplicabilidad práctica de la propuesta, estructurada bajo los lineamientos de la Guía del PMBOK y la norma ISO/IEC 27001:2022. Se detallan los componentes clave del proyecto, desde la integración y el alcance hasta la gestión de cronograma, costos, riesgos y recursos, con el fin de ofrecer una hoja de ruta clara y viable para la implementación del SGSI en LEYDE.

## 1.2 ANTECEDENTES DEL PROBLEMA

El primer ciberataque de la historia con aplicaciones al internet ocurrió en 1988 con el Gusano Morris, creado por Robert Tappan Morris, un estudiante de Cornell. Diseñado como un experimento para medir el tamaño de Internet, un error en el código hizo que el gusano se replicara sin control, infectando alrededor de 6,000 computadoras (10% de Internet en ese momento) y causando interrupciones significativas. Morris fue la primera persona condenada bajo la Ley de Fraude y Abuso Informático de EE. UU., y este incidente marcó el inicio de la ciberseguridad moderna, llevando a la creación del primer Equipo de Respuesta a Emergencias Informáticas (García Romero, 2020).

Los ataques de ransomware se han posicionado como una de las principales amenazas cibernéticas en los últimos años. De acuerdo con el informe Cost of a Data Breach Report 2023 de IBM Security (IBM, 2024a), el costo promedio de una violación de datos en 2023 fue de $4.45 millones de dólares, lo que representa un aumento del 15% respecto a 2020. Este tipo de ataques no solo implica el pago de rescates, sino también costos asociados a la interrupción de operaciones, la pérdida de reputación y las multas regulatorias. Además, el estudio destaca que las organizaciones que implementan un enfoque proactivo en seguridad, como la adopción de estándares internacionales, logran reducir significativamente los costos y el tiempo de recuperación.

Si bien muchas organizaciones pueden ser vulnerables por la falta de inversión en seguridad, es importante destacar que **LEYDE** es una corporación con una estructura organizativa compleja, múltiples áreas operativas y un alto volumen de información sensible. En ese contexto, la implementación de un **Sistema de Gestión de Seguridad de la Información (SGSI)** basado en

la norma **ISO/IEC 27001:2022** no solo debe enfocarse en la protección técnica, sino también en aspectos estratégicos, organizacionales y de gobernanza (Verizon, 2024)

En una corporación como Leche y Derivados S.A (LEYDE), la gestión de la seguridad debe estar alineada con los objetivos de negocio, involucrando a los altos mandos en la toma de decisiones y fomentando una cultura organizacional orientada a la protección de la información. Asimismo, el diseño e implementación del SGSI debe considerar una planificación integral, la asignación de recursos adecuados, la gestión del cambio organizacional y la capacitación constante del personal. El enfoque debe ser transversal, abarcando desde políticas y procedimientos hasta controles tecnológicos avanzados y auditorías internas, con el fin de garantizar la continuidad del negocio y la confianza de los clientes y socios estratégicos.

Este enfoque corporativo robustece la resiliencia ante ciberamenazas crecientes y permite a LEYDE posicionarse como una organización comprometida con la seguridad y la excelencia operativa.

La norma ISO/IEC 27001 es un estándar internacional reconocido para la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI). Publicada por primera vez en 2005 por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), esta norma ha evolucionado para adaptarse a los desafíos emergentes en ciberseguridad, con su última actualización en 2022. ISO/IEC 27001 proporciona un marco estructurado para identificar, gestionar y mitigar los riesgos asociados a la información, garantizando la confidencialidad, integridad y disponibilidad de los datos. Su enfoque basado en la mejora continua y la gestión de riesgos la convierte en una herramienta esencial para organizaciones que buscan proteger sus activos críticos y cumplir con regulaciones como el Reglamento General de Protección de Datos (RGPD) o la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En el contexto actual, donde los ciberataques y las violaciones de datos son cada vez más frecuentes, la implementación de un SGSI basado en ISO/IEC 27001:2022 no solo fortalece la postura de seguridad de las organizaciones, sino que también mejora su reputación y competitividad en el mercado. Además, la norma facilita la alineación con mejores prácticas internacionales, lo que es especialmente relevante para empresas como LEYDE, que buscan garantizar la protección de su información y la continuidad del negocio en un entorno digital en

constante evolución (ISO/IEC 27001, 2022a).

En Honduras, la situación de la ciberseguridad ha mostrado avances, pero aún enfrenta importantes desafíos. En 2023, se registraron aproximadamente **1.8 millones de ataques cibernéticos** dirigidos a sistemas tecnológicos de empresas e instituciones hondureñas, lo que pone de manifiesto la vulnerabilidad de los sistemas en el país (Zapata, 2024). **Del total de estos ataques, un 57% estuvieron dirigidos específicamente a grandes corporaciones**, que, debido a la magnitud de sus operaciones, el volumen de información que manejan y su alta exposición digital, representan un objetivo atractivo para los ciberdelincuentes. Este panorama evidencia la necesidad urgente de fortalecer las capacidades internas de ciberseguridad mediante la implementación de sistemas formales como el **Sistema de Gestión de Seguridad de la Información (SGSI)**, basado en estándares internacionales como la **ISO/IEC 27001:2022**. Dicho sistema debe contemplar no solo aspectos tecnológicos, sino también organizativos y humanos, asegurando una gestión integral del riesgo, la protección de activos críticos, la continuidad operativa y el cumplimiento regulatorio, elementos esenciales para la sostenibilidad y reputación de este tipo de organizaciones.

A pesar de la creciente conciencia sobre la importancia de la ciberseguridad, Honduras carece de una estrategia nacional definida para abordar estos riesgos, lo que limita la capacidad de respuesta ante amenazas cibernéticas. Sin embargo, se han comenzado a tomar medidas para mejorar la situación. La creación de la Ley Nacional de Ciberseguridad, que está en proceso de desarrollo, tiene como objetivo establecer un marco normativo que fortalezca la protección cibernética en el país. Además, el Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT-CR), creado en 2012, desempeña un papel clave en la prevención y respuesta ante ataques cibernéticos que afectan a las instituciones gubernamentales (A. Zambrano & Hernández, 2020).

A pesar de estos esfuerzos, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001:2022 sería fundamental para las empresas hondureñas, especialmente aquellas que manejan información sensible. Esta implementación ayudaría a gestionar los riesgos de manera sistemática y a demostrar el compromiso con la seguridad de la información, lo cual es crucial para la protección de activos y la continuidad del negocio en un entorno digital cada vez más vulnerable.

## 1.3 DEFINICIÓN DEL PROBLEMA

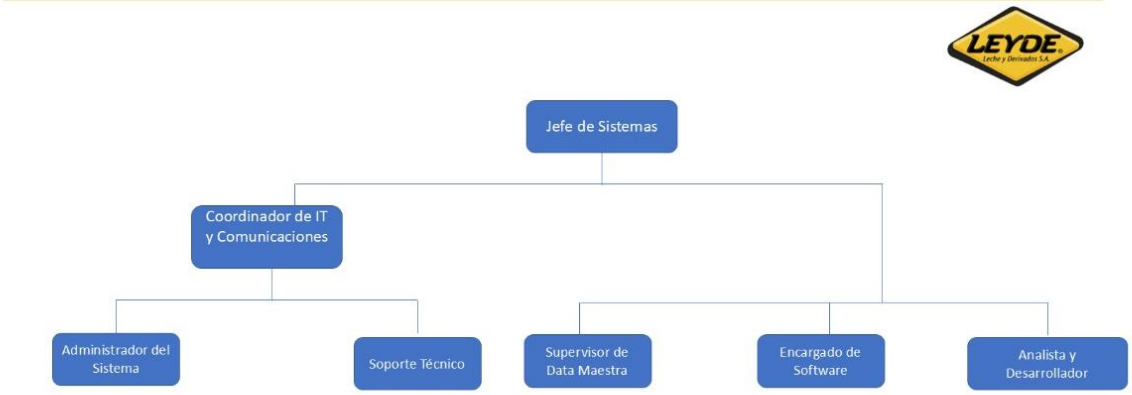
En la actualidad, la ciberseguridad representa uno de los desafíos más significativos para las organizaciones a nivel mundial. La proliferación de ataques cibernéticos ha transformado el entorno empresarial, donde los ciberdelincuentes explotan vulnerabilidades para obtener beneficios ilícitos. Este panorama también afecta a Honduras, donde las empresas, particularmente las pequeñas y medianas, enfrentan una creciente exposición a amenazas como el phishing, el malware, el ransomware y otros tipos de ataques. La rápida digitalización y la adopción de nuevas tecnologías aumentan la superficie de ataque, lo que hace más difícil proteger los activos de información sin un sistema adecuado.

El caso específico de LEYDE destaca una problemática común: la gestión de información sensible sin un sistema de seguridad adecuado. La ausencia de un SGSI genera vulnerabilidades que podrían ser mitigadas con la implementación de controles apropiados. La adopción de un sistema basado en la norma ISO/IEC 27001:2022, con su enfoque estructurado para gestionar riesgos y mejorar continuamente la seguridad, sería crucial para que LEYDE pueda enfrentar de manera efectiva los desafíos cibernéticos y demostrar su compromiso con la protección de datos ante clientes y socios.

Este problema no solo afecta a LEYDE, sino que refleja una tendencia más amplia en Honduras, donde muchas empresas no están plenamente preparadas para enfrentar los riesgos derivados de los ataques cibernéticos. La implementación de un SGSI alineado con estándares internacionales es una necesidad urgente para garantizar la protección de la información, la continuidad del negocio y el cumplimiento de las regulaciones globales en materia de seguridad de la información.

En este contexto, es fundamental contar con una estructura organizacional clara dentro del área de Tecnologías de la Información, que permita una adecuada asignación de roles y responsabilidades en la gestión de la seguridad de la información. A continuación, se presenta el organigrama del área de TI de LEYDE, el cual será clave para comprender la distribución de funciones en la implementación del SGSI conforme a la norma ISO/IEC 27001:2022.

**Figura 1: Organigrama IT - LEYDE**




## 1.4 PREGUNTAS DE INVESTIGACIÓN

### 1.4.1 PREGUNTA GENERAL

¿Cómo puede implementarse un Sistema de Gestión de Seguridad de la Información (SGSI) en LEYDE, basado en la norma ISO/IEC 27001:2022, con el fin de fortalecer la protección, confidencialidad, integridad y disponibilidad de la información?

### 1.4.2 PREGUNTAS ESPECÍFICAS

1. ¿ Cuál es el estado actual de la seguridad de la información en LEYDE y qué brechas se identifican en relación con los requisitos de la norma ISO/IEC 27001:2022?
2. ¿Cuáles son los requisitos y lineamientos establecidos en la norma ISO/IEC 27001:2022 para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI)?
3. ¿Qué metodologías, herramientas y buenas prácticas son recomendables para la implementación de un SGSI en LEYDE, conforme a ISO/IEC 27001:2022?
4. ¿Qué recursos (humanos, técnicos y financieros) son necesarios para la implementación efectiva de un SGSI en LEYDE basado en la norma ISO/IEC 27001: 2022?
5. ¿Qué plan de acción (cronograma, recursos y asignación de responsabilidades) es necesario para implementar efectivamente un SGSI en LEYDE basado en ISO/IEC 27001:2022?

## 1.5 OBJETIVOS DEL PROYECTO

### 1.5.1 OBJETIVO GENERAL

Desarrollar una propuesta de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en LEYDE, basado en la norma ISO/IEC 27001:2022, con el fin de fortalecer la protección, confidencialidad, integridad y disponibilidad de la información.

### 1.5.2 OBJETIVOS ESPECÍFICOS

1. Evaluar el estado actual de la seguridad de la información en LEYDE, identificando las brechas existentes en relación con los requisitos de la norma ISO/IEC 27001:2022.
2. Identificar y analizar los requisitos y lineamientos establecidos en la norma ISO/IEC 27001:2022 para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).
3. Analizar y seleccionar metodologías, herramientas y mejores prácticas internacionales que faciliten la implementación efectiva de un SGSI en LEYDE.
4. Identificar y definir los recursos humanos, técnicos y financieros necesarios para la implementación efectiva del SGSI en LEYDE.
5. Formular un plan de acción detallado que incluya un cronograma, asignación de recursos y responsabilidades, para la adopción efectiva del SGSI en LEYDE basado en ISO/IEC 27001:2022.

## 1.6 JUSTIFICACIÓN

Cada día, las organizaciones enfrentan intentos constantes de ataques por parte de ciberdelincuentes que buscan vulnerar sus sistemas durante un período prolongado. Aunque muchas veces estos ataques no logran su objetivo, los ciberdelincuentes continúan con su búsqueda, focalizándose en aquellas organizaciones con vulnerabilidades de seguridad que están vinculadas a su objetivo principal. De esta manera, utilizan a socios, clientes o proveedores como vías indirectas para ejecutar estos ataques informáticos.

Desde una perspectiva social, este estudio es de gran relevancia, ya que los ciberataques a las empresas no solo afectan a sus operaciones internas, sino que también tienen un impacto

significativo en su imagen y reputación ante el público y los stakeholders. Desde el enfoque financiero, el estudio resulta útil al mostrar cómo los ataques cibernéticos pueden alterar los procesos de negocios, como el aumento de costos operativos, de producción, de ventas y de administración, lo que puede afectar directamente la rentabilidad de la empresa. Además, desde una perspectiva económica, el estudio es valioso para comprender en profundidad los efectos del robo de información y cómo esto puede dañar la estructura organizacional y su competitividad en el mercado.

**Beneficios del Estudio:**

- **Resiliencia operativa y reducción de costos:** La implementación de medidas de seguridad mejora la capacidad de una empresa para resistir ciberataques, reduciendo los costos asociados a los daños generados por estos incidentes, los cuales pueden ascender a millones de dólares y afectar gravemente las operaciones y la producción.
- **Mejora en la toma de decisiones:** El estudio también facilita la capacidad de las empresas para aprovechar los datos de manera más efectiva, lo que contribuye a la toma de decisiones estratégicas y operativas más informadas.
- **Estrategias de protección cibernética:** A través del análisis, las organizaciones pueden diseñar estrategias más efectivas para protegerse contra los ciberataques, minimizando riesgos y vulnerabilidades.
- **Cumplimiento normativo:** El estudio también resalta la importancia del cumplimiento de las leyes y regulaciones sobre privacidad de datos, lo que es esencial para evitar sanciones legales y mantener la confianza del público.

# CAPÍTULO II. MARCO TEÓRICO

## 2.1 MACROENTORNO

### 2.1.1 INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN

En la actualidad, la seguridad de la información se ha convertido en un pilar fundamental para el funcionamiento sostenible y resiliente de gobiernos, empresas y la sociedad en general. Este ámbito no se desarrolla de manera aislada, sino que está profundamente influenciado por un entorno complejo en el que confluyen múltiples factores: avances tecnológicos, amenazas cibernéticas cada vez más sofisticadas, marcos regulatorios en constante evolución y dinámicas económicas globales que imponen nuevos retos.

La transformación digital, impulsada por el crecimiento acelerado del uso de tecnologías emergentes, ha cambiado profundamente la forma en que se generan, procesan y comparten los datos. Hoy en día, dispositivos interconectados, servicios en la nube, inteligencia artificial y el Internet de las Cosas (IoT) son elementos comunes en muchos sectores. Estos avances han generado mejoras notables en la eficiencia operativa y han abierto la puerta a modelos de negocio innovadores, pero al mismo tiempo han ampliado significativamente los posibles puntos de vulnerabilidad, haciendo que la exposición a ciberamenazas sea mayor que nunca. En este escenario, garantizar la seguridad de la información ya no es una opción, sino una condición esencial para proteger activos críticos y asegurar la continuidad operativa en un entorno digital que cambia constantemente (H. M. R. Zambrano, 2023).

En el plano internacional, la interconexión de sistemas e infraestructuras ha creado un contexto en el que las amenazas cibernéticas trascienden fronteras. Actualmente, tanto grupos criminales organizados como actores patrocinados por Estados desarrollan ataques con un alto grado de sofisticación. Estos ataques no solo buscan obtener información sensible, sino que en muchos casos apuntan a comprometer infraestructuras clave y alterar el funcionamiento de gobiernos, instituciones financieras y organizaciones esenciales. Como respuesta, distintos países han comenzado a reforzar sus políticas de seguridad digital y han promovido la cooperación a nivel internacional, lo cual se refleja en la creación de acuerdos y alianzas orientadas a enfrentar estos riesgos de forma coordinada y efectiva.

Al mismo tiempo, el panorama legal y normativo también ha evolucionado con rapidez.

La creciente preocupación por la privacidad y la integridad de la información ha motivado la implementación de leyes más estrictas, como el Reglamento General de Protección de Datos (GDPR) en Europa, y otras regulaciones similares en distintas regiones. Estas normativas no solo establecen reglas claras sobre cómo deben manejarse los datos, sino que también obligan a las organizaciones a adoptar una postura proactiva y responsable en cuanto a la gestión de la seguridad de la información. Este marco legal también está contribuyendo a consolidar una cultura organizacional basada en el respeto a la privacidad, la transparencia y la rendición de cuentas.

Desde una perspectiva económica, el fortalecimiento de la ciberseguridad se ha consolidado como una inversión estratégica indispensable. Tanto el sector público como el privado están destinando recursos considerables a la adquisición de soluciones tecnológicas, la formación de equipos especializados y la implementación de planes de respuesta ante incidentes. Esta tendencia obedece al entendimiento generalizado de que la seguridad de la información no solo protege contra pérdidas y daños, sino que también refuerza la reputación de las organizaciones, genera confianza en los clientes y aporta valor a largo plazo en un mundo cada vez más digitalizado. (Aguilar Antonio, 2021).

### 2.1.2 ANÁLISIS DE LA CIBERSEGURIDAD GLOBAL

La ciberseguridad continúa transformándose en un contexto marcado por amenazas cada vez más sofisticadas y persistentes. El informe **"State of Cybersecurity 2024"** publicado por ISACA, elaborado a partir de una encuesta global con la participación de profesionales del sector, proporciona una visión amplia y actualizada del panorama actual de riesgos. Este estudio recoge perspectivas de expertos provenientes de distintos sectores e industrias, ofreciendo así un diagnóstico integral de cómo las organizaciones están enfrentando los desafíos de seguridad en un entorno digital cada vez más hostil. (ISACA, 2024).

Uno de los hallazgos más significativos del informe es que **el 55% de las organizaciones reportaron un aumento en la cantidad de ciberataques** recibidos en comparación con el año anterior. Si bien esta cifra no representa un salto dramático en relación con reportes anteriores (62% en 2021 y 53% en 2023), sí confirma una tendencia sostenida al alza en la actividad maliciosa en línea. Por el contrario, únicamente un 12% de los encuestados manifestó haber experimentado una reducción en los ataques, lo que refuerza la urgencia de adoptar enfoques más sólidos en la

protección de los activos digitales.

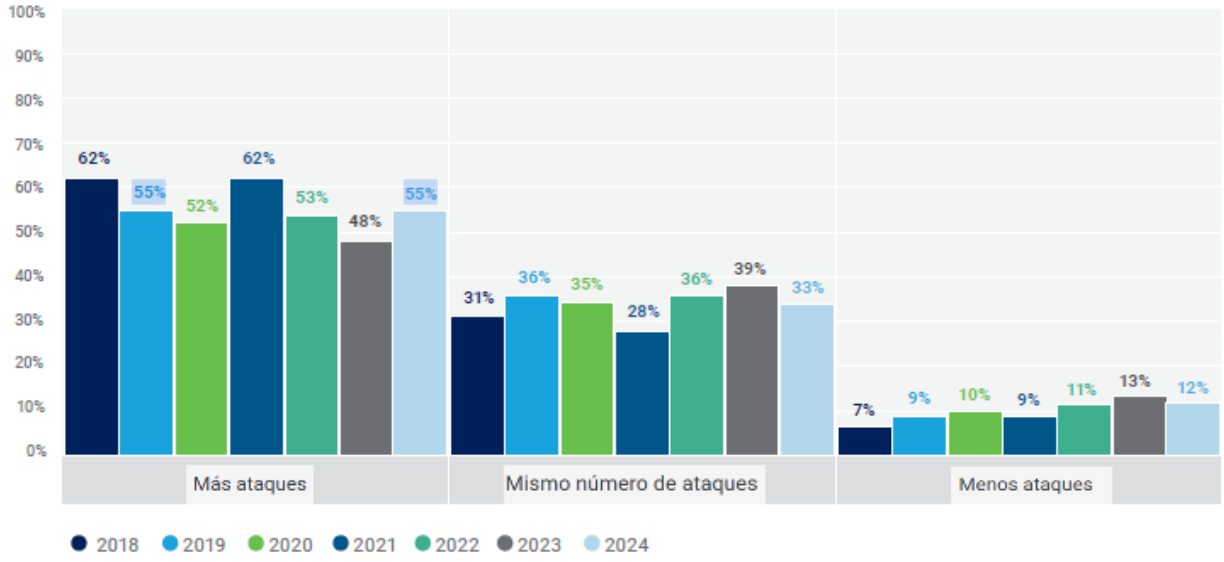



**Figura 2: Comparación de ataques cibernéticos**

Asimismo, el estudio revela que **una proporción considerable de profesionales considera probable que su organización sea víctima de un ataque durante el próximo año**. Esta percepción generalizada de vulnerabilidad evidencia que los ciberataques han dejado de ser una posibilidad remota y se han convertido en una constante dentro de la gestión de riesgos empresariales.

En cuanto a la capacidad de respuesta ante incidentes, los resultados muestran un panorama mixto. **Solo un 39% de los encuestados se sienten completamente o muy seguros respecto a la habilidad de sus equipos para detectar y responder a amenazas**, mientras que **un 16% expresa poca o ninguna confianza en esa capacidad**. Esta brecha sugiere que, a pesar del reconocimiento de los riesgos, muchas organizaciones aún enfrentan desafíos importantes para fortalecer su postura defensiva, especialmente en términos de detección temprana y capacidad de reacción oportuna.

Respecto a los responsables de los ataques, **los cibercriminales organizados continúan encabezando la lista (28%)**, seguidos por los **hackers individuales (20%)**. También destacan los **ataques patrocinados por Estados (13%)**, así como los **insiders maliciosos (12%)**, es decir, personas internas con intenciones dañinas. Por otro lado, los **insiders no maliciosos**, es decir, empleados que comprometen la seguridad sin intención deliberada, representaron solo un 9%,

disminuyendo en dos puntos porcentuales respecto a mediciones anteriores. Esta reducción podría estar relacionada con una mayor efectividad de las campañas de concienciación y formación interna en las organizaciones.

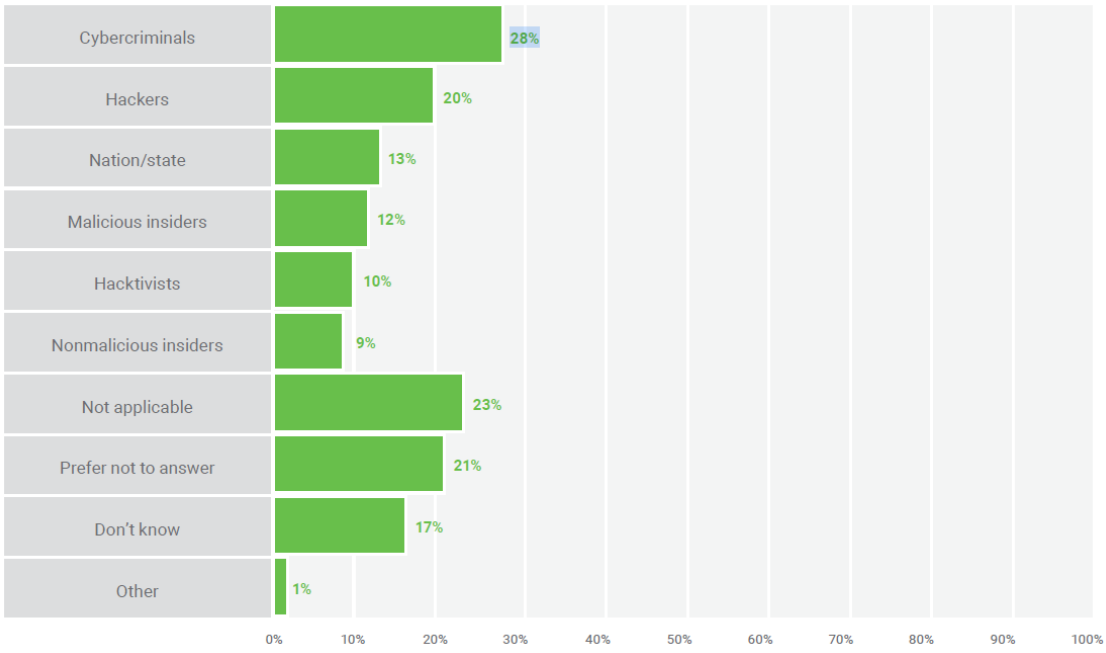



**Figura 3: Actores principales de ciberataques**

El vector de ataque predominante sigue siendo la ingeniería social, que aumentó cuatro puntos porcentuales (19%). Otros ataques frecuentes incluyen malware (13%), denegación de servicio (11%) y explotación de sistemas no parcheados (11%). Estos resultados destacan la importancia de las mejores prácticas de seguridad, como la gestión de parches y la educación de los usuarios para reducir la efectividad de los ataques basados en manipulación psicológica.

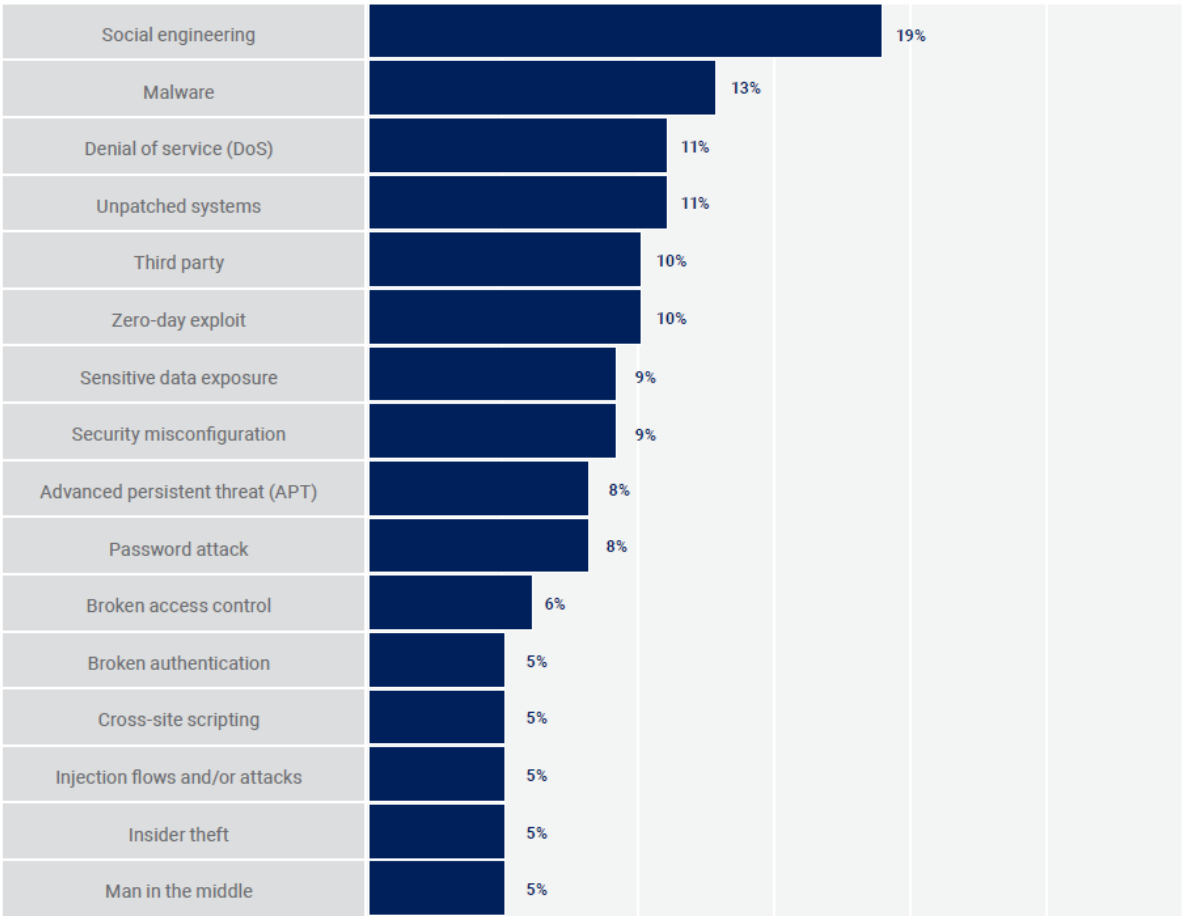



**Figura 4: Tipos de Ataques**

A nivel mundial, las organizaciones están adoptando diferentes estrategias para contrarrestar las amenazas emergentes. Entre las medidas más comunes se encuentran:

1. Automatización de la seguridad: Implementación de soluciones avanzadas de detección y respuesta automatizada para reducir el tiempo de mitigación.

2. Capacitación y concienciación: Programas de formación continua para empleados y directivos, reduciendo el impacto de ataques de ingeniería social.

3. Ciber inteligencia y monitoreo proactivo: Uso de herramientas de inteligencia de amenazas para anticipar y prevenir ataques antes de que ocurran.

4. Refuerzo de marcos regulatorios: Mayor alineación con normativas como GDPR, ISO 27001 y NIST para fortalecer la postura de seguridad.

### 2.1.3 EVOLUCIÓN DE AMENAZAS Y DESAFÍOS INTERNACIONALES

La evolución de las amenazas cibernéticas en las últimas décadas ha sido notable, pasando de ataques bastantes simples a operaciones altamente sofisticadas que representan desafíos significativos a nivel internacional. A continuación, se detallan algunos de los principales aspectos de esta evolución y los desafíos a los que nos enfrentamos:

#### 2.1.3.1 SURGIMIENTO Y SOFISTICACIÓN DE LAS AMENAZAS

- Durante la década de 1980, la ciberseguridad comenzó a tomar relevancia con la aparición de los primeros virus informáticos. Uno de los más conocidos fue el gusano **Morris**, que surgió en 1988 y logró propagarse rápidamente a través de las redes emergentes de la época. Este evento marcó un punto de inflexión, ya que evidenció por primera vez la vulnerabilidad de los sistemas interconectados, sentando las bases para la creación de herramientas y prácticas de protección digital más robusta (Manage Engine, 2024)
- En los años 2000, el panorama se volvió mucho más complejo. Surgieron formas de malware más sofisticadas, entre ellas **Stuxnet**, descubierto en 2010. Este código malicioso fue diseñado con un propósito específico: sabotear infraestructuras críticas, particularmente sistemas industriales. Su existencia demostró que los ciberataques podían ser utilizados como armas en conflictos internacionales, transformando la percepción global sobre el alcance y las implicaciones de las amenazas cibernéticas.
- Hoy en día, la ciberseguridad enfrenta desafíos sin precedentes debido a la proliferación de ataques avanzados y persistentes (APT), el auge del ransomware y la creciente explotación de vulnerabilidades en dispositivos del Internet de las Cosas (IoT). Estos vectores de ataque reflejan no solo un incremento en la frecuencia de los incidentes, sino también una sofisticación técnica cada vez mayor, lo que obliga a las organizaciones a adoptar enfoques más integrales y proactivos para proteger sus activos digitales y operativos.

#### 2.1.3.2 IMPACTO EN SECTORES ESTRATÉGICOS

- Uno de los sectores más sensibles frente a las amenazas cibernéticas es el **sector energético**. Debido a su papel estratégico en la infraestructura crítica de los países, los ataques dirigidos a este ámbito no solo provocan **pérdidas económicas considerables**,

sino que también pueden representar un riesgo directo para la seguridad nacional. Los incidentes en esta industria suelen tener un alto nivel de impacto, ya que afectan sistemas de control industrial y redes de distribución que requieren un funcionamiento continuo y seguro.

#### 2.1.3.3 DESAFÍOS INTERNACIONALES EN CIBERSEGURIDAD

La evolución constante de las amenazas cibernéticas, junto con los desafíos internacionales que estas implican, demanda una respuesta articulada y multidimensional. No basta con implementar soluciones aisladas; es necesario adoptar un enfoque integral que contemple la modernización de las infraestructuras tecnológicas, el fortalecimiento de la cooperación entre países y la formación continua de profesionales y usuarios en buenas prácticas de ciberseguridad. En este contexto, resulta esencial identificar y abordar una serie de desafíos clave que actualmente definen el panorama global de la seguridad de la información:

- **Crecimiento del cibercrimen organizado:** Las actividades delictivas en el ámbito digital han evolucionado significativamente, dando paso a redes criminales estructuradas que operan de forma similar a empresas legítimas. Grupos como LockBit, Conti y REvil han perfeccionado el modelo de *ransomware-as-a-service (RaaS),* lo que permite a individuos sin conocimientos técnicos avanzados lanzar ataques complejos mediante el alquiler de herramientas y servicios. Este fenómeno ha potenciado la frecuencia y gravedad de los ataques, especialmente en sectores estratégicos como el de la salud, la energía y los servicios financieros, generando interrupciones operativas críticas y pérdidas económicas de gran escala.

- **Vulnerabilidades en infraestructuras críticas:** Los sistemas que sostienen los servicios esenciales —como la energía, el transporte, la salud y las telecomunicaciones— se apoyan cada vez más en plataformas digitales interconectadas. Esta creciente dependencia tecnológica ha ampliado considerablemente la superficie de ataque. Un ejemplo alarmante ocurrió en 2023, cuando un ciberataque a una empresa de distribución eléctrica en Canadá provocó cortes de energía en múltiples provincias durante varias horas. Incidentes como este dejan en evidencia la necesidad urgente de fortalecer los mecanismos de protección en infraestructuras críticas y mejorar la capacidad de respuesta ante amenazas dirigidas

(El Periódico de la Energía, 2023).

- **Escasez de talento en ciberseguridad:** Uno de los obstáculos más frecuentes para combatir las amenazas digitales es la falta de profesionales capacitados. La demanda de talento especializado continúa superando ampliamente la oferta disponible en el mercado. Según estimaciones recientes, existen más de 4 millones de vacantes sin cubrir en el ámbito de la ciberseguridad a nivel global (ISC2, 2024). Esta brecha representa un riesgo considerable, ya que limita la capacidad de las organizaciones para prevenir, detectar y mitigar incidentes con eficacia. (ISC2, 2024).
- **Desarrollo de normativas y cumplimiento:** El endurecimiento de los marcos regulatorios en diferentes regiones del mundo ha obligado a las organizaciones a adoptar prácticas más rigurosas en la gestión de la seguridad de la información. Iniciativas como el Reglamento General de Protección de Datos (GDPR) en Europa, la Ley de Ciberseguridad de China y las regulaciones en Estados Unidos reflejan una tendencia hacia el fortalecimiento del cumplimiento normativo. Numerosas empresas de gran escala han enfrentado sanciones económicas por no adherirse a estos requerimientos, lo que ha motivado una mayor inversión en políticas de protección de datos y una cultura corporativa orientada a la gestión responsable del riesgo digital..

### 2.1.4 NORMATIVA INTERNACIONAL EN SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es un elemento fundamental para la protección de datos en organizaciones de todo el mundo. A medida que las amenazas cibernéticas evolucionan, también lo hacen las regulaciones y normativas internacionales para garantizar la integridad, disponibilidad y confidencialidad de la información.

Algunas de las normativas y marcos de referencia más importantes a nivel internacional incluyen:

- **Reglamento General de Protección de Datos (GDPR - General Data Protection Regulation)**: El Reglamento General de Protección de Datos (GDPR), vigente en la Unión Europea desde 2018, exige que las organizaciones obtengan el consentimiento explícito para el uso de datos personales. Establece derechos clave para los usuarios, como el derecho al olvido y la portabilidad de los datos, y obliga a las empresas a ser más

transparentes y responsables en el manejo de la información. (Europea, 2025).

- **Ley de Privacidad del Consumidor de California (CCPA - California Consumer Privacy Act)**: Esta ley, vigente desde 2020, se asemeja al GDPR, pero se enfoca en la protección de la privacidad de los consumidores en California. Otorga a los residentes de este estado el derecho de conocer qué información personal recopilan las empresas y cómo se usa.
- **Ley de Protección de Datos Personales en América Latina**: Países como Argentina, Brasil (con la LGPD - Lei Geral de Proteção de Dados), Chile, México y Colombia han desarrollado sus propias normativas de protección de datos, alineadas en gran parte con el modelo del GDPR (Antequera, 2023).

### 2.1.5 NORMA ISO/IEC 27001:2022 Y SUS REQUISITOS

La ISO/IEC 27001:2022 es un estándar internacional que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI). Su objetivo principal es ayudar a las organizaciones a gestionar de manera efectiva la seguridad de su información, protegiéndola contra riesgos como accesos no autorizados, alteraciones o pérdidas.

**Principales cambios respecto a la versión 2013**

La versión 2022 introduce actualizaciones clave para mejorar la alineación con los desafíos actuales de ciberseguridad. Algunos cambios relevantes incluyen:

- **Reducción del número de controles**: La cantidad de controles en el Anexo A se redujo de 114 (ISO 27001:2013) a 93, agrupados en 4 dominios en lugar de 14.
- **Nuevos controles:** Se añadieron 11 controles que abordan temas como inteligencia de amenazas, seguridad en la nube, prevención de fugas de información y monitorización de seguridad.
- **Mejora en la estructura de requisitos:** Se mantienen los principios de la gestión de riesgos, pero con un enfoque más adaptable a cada organización.

Texto La norma establece una serie de requisitos estructurados en 10 cláusulas principales:

**1. Alcance**

Define los límites y el contexto en el que se implementará el SGSI dentro de la

organización.

**2. Referencias normativas**

Se basa en ISO/IEC 27000, que proporciona términos y definiciones clave en seguridad de la información.

**3. Términos y definiciones**

Explica los conceptos clave utilizados en la norma.

**4. Contexto de la organización**

La empresa debe identificar factores internos y externos que puedan afectar su seguridad de la información y definir los interesados relevantes (empleados, clientes, proveedores, reguladores).

**5. Liderazgo**

La alta dirección debe demostrar compromiso con la seguridad de la información, estableciendo una política y asegurando la asignación de responsabilidades.

**6. Planificación**

Se requiere evaluar riesgos y oportunidades, definir objetivos de seguridad y establecer un plan de tratamiento de riesgos.

**7. Apoyo**

Incluye la gestión de recursos, competencias, formación, comunicación y documentación para la implementación efectiva del SGSI.

**8. Operación**

Implica la implementación de controles y procedimientos de seguridad definidos en el SGSI para gestionar los riesgos identificados.

**9. Evaluación del desempeño**

Se deben realizar auditorías internas y revisiones de la alta dirección para medir la eficacia del SGSI.

**10. Mejora continua**

Incluye acciones para corregir no conformidades, implementar mejoras y optimizar el SGSI con el tiempo.

### 2.1.6 HERRAMIENTAS PARA LA IMPLEMENTACIÓN DE UN SGSI

Para implementar un SGSI de manera efectiva, las organizaciones pueden apoyarse en herramientas especializadas que ayudan en la gestión de riesgos, monitoreo de seguridad, cumplimiento normativo y auditoría. A continuación, se presentan algunas de las herramientas más utilizadas en cada una de estas áreas:

#### 2.1.6.1 HERRAMIENTAS DE GESTIÓN DE RIESGOS

Estas herramientas permiten identificar, evaluar y gestionar riesgos de seguridad de la información.

- **ISO 27005 Risk Manager**: Facilita la gestión de riesgos alineada con la norma ISO 27005.
- **Metodología OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**: Método de análisis de riesgos desarrollado por el CERT de Carnegie Mellon.
- **FAIR (Factor Analysis of Information Risk)**: Marco de análisis de riesgos cuantitativo que complementa la ISO 27001.
- **RiskWatch**: Automatiza la identificación de riesgos y la aplicación de controles de seguridad.

#### 2.1.6.2 HERRAMIENTAS DE GESTIÓN DE DOCUMENTACIÓN Y CUMPLIMIENTO

- **ISMS.online**: Plataforma en la nube que facilita la documentación y certificación ISO 27001.
- **Conformio**: Proporciona plantillas, registros y guías para cumplir con ISO 27001.
- **LogicGate Risk Cloud**: Plataforma flexible para gestionar riesgos y cumplimiento normativo.
- **TrustCloud**: Ayuda en la automatización del cumplimiento de seguridad con certificaciones ISO 27001 y SOC 2.

#### 2.1.6.3 HERRAMIENTAS DE MONITOREO Y SEGURIDAD

Para asegurar el cumplimiento de la norma, es necesario contar con sistemas de monitoreo y detección de amenazas.

- **Splunk**: Permite la recolección, análisis y correlación de eventos de seguridad.
- **IBM QRadar**: Plataforma SIEM que detecta amenazas y facilita la respuesta a incidentes.
- **AlienVault OSSIM**: Herramienta de código abierto que integra múltiples funciones de seguridad.
- **ELK Stack (Elasticsearch, Logstash y Kibana)**: Analiza y visualiza logs de seguridad para la detección de incidentes.
    - Indicadores clave de desempeño (KPIs), dashboards y software de monitoreo para seguimiento de la eficacia de los controles. Herramientas como Power BI o Tableau para visualizar métricas de seguridad.

#### 2.1.6.4 HERRAMIENTAS DE AUDITORÍA Y EVALUACIÓN DE CONTROLES

Un SGSI debe ser auditado regularmente para evaluar su efectividad y detectar áreas de mejora.

- **GRC (Governance, Risk & Compliance) Tools**: Herramientas como RSA Archer o ServiceNow GRC permiten realizar auditorías y asegurar el cumplimiento.
- **Nessus**: Escáner de vulnerabilidades utilizado en auditorías de seguridad.
- **OpenVAS**: Alternativa de código abierto para la detección de vulnerabilidades.
- **CyberGRX**: Plataforma de evaluación de riesgos de terceros alineada con ISO 27001.
- **Sophos:** es una empresa líder en ciberseguridad que ofrece soluciones avanzadas para la protección de endpoints, redes, correos electrónicos y entornos en la nube, utilizando inteligencia artificial y monitoreo proactivo para detectar y responder a amenazas en tiempo real.

### 2.1.7 BENEFICIOS DE UN SGSI

La implementación de un **Sistema de Gestión de Seguridad de la Información (SGSI)** basado en la norma ISO/IEC 27001:2022 proporciona múltiples beneficios a las organizaciones al

mejorar la protección de sus activos de información y fortalecer la resiliencia ante amenazas cibernéticas. Entre los principales beneficios se encuentran:

- **Protección de la información**: Garantiza la confidencialidad, integridad y disponibilidad de los datos, minimizando riesgos de filtraciones o accesos no autorizados.
- **Cumplimiento normativo y legal**: Facilita la alineación con regulaciones internacionales y locales sobre seguridad de la información, privacidad y protección de datos.
- **Reducción de riesgos y amenazas**: Implementa controles y medidas de mitigación para prevenir incidentes de seguridad y minimizar su impacto.
- **Mejora de la confianza y reputación**: Refuerza la credibilidad ante clientes, socios y partes interesadas al demostrar un compromiso con la seguridad de la información.
- **Mayor eficiencia operativa**: Optimiza procesos internos mediante la gestión estructurada de la seguridad, reduciendo costos asociados a incidentes y brechas de datos.
- **Preparación ante incidentes**: Establece procedimientos de respuesta y recuperación que permiten actuar con rapidez y minimizar el impacto de un ataque cibernético.
- **Ventaja competitiva**: Diferencia a la organización en el mercado al adoptar estándares de seguridad reconocidos globalmente.(*ISO/IEC 27001*, 2022b).

### 2.1.8 MODELOS DE GESTIÓN Y PLANIFICACIÓN ESTRATÉGICA PARA SGSI

La implementación y mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI) requiere un enfoque estructurado basado en modelos de gestión y planificación estratégica que permitan su alineación con los objetivos del negocio y la mejora continua. A continuación, se presentan los principales modelos utilizados:

**Ciclo de Deming (PDCA) aplicado al SGSI**

El modelo Plan-Do-Check-Act (PDCA) es ampliamente utilizado en la gestión de un SGSI y está alineado con la norma ISO/IEC 27001:2022. Este enfoque permite la mejora continua y se desarrolla en cuatro fases:

- **Plan (Planificar):** Definir políticas, objetivos y análisis de riesgos para establecer el SGSI.
- **Do (Hacer):** Implementar controles y procedimientos de seguridad.

- **Check (Verificar):** Monitorizar y medir el desempeño del SGSI, evaluando incidentes y cumplimiento de objetivos.
- **Act (Actuar):** Tomar medidas correctivas y mejorar el sistema con base en los resultados obtenidos.

**Modelo de las Tres Líneas de Defensa**

Este modelo, promovido por el IIA (Institute of Internal Auditors), establece una estructura clara para la gestión de riesgos en seguridad de la información:

- **Primera línea:** Equipos operativos y de TI que implementan controles de seguridad.
- **Segunda línea:** Funciones de supervisión y cumplimiento que garantizan la aplicación de normativas.
- **Tercera línea:** Auditoría interna que evalúa la eficacia del SGSI de manera independiente.

**NIST Cybersecurity Framework (CSF)**

El **Marco de Ciberseguridad del NIST** proporciona un enfoque basado en cinco funciones esenciales:

1. **Identificar:** Evaluar activos, riesgos y vulnerabilidades.
2. **Proteger:** Aplicar controles y estrategias de mitigación.
3. **Detectar:** Implementar sistemas de monitoreo y respuesta temprana.
4. **Responder:** Establecer planes de acción ante incidentes.
5. **Recuperar:** Desarrollar estrategias de continuidad y restauración de sistemas.

**4. COBIT para la Gestión de Seguridad de la Información**

El modelo **COBIT (Control Objectives for Information and Related Technologies)** ofrece un marco de gobernanza que ayuda a integrar la seguridad de la información con la estrategia organizacional. Sus principios incluyen la alineación con los objetivos del negocio, la optimización de recursos y el cumplimiento normativo.

**ITIL y la Gestión de Servicios de Seguridad**

El enfoque **ITIL (Information Technology Infrastructure Library)** proporciona

mejores prácticas para la gestión de servicios de TI, incluyendo la seguridad de la información mediante procesos como:

- Gestión de incidentes y respuesta a amenazas.
- Evaluación de riesgos y continuidad del negocio.
- Control de cambios y mejora continua.

### 2.1.9 GESTIÓN DE RIESGOS

La gestión de riesgos en un Sistema de Gestión de Seguridad de la Información (SGSI) es un proceso fundamental para identificar, analizar y mitigar amenazas que puedan comprometer la confidencialidad, integridad y disponibilidad de la información. Este proceso implica la evaluación de vulnerabilidades, la estimación del impacto potencial y la implementación de controles adecuados para reducir los riesgos a niveles aceptables. La norma **ISO/IEC 27005** proporciona directrices para gestionar los riesgos de seguridad de la información, mientras que metodologías como **OCTAVE, NIST RMF y FAIR** permiten un análisis estructurado. Una gestión de riesgos efectiva no solo protege los activos críticos, sino que también fortalece la resiliencia organizacional frente a ciberataques y otras amenazas emergentes.

### 2.1.10 ESTUDIOS DE CASO Y COMPARATIVAS INTERNACIONALES

La implementación de la norma ISO/IEC 27001, referente en la gestión de la seguridad de la información, ha demostrado ser clave para varias organizaciones que buscan proteger sus activos de información y, a su vez, fortalecer su posición en el mercado. A continuación, se presentan dos casos de éxito de empresas que han adoptado esta norma internacional: Thames Security Shredding (TSS) y Fredrickson International.

**Fredrickson International: Transformación en la Gestión de la Información Sensible**

Fredrickson International es una empresa líder en el sector de la cobranza de deudas, que maneja grandes volúmenes de datos financieros y personales altamente sensibles. En un entorno donde la protección de esta información es crucial para mantener la confianza de sus clientes y cumplir con las normativas de privacidad, la compañía enfrentaba el desafío de demostrar que gestionaba eficazmente la seguridad de la información.

Con el objetivo de mejorar sus prácticas de seguridad y cumplir con las expectativas de sus

clientes, Fredrickson decidió implementar un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con los estándares de ISO/IEC 27001. La empresa llevó a cabo una exhaustiva evaluación de riesgos relacionados con la seguridad de la información, estableció políticas claras de seguridad y comenzó una serie de programas de capacitación para su personal.

Los resultados fueron contundentes. La certificación ISO/IEC 27001 permitió a Fredrickson ganar la confianza de sus clientes y facilitar la licitación para contratos más grandes, pues la certificación fue vista como un claro indicativo de que la empresa tomaba en serio la protección de la información. Además, el proceso contribuyó a la creación de una sólida cultura organizacional en torno a la seguridad, mejorando la protección de la información a lo largo de toda la empresa.

**Thames Security Shredding: Garantizando la Confidencialidad en la Destrucción de Documentos**

Por otro lado, Thames Security Shredding (TSS), una empresa especializada en la destrucción segura de documentos confidenciales se enfrentaba a un desafío similar. En su caso, los clientes requerían que la empresa demostrara un compromiso con la gestión de la seguridad de la información para asegurar que los documentos confidenciales fueran destruidos de manera segura y conforme a las normativas legales.

TSS decidió adoptar la norma ISO/IEC 27001 para fortalecer su sistema de gestión de seguridad. Implementaron un SGSI con base en los principios de la norma, lo que les permitió establecer procedimientos claros y rigurosos para la gestión de la seguridad de la información. Además, realizaron auditorías internas para asegurar que el sistema estuviera siempre en cumplimiento con los más altos estándares.

La certificación ISO/IEC 27001 brindó a TSS una ventaja competitiva significativa en el mercado. No solo cumplieron con los requisitos contractuales de sus clientes, sino que la certificación también les permitió destacarse como un proveedor confiable en un sector donde la seguridad de la información es un factor crítico. Esto les permitió atraer nuevos clientes y aumentar su volumen de negocio, consolidándose como líderes en su industria (BSI, 2011).

## 2.2 MICROENTORNO

### 2.2.1 IMPACTO DE LA CIBERSEGURIDAD EN HONDURAS Y CENTRO AMÉRICA

Centroamérica ha experimentado un crecimiento en la adopción de tecnologías digitales en los últimos años, impulsado por la transformación digital en sectores clave como la banca, las telecomunicaciones y el comercio electrónico. Sin embargo, este avance ha estado acompañado de un aumento significativo en la cantidad y sofisticación de los ciberataques, que han puesto en riesgo la información y la operatividad de múltiples instituciones.

Uno de los factores que agrava la vulnerabilidad de la región es la falta de inversión en infraestructura de ciberseguridad y la limitada legislación en materia de delitos informáticos. Según el Global Cybersecurity Index, (*NCSI :: Ranking*, 2023), varios países centroamericanos, incluyendo Honduras, El Salvador y Nicaragua, ocupan posiciones bajas en términos de preparación y respuesta ante incidentes cibernéticos.

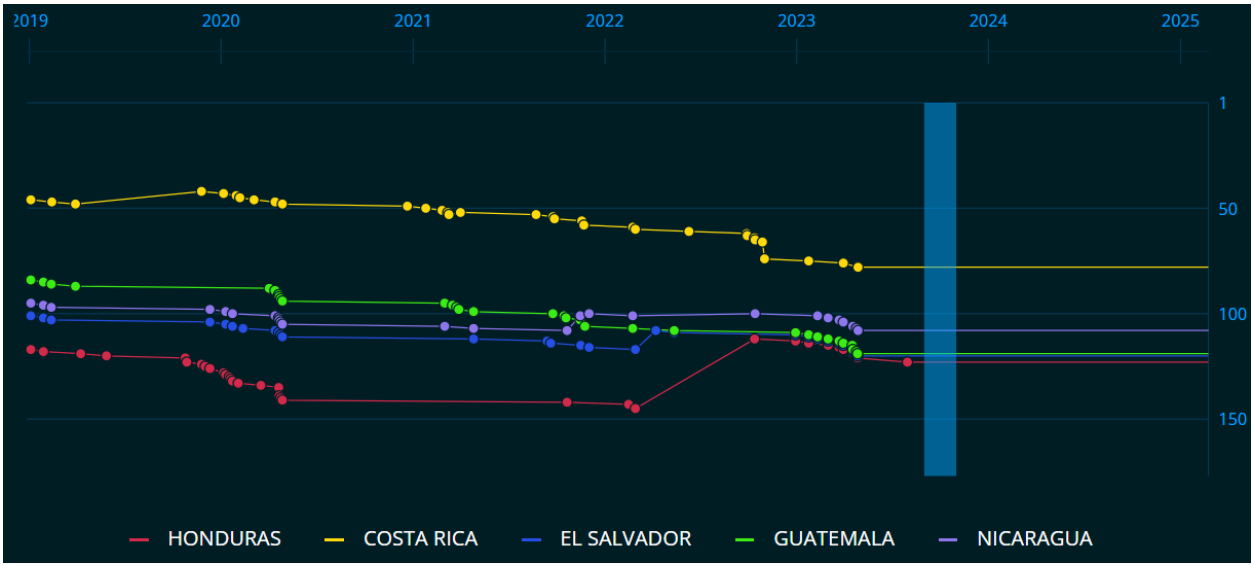



**Figura 5: Clasificación de Ciberseguridad en Centroamérica**

Nota: Adaptado de (*NCSI :: Compare*.)

La imagen muestra una gráfica de la clasificación de ciberseguridad en los países de Centroamérica desde 2019 hasta 2025. Se identifican cinco países:

Honduras (rojo), Costa Rica (amarillo), El Salvador (azul), Guatemala (verde) y Nicaragua

(morado)

Costa Rica ha mantenido una posición relativamente alta en el ranking, con una ligera tendencia descendente en los últimos años. El Salvador, Guatemala y Nicaragua han mantenido posiciones cercanas entre sí, con fluctuaciones. Honduras ha estado en una posición más baja en comparación con los demás países y ha mostrado una mejoría en los últimos años. Los principales tipos de ataques que afectan a la región incluyen:

- **Ataques de ransomware**, donde los ciberdelincuentes secuestran datos y exigen pagos en criptomonedas.
- **Ataques de phishing**, dirigidos tanto a individuos como a instituciones financieras.
- **Ataques de denegación de servicio (DDoS)**, que buscan desestabilizar la infraestructura digital de bancos y empresas de telecomunicaciones.
- **Explotación de vulnerabilidades en infraestructura crítica**, como sistemas gubernamentales y redes de telecomunicaciones.

Uno de los eventos más relevantes en términos de ciberseguridad en la región fue el ataque sufrido por Claro Centroamérica en 2024. Claro es uno de los principales proveedores de servicios de telecomunicaciones en la región, con millones de usuarios en países como Honduras, Guatemala, El Salvador y Nicaragua.

El incidente, que se reportó a principios de 2024, involucró una brecha de seguridad que permitió a los atacantes acceder a información sensible de clientes y sistemas internos. Se sospecha que el ataque fue perpetrado por un grupo de ciberdelincuentes con motivaciones financieras. (Barrera, 2024)

Según un informe de Frost & Sullivan, se proyecta que el mercado de servicios de ciberseguridad gestionada en América Latina alcanzará los 1.708 millones de dólares en 2024, lo que representa un crecimiento del 12,8% respecto al año anterior. En este contexto, Centroamérica contribuye con 130,5 millones de dólares en inversiones en ciberseguridad para el mismo año.

Dentro de la región, Panamá y Guatemala lideran en términos de crecimiento del mercado de ciberseguridad. Panamá muestra un incremento del 34% en 2024, alcanzando ingresos de 51,2 millones de dólares, mientras que Guatemala registra un crecimiento del 31%, con ingresos de 39,8 millones de dólares. Por su parte, Honduras experimenta un crecimiento del 12%, totalizando

ingresos de 10,4 millones de dólares en el sector de ciberseguridad. (Revista EyN, 2024)

### 2.2.2 NORMATIVA HONDUREÑA EN CIBERSEGURIDAD

Según el National Cyber Security Index, Honduras se ubica en la posición 122 a nivel mundial en términos de ciberseguridad (*NCSI :: Ranking*, 2023) . Esta clasificación refleja desafíos significativos en la implementación de medidas efectivas para proteger la infraestructura digital y los datos sensibles en el país.

Según un artículo publicado en Innovare: Revista de Ciencia y Tecnología, Honduras actualmente carece de los elementos esenciales requeridos en el Índice Mundial de Ciberseguridad. Entre estos elementos se incluyen la legislación criminal en materia de delitos informáticos, regulaciones y mecanismos de cumplimiento, la existencia de un centro de respuesta a incidentes cibernéticos, la adopción oficial de estándares internacionales, así como requerimientos de certificación para entidades y profesionales en el ámbito de la ciberseguridad. (Centeno, 2018).

**Tabla 1: Índice mundial de ciberseguridad y perfiles de ciber bienestar – Honduras**

| Pilares del reporte del estado de ciberseguridad | ¿Cumple requerimientos? |
|---|---|
| **1.Medidas legales** | |
| 1.1 Legislación criminal | No |
| 1.2 Regulación y cumplimiento | No |
| **2. Medidas técnicas** | |
| 2.1 Centro de respuesta a incidentes | No |
| 2.2 Marco estándar de ciberseguridad | No |
| 2.3 Requerimientos de certificación y acreditación | No |
| **3. Medidas organizacionales** | |
| 3.1 Política de ciberseguridad | No |
| 3.2 Mapa de ruta para gobernabilidad de ciberseguridad | No |
| 3.3 Agencia oficial responsable para ciberseguridad | No |
| 3.4 Estadísticas y medidas oficiales para comparaciones | No |
| **4. Construcción de capacidades** | |

| | |
|---|---|
| 4.1 Estándares oficiales de ciberseguridad, mejores prácticas | No |
| 4.2 Desarrollo profesional de alto nivel en ciberseguridad | No |
| 4.3 Cuantificación de profesionales certificados internacionalmente | No |
| 4.4 Agencias certificadas en materia de ciberseguridad | No |
| **5. Cooperación** | |
| 5.1 Marco oficial de trabajo para cooperación a nivel estatal | No |
| 5.2 Marco oficial de trabajo para cooperación a nivel de agencias | No |
| 5.3 Patrocinio para compartir ciberseguridad entre entes públicos y privados | No |
| 5.4 Cooperación Internacional | Sí |

Nota: Adaptado de (Centeno, 2018)

### 2.2.3 SITUACIÓN ACTUAL DE LEYDE EN SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se ha convertido en un elemento esencial para empresas y organizaciones en la era digital actual. La protección de datos confidenciales, la prevención de amenazas cibernéticas y el cumplimiento de regulaciones son aspectos críticos para garantizar la integridad y confidencialidad de la información.(Perez, 2024). En el caso de LEYDE, se han realizado avances significativos en la adopción de tecnologías para fortalecer su infraestructura; sin embargo, aún existen oportunidades de mejora en la formalización de políticas y procedimientos alineados con estándares internacionales como la ISO/IEC 27001:2022.

LEYDE ha migrado sus aplicaciones principales a la nube, lo que ha permitido contar con una infraestructura más robusta y escalable. Adicionalmente, se han instalado dispositivos de seguridad perimetral, como firewalls avanzados, para controlar y monitorear el tráfico de la red. Para mitigar los riesgos asociados a ataques cibernéticos, la empresa ha implementado diversas herramientas de seguridad, incluyendo software antivirus, protección de capa DNS y autenticación multifactor (MFA). Estas iniciativas representan un paso importante en la protección de la información, aunque es necesario complementarlas con un enfoque integral basado en la gestión de riesgos y el cumplimiento normativo (*ISO/IEC 27001*, 2022b).

Actualmente, LEYDE cuenta con lineamientos y procedimientos básicos relacionados con

la gestión de accesos, tales como la creación de usuarios en sistemas y el uso de contraseñas. Asimismo, se han establecido restricciones para el acceso no autorizado a dispositivos de almacenamiento extraíbles (USB) y la navegación en sitios web no permitidos. No obstante, estos procedimientos carecen de formalización en políticas documentadas que aborden de manera estructurada todos los aspectos clave de la seguridad de la información, lo que representa una brecha en el cumplimiento de estándares internacionales.

Actualmente, LEYDE no cuenta con una certificación bajo la norma ISO/IEC 27001:2022, lo que evidencia la necesidad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Si bien se han adoptado medidas de protección, estas no están alineadas con un marco de referencia que garantice su efectividad y mejora continua. La ausencia de una estrategia formal para la gestión de la seguridad de la información puede representar un riesgo para la organización en términos de confidencialidad, integridad y disponibilidad de los datos (*ISO/IEC 27001*, 2022b).

Si bien se han implementado controles técnicos y algunos procedimientos operativos, la principal brecha radica en la falta de un marco formal de políticas y procedimientos que aborde de manera integral la seguridad de la información. La norma ISO 27001 proporciona un marco integral para que las organizaciones gestionen y protejan sus datos confidenciales y otra información, reduciendo el riesgo de violaciones de datos, ciberataques y otros incidentes de seguridad.(IBM, 2024b)

### 2.2.4 RELEVANCIA DEL SGSI EN LEYDE

LEYDE ha identificado la necesidad de fortalecer la seguridad de la información dentro de la organización, asegurando la confidencialidad, integridad y disponibilidad de sus activos digitales. La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 permitirá establecer un marco estructurado para la protección de la información, minimizando riesgos y garantizando el cumplimiento de estándares internacionales.

### 2.2.5 IMPACTO ORGANIZACIONAL Y CULTURAL DE LA IMPLEMENTACIÓN DE UN SGSI

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en

LEYDE no solo transformará los procesos internos, sino que también influirá profundamente en la cultura organizacional. Adoptar un SGSI fomenta una mentalidad colectiva orientada hacia la seguridad de la información, la responsabilidad compartida y la mejora continua, aspectos esenciales para enfrentar las crecientes amenazas cibernéticas.

Integrar un SGSI según la norma ISO/IEC 27001:2022 implica establecer políticas y procedimientos claros que promuevan prácticas seguras en toda la organización. Este enfoque integral alienta a todo el personal a comprender los riesgos asociados con los activos de información y a adoptar medidas preventivas en sus actividades diarias. Según (López, 2023), un SGSI proporciona un marco que no se limita al área de TI, sino que abarca a toda la organización, mejorando la cultura empresarial en términos de seguridad.

La eficacia de un SGSI depende en gran medida de la concienciación y formación de los empleados. Programas de capacitación regulares aseguran que el personal esté al tanto de las políticas de seguridad y de cómo aplicarlas en su trabajo diario. El Instituto Nacional de Ciberseguridad (INCIBE) destaca que la formación en ciberseguridad crea una cultura de seguridad en la empresa, estableciendo las bases para proteger la información confidencial de la organización y de sus clientes y proveedores. (INCIBE, 2022).

Es natural que la introducción de un SGSI enfrente cierta resistencia al cambio por parte de los empleados. Para mitigar este desafío, es crucial involucrar a todo el personal desde las etapas iniciales del proyecto, comunicando claramente los beneficios y proporcionando formación adecuada. Según (Cano, 2021), comprender la dinámica de la cultura organizacional es esencial para implementar cambios efectivos en seguridad de la información, ya que implica abordar comportamientos, actitudes y valores arraigados en la organización.

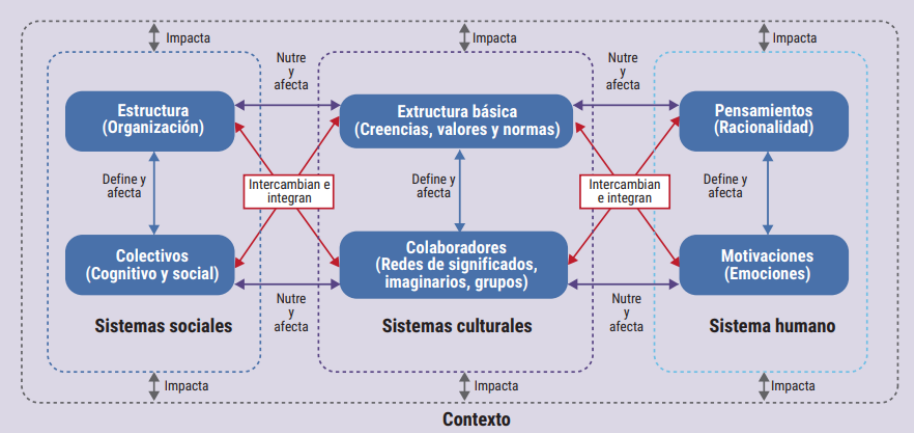



**Figura 6: Perspectiva sistémica de articulación de sistemas sociales, culturales y humanos**

Nota: Adaptado de (Cano, 2021)

### 2.2.6 EVALUACIÓN DE RECURSOS NECESARIOS PARA LA IMPLEMENTACIÓN DE UN SGSI EN LEYDE

Para implementar de manera exitosa un Sistema de Gestión de Seguridad de la Información (SGSI) en LEYDE, es fundamental contar con una adecuada asignación de recursos humanos, técnicos y financieros. Esta asignación no solo influye en la capacidad de la organización para gestionar de manera efectiva los riesgos, sino que también determina el grado de madurez y resiliencia ante amenazas cibernéticas.

#### Recursos Humanos

La implementación de un SGSI en LEYDE depende en gran medida de la disponibilidad de personal capacitado en el área de la ciberseguridad. La escasez de expertos en seguridad es un problema reconocido a nivel global, lo que dificulta la creación de inteligencia en seguridad corporativa y aumenta la vulnerabilidad ante brechas que pueden ocasionar daños significativos.

Un informe de (Kaspersky Lab, 2016) evidencia que la falta de experiencia en seguridad es un problema real para las corporaciones. Según este estudio, realizado mediante una encuesta a más de 4,000 representantes de empresas de diversas industrias, el 33 % de las compañías a nivel mundial considera esencial invertir en mejorar la experiencia de sus expertos en seguridad. Además, aproximadamente la mitad de las empresas encuestadas admitió la existencia de una notable escasez de talento, lo cual agrava la demanda de especialistas en ciberseguridad.

El informe destaca que el campo de la ciberseguridad exige competencias muy

especializadas: curiosidad, capacidad autodidacta y un conocimiento profundo y multidisciplinario, cualidades que no se adquieren de manera casual. Esto significa que la contratación de personal calificado en este ámbito resulta un desafío, y muchas veces las empresas deben recurrir a estrategias como la externalización de ciertos servicios o la inversión en programas de formación continua para superar esta brecha.

Para LEYDE, reconocer y abordar esta limitación es fundamental para la implementación exitosa del SGSI. Es necesario evaluar la capacidad actual del equipo, identificar las áreas en las que se requieren nuevos conocimientos y, en caso de ser necesario, contratar especialistas o recurrir a servicios externos que complementen la expertise interna. Esta inversión en recursos humanos garantizará que la organización pueda gestionar de manera efectiva los riesgos y responder de forma ágil ante posibles incidentes de seguridad.

**Recursos Técnicos**

La infraestructura tecnológica necesaria para un SGSI abarca tanto hardware como software. Es indispensable contar con:

- Herramientas para el monitoreo y la detección de incidentes de seguridad, como firewalls, sistemas de detección de intrusos y soluciones de autenticación multifactor.
- Plataformas de gestión de vulnerabilidades y riesgos, que permitan una evaluación continua y la implementación de medidas correctivas oportunas.
- Soluciones que faciliten la integración y centralización de la información, asegurando la interoperabilidad entre diferentes sistemas y procesos internos.

**Recursos Financieros**

La organización debe contar con los recursos financieros necesarios para invertir en su SGSI. Esto incluye los costos de contratación y capacitación del personal, compra y mantenimiento de la infraestructura e implementación de controles de seguridad. (DataGuard, 2023)

La implementación y el mantenimiento de un SGSI requieren de una inversión financiera que cubra:

- La adquisición y actualización de tecnologías y equipos necesarios.

- Programas de capacitación y formación continua para el personal.
- Servicios de consultoría externa y auditorías periódicas que garanticen el cumplimiento de los estándares internacionales, como la ISO/IEC 27001:2022.

## 2.3 TEORÍAS DE SUSTENTO

### 2.3.1 CUARTA REVOLUCIÓN INDUSTRIAL

La Cuarta Revolución Industrial, conocida también como Industria 4.0, representa una transformación radical en la forma en que las empresas operan, integrando de manera sinérgica tecnologías digitales, físicas y biológicas. Según Peralta Abarca, Martínez Bahena y Enríquez Urbano (2020), esta revolución se fundamenta en la convergencia de sistemas ciberfísicos, el Internet de las Cosas (IoT), el Big Data y la inteligencia artificial, lo que permite la automatización integral y la optimización de los procesos productivos.

Esta transformación tecnológica implica la creación de "fábricas inteligentes", donde la interconexión de dispositivos y sistemas posibilita la recolección y análisis en tiempo real de datos críticos para la toma de decisiones. La integración de sensores y software de recolección de datos facilita no solo la automatización de tareas, sino también la identificación y corrección de ineficiencias en las cadenas de producción. De este modo, la Industria 4.0 no solo mejora la eficiencia operativa y reduce costos, sino que también permite a las empresas adaptarse rápidamente a las demandas del mercado global.

Además, Peralta Abarca et al. (2020) destacan que la Cuarta Revolución Industrial conlleva un cambio cultural y organizacional, exigiendo una actualización constante en las competencias del capital humano. La transformación digital demanda una capacitación continua y la adopción de nuevos modelos de gestión que integren la tecnología en todos los niveles de la organización, promoviendo la innovación y la mejora continua. Este enfoque integral es crucial para que las empresas se mantengan competitivas y resilientes ante los retos de un entorno cada vez más digitalizado.

**Tabla 2: Evolución de la industria 1.0 a la industria 4.0**

| Versión | Nombre | Innovación | Características |
|---|---|---|---|
| 1.0 | Primera revolución industrial | Talleres mecánicos (1874) | Entre los siglos XVIII y XIX, apoyada en la introducción de equipos de producción mecánicos impulsados por agua y vapor. |
| 2.0 | Segunda revolución industrial | Líneas de producción transportadoras (1870) | En el siglo XX, basada en la producción en masa gracias al concepto de división de tareas y el uso de energía eléctrica. |
| 3.0 | Tercera revolución industrial | Controladores lógicos programables (1969) | Final del siglo XX, debido al uso de la electrónica y la informática en los procesos, permitiendo automatizar algunas tareas repetitivas en las líneas de producción. |
| 4.0 | Cuarta revolución industrial | Sistemas ciberfísicos e internet de las cosas (actualmente) | Comenzó a principios del siglo XXI, gracias a los avances tecnológicos de la mano del internet. La "cuarta revolución industrial" trae consigo las "fábricas inteligentes", fundamentada en el uso de sistemas de información, recolección de datos y el internet de las cosas. |

Nota: Adaptado de (Peralta Abarca et al., 2020)

En el contexto de este proyecto, que propone la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 en LEYDE, la Industria 4.0 juega un papel fundamental, ya que el aumento en la digitalización y la automatización de los procesos empresariales conlleva mayores desafíos en la gestión de la seguridad de la información.

La implementación del SGSI no solo fortalecerá la seguridad de la información en LEYDE, sino que también impulsará una cultura organizacional basada en la mejora continua y la capacitación del personal, alineándose con la necesidad de innovación y resiliencia en la era digital.

Este proyecto se enmarca en el contexto de la Cuarta Revolución Industrial, abordando los desafíos que trae consigo la digitalización en términos de seguridad de la información. La adopción de la norma ISO/IEC 27001:2022 en LEYDE permitirá gestionar los riesgos asociados a la transformación tecnológica, garantizando un entorno seguro y eficiente para la operación de la empresa en un mercado cada vez más competitivo y digitalizado.

### 2.3.2 NORMAS ISO

La Organización Internacional de Normalización (ISO), fundada en 1947, es una entidad global encargada de desarrollar estándares voluntarios para garantizar calidad, seguridad y eficiencia en productos y servicios (*ISO - Organización Internacional de Normalización*, 2025). Estos estándares, basados en consensos multilaterales, buscan reducir barreras comerciales y promover la interoperabilidad técnica. Entre sus principios clave destacan el enfoque en el cliente, la mejora continua (basada en el ciclo PDCA) y la gestión de riesgos.

Las normas ISO surgieron en un contexto posguerra para estandarizar procesos industriales. En la década de 1980, la ISO 9001 (1987) marcó un hito al enfocarse en sistemas de gestión de calidad (SGC). Posteriormente, en los 90, la ISO 14001 (1996) abordó la gestión ambiental. La ISO 27001, publicada en 2005, adaptándose a los desafíos de la seguridad de la información. Sus actualizaciones más relevantes incluyen:

- **ISO 27001:2013:** Introdujo un enfoque flexible para la evaluación de riesgos y mayor alineación con otros estándares (*ISO/IEC 27001*, 2013)
- **ISO 27001:2022:** Actualizó los controles de seguridad, incorporando temas como ciberseguridad en la nube y teletrabajo (*ISO/IEC 27001*, 2022b) .

La implementación de la ISO/IEC 27001 permite a las organizaciones establecer un proceso estructurado y medible para la gestión de la seguridad de la información. La norma promueve la identificación y evaluación de riesgos, la implementación de controles adecuados y la realización de auditorías internas para asegurar el cumplimiento normativo. En este sentido, las normas ISO han evolucionado de ser simples guías de buenas prácticas a convertirse en herramientas estratégicas que impulsan la innovación y la mejora continua en la gestión de la seguridad.

## 2.4 METODOLOGÍAS APLICADAS

### 2.4.1 ISO 27001: CICLO PDCA (PLAN-DO-CHECK-ACT)

#### 2.3.3.1 Definición

El Ciclo PDCA (Plan-Do-Check-Act) es un modelo de gestión utilizado para la mejora continua de procesos en diversas áreas, incluyendo la gestión de calidad, TI, seguridad y negocios.

Se basa en cuatro fases interdependientes: Planificar (Plan), donde se identifican problemas, se analizan causas y se establecen objetivos con un plan de acción; Hacer (Do), que implica la ejecución de las actividades planificadas en un entorno controlado o a pequeña escala; Verificar (Check), donde se evalúan los resultados obtenidos comparándolos con las expectativas y métricas establecidas, identificando desviaciones o áreas de mejora; y Actuar (Act), que consiste en estandarizar los procesos exitosos, corregir errores y aplicar mejoras antes de reiniciar el ciclo para una optimización continua. (Martins, 2024)

Este enfoque, desarrollado por Walter Shewhart y popularizado por W. Edwards Deming, es ampliamente utilizado en metodologías como ITIL, Lean, Six Sigma, COBIT y DevOps, ya que permite una gestión iterativa, basada en datos, con énfasis en la eficiencia y la mitigación de riesgos. Su flexibilidad lo convierte en una herramienta clave en organizaciones que buscan incrementar la calidad, reducir desperdicios y mejorar la toma de decisiones estratégicas mediante la retroalimentación constante y la adaptación progresiva de sus procesos. (Culture, 2024).

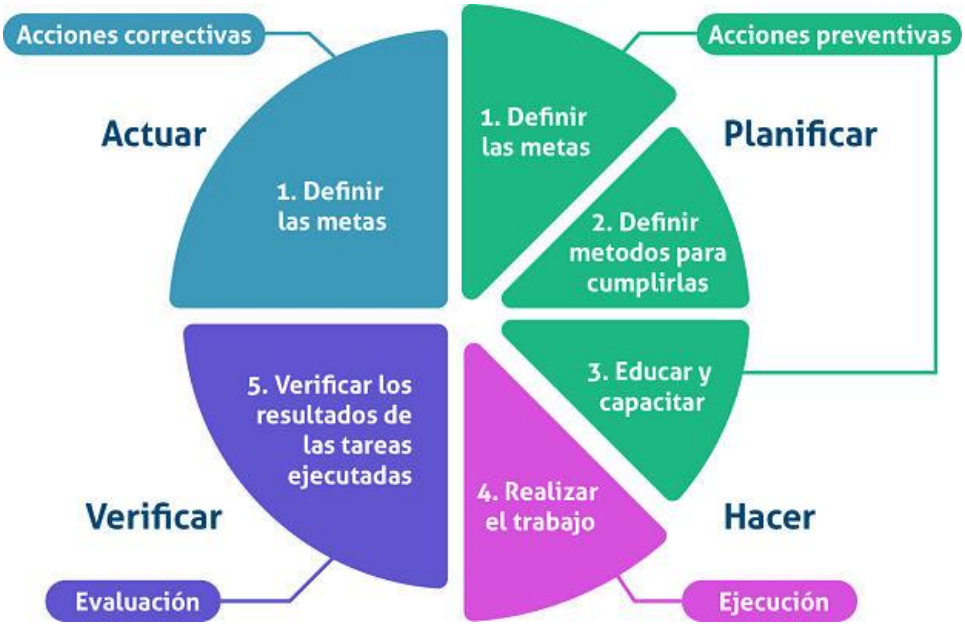



**Figura 7: Fases del Ciclo PDCA**

#### 2.3.3.2 Antecedentes

El Ciclo PDCA (Plan-Do-Check-Act) tiene sus orígenes en el trabajo del estadístico estadounidense Walter A. Shewhart en la década de 1930, quien desarrolló un modelo de control de calidad basado en la observación y mejora continua de procesos. Sin embargo, fue W. Edwards

Deming, uno de los principales impulsores de la gestión de calidad en Japón después de la Segunda Guerra Mundial, quien popularizó y perfeccionó el modelo, convirtiéndolo en un pilar fundamental para la gestión empresarial y la mejora continua. En Japón, su aplicación permitió la evolución del Toyota Production System (TPS) y el enfoque Lean Manufacturing, que hoy en día son modelos de referencia para la eficiencia operativa en múltiples industrias. Con el tiempo, el PDCA ha sido adoptado en gestión de calidad (ISO 9001), ITIL, COBIT, Lean, Six Sigma, DevOps y Agile, consolidándose como una metodología universal para la optimización de procesos. (EXCELENCIA, 2020).

#### 2.3.3.3 Aplicación al proyecto

El ciclo PDCA se aplicará en el proyecto para estructurar y gestionar de forma sistemática la implementación del SGSI en LEYDE. Específicamente:

1. Plan (Planificar): Esta fase consiste en establecer el alcance del SGSI, definir la política de seguridad de la información, identificar los activos críticos, evaluar los riesgos de seguridad y diseñar controles para mitigarlos.
2. Do (Hacer): Se implementan los controles definidos en la fase de planificación. Esto incluye la aplicación de medidas técnicas y organizativas, como autenticación multifactorial, cifrado de datos, gestión de accesos y capacitación del personal. También se documentan los procesos y se realizan pruebas para garantizar que los controles sean efectivos en la protección de la información. (Ardanza, 2022)
3. Check (Verificar): Se monitorea el desempeño del SGSI mediante auditorías internas, revisión de logs de seguridad, análisis de eventos y pruebas de penetración. Se comparan los resultados con los objetivos de seguridad establecidos, identificando brechas o áreas de mejora.
4. Act (Actuar o Ajustar): Se toman acciones correctivas y preventivas con base en los hallazgos de auditorías y análisis de riesgos. Se ajustan los controles, se refuerzan políticas de seguridad y se mejora la capacitación del personal. Además, se revisan y actualizan los procedimientos para garantizar que el SGSI continúe evolucionando y respondiendo a nuevas amenazas (SYDLE, 2023).

**Tabla 3: Tabla Resumen, Fases PDCA ISO 27001**

| Fase | Descripción | Aplicación en ISO 27001 |
|---|---|---|
| Plan (Planificar) | Se establecen políticas, objetivos y controles de seguridad basados en el análisis de riesgos. | Identificar riesgos con ISO 27005 y seleccionar controles del Anexo A. |
| Do (Hacer) | Se implementan los controles de seguridad definidos en la fase de planificación. | Aplicar autenticación multifactor, cifrado de datos y gestión de accesos. |
| Check (Verificar) | Se monitorea el SGSI mediante auditorías, análisis de eventos y revisiones de seguridad. | Realizar auditorías internas y pruebas de penetración para evaluar la efectividad de los controles. |
| Act (Actuar o Ajustar) | Se aplican mejoras y correcciones en función de los hallazgos de auditoría y análisis de riesgos. | Ajustar políticas de seguridad, mejorar la capacitación y actualizar controles. |

## 2.4.2 METODOLOGÍA OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION)

### 2.3.3.4 Definición

La metodología OCTAVE corresponde a las siglas Operational Critical, Threat, Asset and Vulnerability Evaluation (evaluación operativa crítica, de amenazas, de activos y de vulnerabilidad). Esta metodología se enfoca en el análisis y gestión de riesgos con el propósito de garantizar la seguridad de los sistemas informáticos dentro de una organización.

La aplicación de la metodología OCTAVE implica la participación conjunta de profesionales de diferentes áreas, incluyendo negocios, tecnologías de la información y operaciones. Este trabajo colaborativo tiene como objetivo abordar las necesidades de seguridad de manera integral, asegurando un equilibrio entre los riesgos operativos, la tecnología y las prácticas de seguridad (Cruz, 2021).

### 2.3.3.5 Antecedentes

El Software Engineering Institute (SEI) ha publicado diversas versiones de la metodología OCTAVE a lo largo de los años, desde su primera edición en el año 2000. Las principales versiones actuales son:

**OCTAVE 2.0:** Diseñada para empresas con más de 300 empleados, infraestructura propia y estructura organizacional multinivel. Requiere la capacidad de ejecutar herramientas de

identificación de vulnerabilidades e interpretar sus resultados. Esta versión establece procedimientos, guías, catálogos y entrenamientos aplicables a distintos niveles organizacionales (estratégico, táctico y operativo). Además, considera la tecnología que respalda los activos gestionados, alineando la organización en torno a estos para identificar amenazas, vulnerabilidades y riesgos, desarrollando así planes de mitigación efectivos. El levantamiento de información se basa en workshops.

**OCTAVE-S:** Dirigida a organizaciones pequeñas (menos de 100 empleados). También consta de tres fases, pero a diferencia de OCTAVE 2.0, no requiere workshops para la recopilación de información. Se asume que el equipo ejecutor tiene un conocimiento detallado de los activos, sus requerimientos de seguridad y las amenazas que enfrenta la organización.

**OCTAVE Allegro:** Pensada para grupos que desean evaluar riesgos sin un gran involucramiento organizacional ni la necesidad de contar con expertos en todos los activos.

**OCTAVE FORTE:** La versión más reciente, enfocada en la gestión de riesgos operacionales dentro de la empresa. Adopta una visión holística del riesgo, integrando la ciberseguridad con el resto del portafolio de riesgos organizacionales. (Fernández et al., 2021)

#### 2.3.3.6 Aplicación al proyecto

La metodología OCTAVE se utilizó en el proyecto para identificar y evaluar de forma integral los activos críticos, vulnerabilidades y amenazas asociadas a la seguridad de la información en LEYDE. Específicamente para:

- Identificar los activos y procesos críticos: Nos ayudó a mapear y clasificar los elementos clave que requieren protección, permitiendo una visión clara de la infraestructura y los recursos críticos de la organización.
- Evaluar riesgos y priorizar acciones: Mediante el uso de matrices de riesgo y talleres de evaluación, la metodología OCTAVE resolvió la problemática de determinar qué riesgos son más significativos y, por lo tanto, deben abordarse con prioridad.
- Desarrollar estrategias de mitigación: Facilitó la formulación de planes de acción concretos y adaptados a las necesidades de LEYDE, lo que nos permitirá implementar controles efectivos para reducir la exposición a amenazas.

- Fomentar la participación y el conocimiento interno: Al involucrar a diversos actores de la organización en el proceso de identificación y evaluación de riesgos, contribuirá a la creación de una cultura de seguridad y al fortalecimiento del conocimiento interno en temas de ciberseguridad.

### 2.4.3 PMBOK COMO METODOLOGÍA

La Guía PMBOK® establece un marco de referencia que integra las mejores prácticas en la gestión de proyectos y, al mismo tiempo, se adapta a sus necesidades específicas. Para ello, presenta un conjunto de procesos destinados a planificar, ejecutar y controlar el proyecto, organizados en áreas de conocimiento que garantizan el logro de los objetivos planteados.

Según la sección 1.4.2.1 de la Guía PMBOK®, "el ciclo de vida del proyecto debe ser lo suficientemente flexible para afrontar la diversidad de factores presentes en el mismo". En esencia, los proyectos evolucionan conforme se dispone de información más detallada y precisa. Esta capacidad de adaptación resulta especialmente valiosa en entornos caracterizados por un alto nivel de cambio e incertidumbre, o donde los interesados manejan interpretaciones y expectativas muy variadas (*PMBOK Guide | Project Management Institute*, 2021).


**Figura 8: Ciclo de Vida del Proyecto**

La guía PMBOK será fundamental para llevar paso a paso la implementación del SGSI en LEYDE, desde arrancar con una buena definición del alcance hasta cerrar el proyecto con las lecciones aprendidas, pasando por la planificación detallada, la ejecución controlada y el seguimiento de riesgos y calidad; así, tengo se tendrá una guía clara para coordinar recursos, comunicar avances y ajustar el rumbo cuando cambian las necesidades o surgen nuevos desafíos, de manera que la norma ISO/IEC 27001:2022 se cumpla al pie de la letra y el sistema de seguridad realmente responda a lo que la empresa necesita.

En la fase de Iniciación del proyecto SGSI en LEYDE se levantará el acta de constitución y se mapearán los interesados clave desde la alta gerencia hasta los responsables de TI para garantizar que todos compartan una visión común de los objetivos de seguridad; durante la Planificación definiremos el alcance de las políticas y controles, elaboraremos el cronograma de actividades, estimaremos costos y prepararemos el plan de tratamiento de riesgos, de modo que cada recurso y esfuerzo apunte a cumplir los requisitos de la ISO/IEC 27001:2022; en la Ejecución pondremos en marcha las actividades previstas instalación de herramientas, capacitación y despliegue de controles gestionando eficientemente los equipos y proveedores; el Monitoreo y Control nos permitirá seguir el avance mediante indicadores de desempeño y auditorías internas, ajustando en tiempo real las respuestas a incidentes o brechas detectadas; y, finalmente, en Cierre formalizaremos la entrega del SGSI, documentaremos las lecciones aprendidas y estabilizaremos los procesos para que LEYDE disponga de un sistema de seguridad robusto, alineado con sus metas operativas y listo para evolucionar.

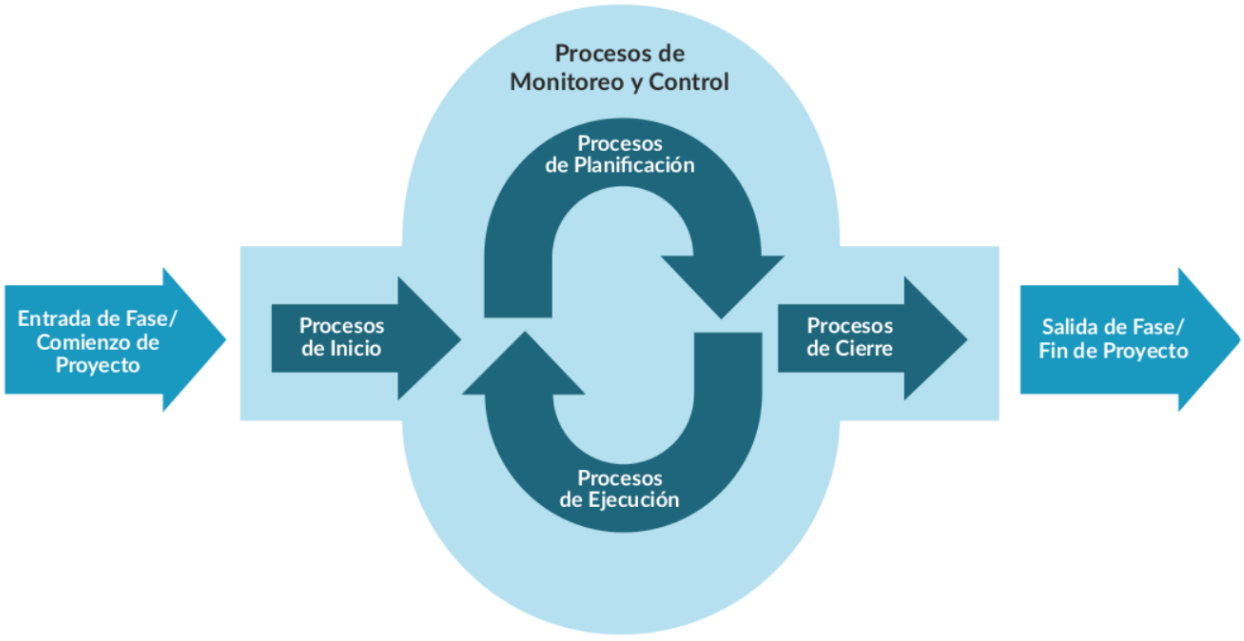



**Figura 9: Procesos de la dirección de proyectos**

En el proyecto de implementación del SGSI en LEYDE, además de los cinco grupos de procesos (Iniciación, Planificación, Ejecución, Monitoreo y Control, Cierre), estos se organizan en diez Áreas de Conocimiento que aseguran una gestión integral y alineada con ISO/IEC 27001:2022.

1. Gestión de la integración del proyecto
2. Gestión del alcance del proyecto
3. Gestión del cronograma del proyecto
4. Gestión de los costos del proyecto
5. Gestión de la calidad del proyecto
6. Gestión de los recursos del proyecto
7. Gestión de las comunicaciones del proyecto
8. Gestión de los riesgos del proyecto
9. Gestión de las adquisiciones del proyecto
10. Gestión de los interesados del proyecto

Cada una de estas áreas de conocimiento ofrece un marco universal, válido para cualquier iniciativa sin importar su sector, tamaño o enfoque metodológico, y se adapta perfectamente al proyecto de implementación del SGSI basado en ISO/IEC 27001:2022 en LEYDE. Gracias a ellas, el equipo cuenta con pautas claras para planificar, ejecutar, monitorear y controlar cada fase hasta su cierre. Al seguir la Guía PMBOK, se organiza el trabajo de forma coherente, se minimizan los riesgos de seguridad y se maximizan las probabilidades de éxito en la adopción de un sistema de gestión de la información sólido y alineado con los objetivos de la empresa.

## 2.5 INSTRUMENTOS UTILIZADOS

### 2.5.1 HERRAMIENTAS DEL CICLO PDCA.

**Fase Planificar:**

- **Análisis de riesgos y evaluación:** Matrices de riesgos, análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas).
- **Planificación de acciones:** Diagramas de flujo de procesos, cronogramas y software de gestión de proyectos.

**Fase Hacer:**

- **Implementación de controles:** Listas de verificación (checklists), manuales de procedimientos y documentación de políticas de seguridad. Herramientas de Seguridad: Firewalls (FortiGate).
- **Capacitación:** Programas y módulos de formación para el personal, talleres y seminarios. Cursos en línea (KnowBe4) para entrenar empleados en seguridad.

**Fase Verificar:**

- **Auditorías y revisiones:** Auditorías internas, revisiones periódicas y evaluaciones de cumplimiento mediante cuestionarios y auditorías de sistemas. Listas de Verificación (Checklists): Basadas en los requisitos de ISO 27001

**Actuar:**

- **Planes de acción correctiva:** Herramientas para el seguimiento y la actualización de medidas, y registros de acciones de mejora continua. Software de Gestión de Incidentes: Herramientas como Jira Service Management para rastrear acciones correctivas.

### 2.5.2 HERRAMIENTAS DE LA METODOLOGÍA OCTAVE.

**Matriz de activos y priorización:**

Tablas o matrices para listar activos (ej.: datos, sistemas, procesos) y clasificarlos según su criticidad operativa (ej.: impacto en la confidencialidad, integridad o disponibilidad).

**Matrices de impacto y probabilidad:**

Gráficos o tablas para evaluar el impacto operacional de una amenaza y su probabilidad de ocurrencia. Ejemplo: Matriz de calor (heatmap) con ejes de "impacto" vs. "probabilidad".

**Herramientas de evaluación técnica:**

Software como Nessus, OpenVAS o Qualys para escanear vulnerabilidades técnicas en sistemas.

**Plataformas de gestión de proyectos:**

Herramientas como Trello, Jira o Microsoft Planner para asignar tareas de mitigación y dar seguimiento.

### 2.5.3 HERRAMIENTAS DEL PMBOK.

Las herramientas que se emplearán para aplicar la metodología PMBOK en la implementación del SGSI basado en ISO/IEC 27001:2022 en LEYDE son:

- **Acta de Constitución del Proyecto**: Formaliza el arranque del SGSI, definiendo objetivos de seguridad específicos (alcance, recursos y responsables) y autorizando los recursos necesarios.
- **Matriz de Riesgos:** Permite identificar, analizar y priorizar las amenazas y vulnerabilidades propias de los activos de LEYDE, facilitando la planificación de respuestas según criterios de OCTAVE y los requerimientos de ISO 27001.
- **Cronograma del Proyecto:** Diagrama de Gantt que visualiza las actividades clave (levantamiento de brechas, diseño de controles, formación y auditorías internas), sus dependencias y duraciones, para asegurar el cumplimiento de plazos y la coordinación con otras áreas.
- **Registro de Interesados:** Inventario de todos los stakeholders desde la alta dirección hasta usuarios finales y proveedores de tecnología con su nivel de influencia e interés, para gestionar eficientemente la comunicación y el compromiso durante todo el ciclo de vida del SGSI.
- **EDT (Estructura de Desglose del Trabajo):** Descomposición jerárquica de las entregas del SGSI (políticas, procedimientos, herramientas y capacitaciones), facilitando la asignación de tareas y la estimación de recursos necesarios para cada paquete de trabajo.
- **Diccionario de la EDT:** Descripción detallada de cada componente de la EDT, incluyendo criterios de aceptación, responsables y recursos asignados, garantizando claridad en las actividades y entregables.
- **Plan de Gestión del Cronograma:** Documento que especifica cómo se definirán, supervisarán y controlarán las fechas del SGSI, incluyendo técnicas de estimación, niveles de precisión y herramientas de software para el seguimiento.

## 2.6 CONCEPTUALIZACIÓN

**La Seguridad de la Información:** se refiere a la práctica de proteger la información y los sistemas de información contra accesos no autorizados, uso, divulgación, interrupción, modificación o destrucción. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de los datos.

**Amenazas Cibernéticas**: son acciones o eventos que pueden comprometer la seguridad de los sistemas de información. Estas amenazas pueden ser intencionadas, como ataques dirigidos por ciberdelincuentes, o no intencionadas, como errores humanos o fallos técnicos. La identificación y comprensión de estas amenazas son fundamentales para desarrollar estrategias de defensa efectivas y proteger la infraestructura de información de una organización (IBM, 2024c).

**La ISO/IEC 27001:2022:** es una norma internacional que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Esta norma adopta un enfoque basado en la gestión de riesgos y está diseñada para garantizar que las organizaciones implementen controles de seguridad adecuados y proporcionados. La norma sigue la estructura de alto nivel (HLS) común a otras normas de sistemas de gestión, facilitando su integración con estándares como ISO 9001 (gestión de la calidad) e ISO 14001 (gestión ambiental). La certificación según ISO/IEC 27001:2022 demuestra el compromiso de una organización con la seguridad de la información y proporciona confianza a clientes y partes interesadas sobre la protección de sus datos. (consulting, 2024)

**Sistema de Gestión de Seguridad de la Información (SGSI)**: es un enfoque sistemático para gestionar información sensible, que abarca políticas, procedimientos y controles diseñados para mitigar riesgos y garantizar la seguridad de la información. La implementación de un SGSI permite a las organizaciones identificar amenazas, evaluar riesgos y aplicar medidas de seguridad adecuadas, alineándose con las mejores prácticas y normativas internacionales (Disterer, 2013).

**Herramientas de Gestión de Documentación y Cumplimiento:** son soluciones tecnológicas que facilitan la administración y organización de documentos relacionados con políticas, procedimientos y registros de seguridad. Estas herramientas aseguran que la documentación esté actualizada, sea accesible y cumpla con las normativas aplicables, permitiendo a las organizaciones demostrar su conformidad y gestionar eficientemente sus procesos de seguridad (Ayerdi, 2024).

**Auditoría y Evaluación de Controles**: implica la revisión sistemática de los controles de seguridad implementados para garantizar su eficacia y adecuación. Este proceso puede ser interno o externo y busca identificar deficiencias, asegurar el cumplimiento con políticas y normativas, y recomendar mejoras. Una auditoría efectiva es esencial para mantener la confianza en el SGSI y asegurar la protección continua de la información (Rodríguez, 2023).

**El ciclo PDCA (Planificar-Hacer-Verificar-Actuar):** es una metodología de mejora continua utilizada en la gestión de procesos, incluyendo la seguridad de la información. Este enfoque iterativo permite a las organizaciones planificar acciones, implementarlas, verificar su eficacia y actuar sobre los resultados para optimizar continuamente sus sistemas de gestión. (Culture, 2024).

**Metodología OCTAVE:** es una metodología de análisis y gestión de riesgos enfocada en la seguridad informática empresarial. Requiere la colaboración de distintas áreas para equilibrar riesgos operativos, tecnología y prácticas de seguridad. (Cruz, 2021).

**Metodologías Ágiles:** permite desarrollar proyectos con rapidez y flexibilidad, adaptándose a las necesidades del cliente. Divide el trabajo en partes iterativas, ajustándose sobre la marcha mediante feedback constante, sin requerir un alcance definido desde el inicio.(Nelson, 2024).

**Gestión de Riesgo**: en seguridad de la información implica identificar, evaluar y tratar riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información. Este proceso sistemático permite a las organizaciones priorizar recursos y aplicar controles adecuados para mitigar riesgos, alineándose con su apetito de riesgo y objetivos estratégicos (Certification & Webmaster, 2021).

**Normativas en Ciberseguridad**: son conjuntos de directrices, leyes y estándares diseñados para proteger la información y los sistemas informáticos contra amenazas cibernéticas. Estas normativas, como el Reglamento General de Protección de Datos (GDPR) o la Ley de Protección de Datos Personales, establecen requisitos que las organizaciones deben cumplir para asegurar la protección de datos y la privacidad de los usuarios (GlobalSuite, 2021).

**Vulnerabilidades**: son debilidades o fallos en sistemas, aplicaciones o procesos que pueden ser explotados por amenazas para comprometer la seguridad de la información. La

identificación y gestión de vulnerabilidades son esenciales para prevenir incidentes de seguridad y mantener la integridad de los sistemas de información (Daniels, 2023).

**Amenaza**: es cualquier elemento o acción que pueda comprometer la seguridad de la información. Surge de la existencia de vulnerabilidades y puede afectar un sistema, incluso si no se concreta un ataque. El avance de la ingeniería social, la falta de capacitación y la rentabilidad de los ataques han incrementado las amenazas intencionales. (*Amenazas a la Seguridad de la Información | Departamento de Seguridad Informática*, 2024).

**Activo de Información:** Los activos, según ISO 27001, son los recursos clave para el funcionamiento y cumplimiento de los objetivos de una empresa. En un proyecto de seguridad, se protegen los activos del dominio en estudio, considerando sus relaciones con el entorno.(Toro, 2015).

**Confidencialidad**: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

**Integridad**: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

**Disponibilidad**: acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

**Control de Acceso:** es un mecanismo de seguridad que regula quién puede acceder a datos, aplicaciones y recursos, así como en qué condiciones. Funciona de manera similar a las claves y listas de invitados en un entorno físico, asegurando que solo las personas autorizadas puedan ingresar a los espacios digitales. (*¿Qué es Access Control?*, 2024)

## 2.7 MARCO LEGAL

### 2.7.1 MARCO LEGAL INTERNACIONAL

**Tabla 4: Regulaciones Internacionales Aplicables**

| Regulación / Ley | Última Actualización | Artículos Claves | Relevancia |
|---|---|---|---|
| ISO/IEC 27001:2022 | 2022 | Cláusulas 4-10 | Estándar global para implementar un SGSI.<br>Base para controles de seguridad.<br>Cláusula 4: Contexto de la organización.<br>Cláusula 5: Liderazgo<br>Cláusula 6: Planificación<br>Cláusula 7: Apoyo<br>Cláusula 8: Funcionamiento<br>Cláusula 9: Evaluación del rendimiento.<br>Cláusula 10: Mejora |
| GDPR (UE 2016/679) | 2018 | Art. 5, 25, 32 | Aplica si se procesan datos de ciudadanos de la UE. Exige privacidad y seguridad.<br>ARTÍCULO 5: Principios relativos al tratamiento de datos personales.<br>ARTÍCULO 25: Protección de datos desde el diseño y por defecto.<br>ARTÍCULO 32: Seguridad del procesamiento. |
| Convenio de Budapest | 2001 | Art. 2-6 | Referencia contra ciberdelitos.<br>ARTÍCULO 2: Acceso ilícito<br>ARTÍCULO 3: Interceptación ilícita.<br>ARTÍCULO 4: Ataques a la integridad de los datos.<br>ARTÍCULO 5: Ataques a la integridad del sistema.<br>ARTÍCULO 6: Abuso de los dispositivos |

Fuente: (*ISO/IEC 27001*, 2022b), (*General Data Protection Regulation (GDPR) – Legal Text*, 2018), (*Convention on Cybercrime - Cybercrime - Www.Coe.Int*, 2001)

### 2.7.2 MARCO LEGAL EN HONDURAS

**Tabla 5: Regulaciones Nacionales Aplicables**

| Regulación / Ley | Última Actualización | Artículos Claves | Relevancia |
|---|---|---|---|
| Constitución de la República | 2021 (reforma) | Art. 76, 182 | Garantiza derechos a la intimidad y secreto de comunicaciones. ARTÍCULO 76. Se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen. ARTÍCULO 182. Toda persona tiene el derecho de acceso a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o suprimirla. No podrá afectarse el secreto de las fuentes de información periodística. |
| Ley de Comercio Electrónico (Decreto 149-2014) | 2014 | Art. 17, 23 | Regula seguridad en transacciones electrónicas y validez de documentos digitales. ARTÍCULO 17. El destinatario tiene derecho a considerar, que cada Mensaje de Datos recibido es un Mensaje de Datos diferente y a actuar en consecuencia salvo en la medida en que duplique otro Mensaje de Datos y que el destinatario sepa, o debería saberlo, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que era un duplicado. ARTÍCULO 23. Cuando se conceda algún derecho a una persona determinada y a ninguna otra, o ésta adquiera alguna obligación y la Ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío o la utilización, de un documento, ese requisito queda satisfecho si el derecho o la obligación se transfiere mediante la utilización de uno o más Mensajes de Datos, siempre que se emplee un método confiable para garantizar la singularidad de ese Mensaje de Datos. |

Fuente: (*Constitución de la República de Honduras*, 2021), (*Ley sobre Comercio Electrónico*, 2014)

Honduras enfrenta desafíos significativos en materia de privacidad y derechos digitales, lo que lo posiciona en una situación de vulnerabilidad frente a las amenazas cibernéticas y a posibles violaciones de derechos fundamentales en línea. Un informe reciente del International Center for Not-for-Profit Law (ICNL) expone que, si bien el país cuenta con algunas leyes en esta materia, muchas de ellas no cumplen con los estándares internacionales de protección de derechos humanos y están orientadas hacia la censura y el control estatal. Además, no se cuenta con una ley integral de protección de datos personales en el entorno digital ni ciberseguridad, dejando a las y los

ciudadanos vulnerables a la explotación y uso inadecuado de sus datos. (INCL, 2024).

El Congreso Nacional de Honduras está trabajando en la creación de un paquete de leyes destinadas a la protección de datos y la ciberseguridad. Entre las propuestas destacan la firma electrónica, la ley de ciberseguridad y la ley de protección de datos personales, todas orientadas a mitigar los riesgos derivados de delitos cibernéticos como el robo de identidad, el fraude financiero y la extorsión digital (La Prensa, 2023).

# CAPÍTULO III. METODOLOGÍA DE LA INVESTIGACIÓN

## 3.1 ENFOQUE

El enfoque de esta investigación está basado en el Método de Investigación Mixto (cualitativo-cuantitativo). Por un lado, se recolectarán datos cuantificables que permitan medir el estado actual de la seguridad de la información en LEYDE, y por otro, se aplicarán técnicas cualitativas (como entrevistas y análisis documental) para comprender los procesos, percepciones y necesidades relacionadas con la implementación del SGSI basado en la norma ISO/IEC 27001:2022.

El enfoque mixto adoptado en esta investigación presenta una predominancia cualitativa, ya que la implementación de un SGSI en LEYDE exige interpretar requisitos normativos (ISO/IEC 27001:2022), analizar procesos organizacionales mediante entrevistas a actores clave (equipos de TI, gerentes) y evaluar contextos operativos para diseñar una propuesta adaptada. No obstante, se integran elementos cuantitativos para cuantificar brechas de cumplimiento (ej. porcentaje de controles no implementados) y estimar recursos financieros o técnicos requeridos.

Según (Hernández Sampieri et al., 2014) la metodología de la investigación puede abordarse desde tres enfoques: cuantitativo, cualitativo y mixto. El enfoque cuantitativo se caracteriza por el uso de estadísticas, la prueba de hipótesis y el análisis de causa-efecto. En contraste, el enfoque cualitativo profundiza en los fundamentos, extrae significados a partir de los datos y no se basa en la estadística. Finalmente, el enfoque mixto combina elementos de ambos enfoques, permitiendo una integración de métodos para un análisis más completo.

## 3.2 ALCANCE

El enfoque de esta investigación es de carácter mixto, ya que combina elementos cualitativos y cuantitativos para obtener una visión más integral del estado actual del Sistema de Gestión de Seguridad de la Información en LEYDE.

Desde el enfoque cualitativo, el estudio es exploratorio, orientado a analizar los requisitos de la norma ISO/IEC 27001:2022, identificar metodologías recomendadas y comprender el contexto organizacional de LEYDE. Este análisis permite abrir nuevas perspectivas y detectar oportunidades de mejora en la gestión de la seguridad de la información.

Desde el enfoque cuantitativo, el estudio es descriptivo, ya que incluye la recolección de datos mediante encuestas aplicadas a colaboradores estratégicos. Esto permite medir variables como el porcentaje de controles de seguridad no implementados, el tiempo estimado para cerrar brechas identificadas y los costos asociados a recursos técnicos y humanos.

Según (Hernández Sampieri et al., 2014) señalan que los estudios descriptivos permiten detallar características de un fenómeno, mientras que los exploratorios abren caminos para soluciones prácticas, lo que coincide con los objetivos de diagnóstico y propuesta del proyecto.

## 3.3 DISEÑO

### 3.3.1 POBLACIÓN

La población objetivo del estudio está conformada por los empleados de LEYDE que, por la naturaleza de sus funciones, tienen relación directa con la gestión, manejo y protección de la información. Esto incluye personal del área de Tecnología de la Información (TI), gerentes de áreas estratégicas, y colaboradores que, por el alcance de sus responsabilidades, manejan datos sensibles o críticos. Esta población, identificada como clave para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), representa un subconjunto de los 92 empleados que integran la empresa.

Según Creswell (2014) y otros referentes en metodología de investigación, la definición precisa de la población es esencial para asegurar que los hallazgos sean aplicables al fenómeno estudiado. En este caso, se delimitó la población a aquellos empleados estratégicos con funciones vinculadas directamente a la seguridad de la información, ya que su perspectiva es fundamental para el análisis.

También se consideraron como parte del objeto de estudio cuatro documentos institucionales, incluyendo políticas internas de LEYDE, que contienen lineamientos sobre el manejo de la información.

### 3.3.2 MUESTRA

Para este estudio se utilizó una muestra no probabilística, de tipo intencional, compuesta por 15 colaboradores estratégicos seleccionados con base en criterios de:

- Relevancia funcional en la organización.

- Acceso y responsabilidad sobre información sensible.
- Participación directa en la gestión tecnológica y de procesos críticos.

La muestra incluyó personal del área de TI, gerentes de departamentos clave, y otros colaboradores con responsabilidad sobre la confidencialidad, integridad y disponibilidad de la información. Estos perfiles fueron considerados idóneos para brindar una visión completa y especializada sobre el estado actual de la seguridad de la información en LEYDE

Además, se complementó la información con el análisis de 4 documentos institucionales relevantes.

La selección se orientó a representar a los actores clave para el éxito de un SGSI, sin pretender generalizar los resultados a la totalidad de la empresa, sino profundizar en la perspectiva de quienes tienen mayor impacto en la gestión de la información."(Hernández Sampieri et al., 2014) .

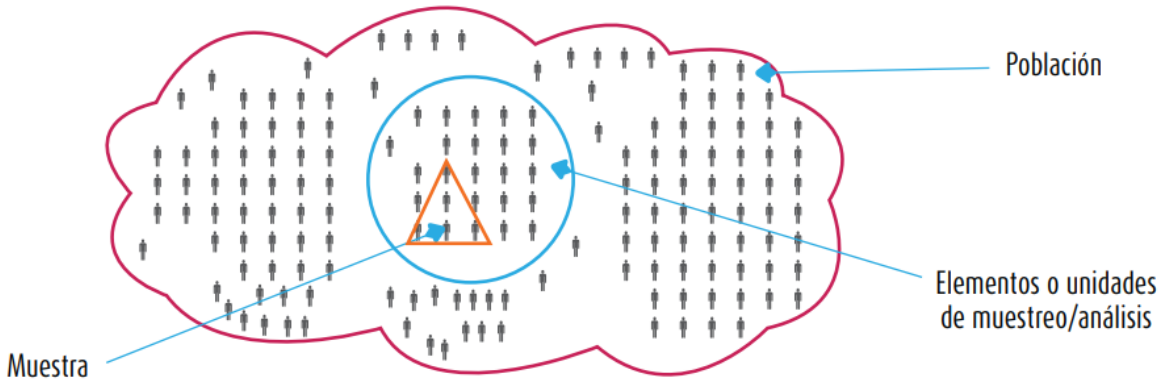



**Figura 10: Representación de una muestra como subgrupo**

### 3.3.3 TÉCNICAS DE MUESTREO

Para la selección de los participantes se emplearán técnicas de muestreo no probabilístico, específicamente el muestreo intencional o dirigido, y muestreo por conveniencia para acceder a documentos críticos.

**Muestreo Intencional o Dirigido:** Esta técnica se basa en la selección de participantes que poseen características específicas relevantes para los objetivos del estudio. Se emplea cuando es fundamental obtener información detallada de personas con conocimientos o experiencias

particulares sobre el fenómeno de interés (Coyne, 1997).

**Muestreo por Conveniencia:** Este método consiste en elegir a los participantes que se encuentran más fácilmente disponibles y están dispuestos a colaborar en el estudio. Aunque puede generar sesgos, resulta útil para obtener información de manera rápida y accesible (Etikan et al., 2016).

## 3.4 CRITERIOS DE SELECCIÓN DE LA MUESTRA

**Tabla 6: Criterios de Selección de la Muestra para el Estudio del SGSI en LEYDE**

| Criterios de Inclusión | Criterios de Exclusión |
|---|---|
| Empleados con acceso a datos sensibles. | Empleados sin vinculación o conocimiento en procesos de seguridad de la información. |
| Colaboradores con experiencia en áreas de TI, auditoría, y seguridad | Personal con menos de seis meses de vinculación en la empresa (poca experiencia organizacional) |
| Responsables y tomadores de decisiones en temas de gestión de la información. | Colaboradores que no estén autorizados a proveer información sobre procesos internos. |
| Documentos vigentes relacionados con seguridad. | Documentos obsoletos o no oficiales. |
| Áreas con historial de incidentes de seguridad. | Áreas sin impacto en la gestión de información. |

## 3.5 OPERACIONALIZACIÓN DE LAS VARIABLES

**Tabla 7: Operacionalización de variables**

| Variable | Dimensión | Indicadores | Instrumentos de Medición |
|---|---|---|---|
| **Implementación de un SGSI basado en ISO/IEC 27001:2022** | Gestión de Seguridad de la Información | Existencia de políticas y procedimientos de seguridad | Entrevistas, revisión documental |
| | | Nivel de cumplimiento de la norma ISO/IEC 27001:2022 | Lista de verificación, encuestas |
| | | Grado de concienciación y capacitación del personal | Encuestas, entrevistas |
| **Estado actual de la seguridad de la información en LEYDE** | Políticas y controles actuales | Documentación y aplicación de políticas de seguridad | Revisión documental, entrevistas |
| | Concienciación del personal | Nivel de conocimientos en seguridad de la información | Encuestas, observación |

| | | | |
|---|---|---|---|
| | Brechas de seguridad | Vulnerabilidades identificadas en auditorías internas | Informes de auditoría, listas de verificación |
| **Recursos para la implementación del SGSI** | Recursos humanos | Disponibilidad de personal especializado en seguridad | Entrevistas, revisión de estructura organizacional |
| | Recursos técnicos | Existencia de infraestructura y herramientas tecnológicas | Revisión documental, encuestas |
| | Recursos financieros | Presupuesto asignado para la implementación del SGSI | Encuestas a stakeholders, análisis presupuestario |
| **Plan de acción para la implementación del SGSI** | Estrategias y cronograma | Existencia de un plan detallado con tiempos y responsables | Análisis documental, entrevistas |
| | Roles y responsabilidades | Asignación de tareas según perfiles y competencias | Revisión documental, encuestas |

## 3.6 TÉCNICAS, INSTRUMENTOS Y PROCEDIMIENTOS APLICADOS

### 3.6.1 TÉCNICAS

Se utilizarán técnicas mixtas, que combinan enfoques cualitativos y cuantitativos, para obtener una visión integral del estado actual y las necesidades de implementación del SGSI:

**a) Revisión Documental**

La revisión documental es una técnica de investigación que consiste en recopilar, analizar y evaluar de manera sistemática la información contenida en documentos ya existentes (como libros, artículos científicos, informes y normativas) para obtener datos relevantes que permitan comprender el estado del arte y fundamentar teóricamente el estudio. Esta técnica permite identificar antecedentes, teorías y enfoques que orientan la investigación (Hernández Sampieri et al., 2014).

En esta investigación utilizaremos la técnica de revisión documental para fundamentar teóricamente el estudio y obtener información relevante sobre la implementación del SGSI en LEYDE. Esto se realizará mediante la búsqueda y análisis de documentos clave como la norma ISO/IEC 27001:2022, políticas internas de la empresa e informes de auditoría.

**b) La entrevista**

La entrevista es un proceso de interacción y diálogo entre dos o más personas, generalmente entre el entrevistador y el entrevistado. Existen diversas modalidades de entrevista, entre las cuales se encuentran la entrevista asistemática o libre, la entrevista estructurada, la

entrevista focalizada, la entrevista simultánea y la entrevista sucesiva. Según (Díaz-Bravo et al., 2013) la entrevista se define como una conversación con un propósito específico, más allá del simple intercambio de palabras.

**c) Encuestas**

La encuesta es una técnica de recolección de datos que consiste en la aplicación de un cuestionario estructurado a una muestra representativa de una población, con el fin de obtener información sobre opiniones, actitudes o comportamientos (Hernández Sampieri et al., 2014).

En este estudio, la encuesta se utilizará como una técnica clave para recopilar información sobre el estado actual de la seguridad de la información en LEYDE, identificando las brechas existentes y evaluando la percepción del personal respecto a la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001:2022.

**d) Análisis de brechas**

Según (H. González, 2016), el análisis de brecha es una herramienta utilizada para comparar el estado y desempeño real de una organización, situación o entidad en un momento determinado con uno o más puntos de referencia seleccionados a nivel local, regional, nacional o internacional.

El análisis de brecha será una técnica clave en este estudio para evaluar la diferencia entre el estado actual de la seguridad de la información en LEYDE y los requisitos establecidos en la norma ISO/IEC 27001:2022. Su aplicación permitirá identificar áreas en las que la empresa ya cumple con los estándares y aquellas en las que existen deficiencias que requieren mejoras.

### 3.6.2 INSTRUMENTOS ELABORADOS

**a) Matriz de análisis documental**

El análisis documental es un proceso de construcción del conocimiento basado principalmente en el estudio de documentos escritos, como artículos, libros, gacetas, revistas, tesis, manuales y diccionarios. Aunque inicialmente estos documentos eran impresos, el avance tecnológico ha permitido su evolución hacia formatos digitales o electrónicos (Arias Odón, 2023). Por otro lado, el análisis de información abarca una variedad de fuentes que no se limitan a textos escritos, incluyendo videos, ponencias, audios y conferencias (Dulzaides Iglesias & Molina Gómez, 2004).

En este estudio la matriz de análisis documental se utilizará para registrar y analizar información clave extraída de documentos como la norma ISO/IEC 27001:2022, políticas internas de LEYDE, estudios previos y normativas de seguridad de la información. Ver ANEXO 2: MATRIZ DE ANÁLISIS DOCUMENTAL.

**b) Guion de entrevista semiestructurada**

El tipo de entrevista que se estará utilizando en este proyecto son las entrevistas semiestructuradas. Estas permiten un mayor grado de flexibilidad en comparación con las entrevistas estructuradas, ya que parten de preguntas previamente diseñadas, pero pueden ajustarse según las respuestas y experiencias de los entrevistados.

Las entrevistas están diseñadas para recopilar las percepciones y recomendaciones de los empleados y directivos de LEYDE respecto a la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022. Con una duración aproximada de dos horas, estas entrevistas se centrarán en identificar las principales brechas de seguridad, evaluar el nivel de conocimiento y compromiso del personal con la seguridad de la información, y recoger sugerencias clave para la planificación y ejecución del SGSI.

Se espera que los participantes ofrezcan respuestas claras y detalladas, reconociendo la importancia de su contribución para adaptar la propuesta de implementación a las necesidades reales de la organización y asegurar su éxito en el fortalecimiento de la protección, confidencialidad, integridad y disponibilidad de la información en LEYDE. Ver ANEXO 3: GUION DE ENTREVISTA SEMIESTRUCTURADA.

**c) Cuestionario**

Un cuestionario es una herramienta de recolección de datos que consiste en un conjunto de preguntas organizadas de manera estructurada y diseñada para obtener información de los encuestados. Los cuestionarios pueden ser utilizados en investigaciones de tipo cuantitativo o cualitativo, y sus preguntas pueden ser cerradas (con opciones de respuesta predefinidas) o abiertas (donde los encuestados proporcionan sus respuestas de manera libre). Este instrumento es ampliamente utilizado por su facilidad para recolectar grandes cantidades de información de manera estandarizada, lo que permite un análisis comparativo eficiente. (Hernández Sampieri et al., 2014)

En este estudio, se empleará el cuestionario como herramienta de recolección de datos. Conforme a (Hernández Sampieri et al., 2014) el cuestionario se define como un instrumento compuesto por una serie de preguntas relacionadas con una o más variables, las cuales serán objeto de medición. Ver ANEXO 4: CUESTIONARIO

**d) Lista de Verificación de Cumplimiento**

Una lista de verificación es un instrumento estructurado utilizado para asegurar que todos los elementos necesarios o pasos en un proceso determinado han sido completados o revisados. Generalmente, se utiliza en auditorías, inspecciones o cualquier situación donde es importante garantizar que se sigan procedimientos o se cumplan ciertos criterios establecidos. La lista ayuda a organizar y facilitar la recolección de información, mejorando la precisión y la eficiencia en la verificación de cumplimiento.(Melo, 2021)

En este proyecto, la Lista de Verificación de Cumplimiento será utilizada como una herramienta para evaluar y verificar la implementación de los requisitos establecidos por la norma ISO/IEC 27001:2022 en LEYDE. A lo largo de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), esta lista servirá para asegurarse de que todos los elementos clave del SGSI están siendo cumplidos de acuerdo con los estándares de la norma. Ver ANEXO 5: LISTA DE VERIFICACIÓN DE CUMPLIMIENTO

### 3.6.3 PROCEDIMIENTOS

**a) Revisión Documental**

El procedimiento consistirá en reunir y seleccionar los documentos clave relacionados con la seguridad de la información, como políticas, procedimientos, auditorías anteriores y normas internas de LEYDE. Estos documentos se analizarán de acuerdo con los lineamientos de la norma ISO/IEC 27001:2022, con el objetivo de identificar áreas de mejora y brechas en la implementación del SGSI. La revisión será realizada por un equipo encargado de analizar la información a fondo.

**b) Entrevistas**

Para aplicar la técnica de la entrevista semiestructurada, se diseñará un guion de preguntas previamente preparado. Las entrevistas serán realizadas con personal clave de LEYDE, como responsables de seguridad, directivos y personal operativo. Estas entrevistas se llevarán a cabo de

forma presencial o virtual según la disponibilidad y se grabarán con el consentimiento de los entrevistados. Se analizarán las respuestas cualitativas obtenidas para identificar puntos críticos y mejorar la implementación del SGSI.

**c) Encuestas**

El cuestionario estructurado será aplicado a través de una plataforma en línea, como Google Forms, para obtener datos cuantitativos. Se realizará una prueba piloto con una muestra representativa de 5 personas para validar la claridad de las preguntas. Posteriormente, el cuestionario será enviado a los participantes a través de correo electrónico o WhatsApp, según sea conveniente. Las respuestas se recopilarán y se analizarán en Excel para identificar tendencias y áreas de oportunidad.

**d) Análisis de Brechas**

Para el análisis de brechas, se compararán los resultados obtenidos de la revisión documental, entrevistas y encuestas con los requisitos establecidos en la norma ISO/IEC 27001:2022. Se identificarán las diferencias entre el estado actual de la seguridad de la información en LEYDE y lo que establece la norma, con el fin de desarrollar estrategias de mejora. Se utilizará una lista de verificación de cumplimiento basada en los controles y requisitos de la norma ISO/IEC 27001:2022.

### 3.6.4 PLAN DE ANALISIS

**a) Revisión Documental**

Se utilizó la matriz de análisis documental para sistematizar la información relevante, permitiendo identificar coincidencias y discrepancias entre la normativa y la situación actual en LEYDE.

**b) Entrevistas**

La información de las entrevistas se transcribirá y se realizará un análisis cualitativo mediante técnicas de codificación. Se identificarán temas recurrentes, opiniones y sugerencias, que serán organizados en categorías que permitan responder a los objetivos de la investigación. Los resultados cualitativos de las entrevistas serán analizados mediante técnicas de codificación para extraer temas recurrentes y patrones clave.

**c) Encuestas**

Los datos se exportarán desde Google Forms a Excel y se realizarán análisis estadísticos descriptivos (frecuencias, porcentajes) y, de ser necesario gráficos que faciliten la interpretación.

**d) Análisis de brechas**

Los datos de la revisión documental se compararán con los requisitos de la norma ISO/IEC 27001:2022 para identificar las brechas en el SGSI de LEYDE.

## 3.7 FUENTES DE INFORMACIÓN

### 3.7.1 FUENTES PRIMARIAS

Las fuentes primarias, también conocidas como fuentes de primera mano, son aquellos recursos documentales que se publican por primera vez, sin haber sido filtrados, resumidos o interpretados por algún individuo. Este tipo de fuentes provienen directamente de la actividad investigativa de los seres humanos. Entre las características de una fuente primaria se destacan: su originalidad, que actúan como evidencia directa para una investigación y su gran valor para todas las disciplinas (G. González, 2020).

En este caso de investigación se utilizaron las siguientes fuentes primarias:

- Se llevará a cabo un conjunto de entrevistas semiestructuradas con personal clave de LEYDE, como responsables de la seguridad de la información, directivos y empleados clave. Las entrevistas proporcionarán información detallada y cualitativa sobre las percepciones, desafíos y oportunidades en la implementación de un SGSI basado en la norma ISO/IEC 27001:2022.

- Se aplicará un cuestionario estructurado a los empleados de LEYDE, que permitirá recoger información cuantitativa sobre el nivel de conocimiento y cumplimiento de las políticas de seguridad de la información dentro de la organización.

- Se realizarán visitas a los diferentes departamentos de LEYDE para observar directamente las prácticas relacionadas con la seguridad de la información, lo que permitirá identificar posibles brechas y áreas de mejora en los procesos actuales.

### 3.7.2 FUENTES SECUNDARIAS

Las fuentes secundarias son aquellas que proporcionan información previamente recolectada y publicada por otros autores o instituciones. En este caso, las fuentes secundarias

servirán para contextualizar el marco teórico y comparar las prácticas actuales de LEYDE con las mejores prácticas y estándares internacionales.

En este caso de investigación se utilizaron las siguientes fuentes secundarias:

a) CRAI/Bases de datos, libros electrónicos.

b) Páginas web de organismos internacionales, como ISO.

c) Tesis titulada " ANÁLISIS DEL SISTEMA DE INFORMACIÓN EN ELCATEX SEGÚN NORMA ISO 27001:2013", sustentada por José María Garrido Álvarez y Juan José Flores Murillo.

## 3.8 MATRIZ DE CONGRUENCIA METODOLÓGICA

| Preguntas de Investigación | Objetivos | Metodología (Cualitativa, Cuantitativa) | Variables | Dimensiones | Indicadores | Instrumentos |
|---|---|---|---|---|---|---|
| ¿Cuáles son los requisitos y lineamientos establecidos en la norma ISO/IEC 27001:2022 para la implementación de un SGSI? | Identificar y analizar los requisitos y lineamientos establecidos en la norma ISO/IEC 27001:2022 para la implementación de un SGSI. | Cualitativa | Requisitos de la norma ISO/IEC 27001:2022 | Políticas y procedimientos de seguridad | Existencia de políticas y procedimientos | Revisión documental, guías de entrevista |
| ¿Cuál es el estado actual de la seguridad de la información en LEYDE y qué brechas se identifican en relación con los requisitos de la norma ISO/IEC 27001:2022? | Evaluar el estado actual de la seguridad de la información en LEYDE, identificando las brechas existentes en relación con los requisitos de la norma ISO/IEC 27001:2022 | Cualitativa | Estado actual de la seguridad de la información en LEYDE | Estado de las políticas de seguridad, vulnerabilidades identificadas, nivel de conocimiento del personal | Políticas de seguridad existentes, vulnerabilidades identificadas, nivel de conocimiento del personal | Encuestas, entrevistas, análisis de brechas |
| ¿Qué metodologías, herramientas y buenas prácticas son recomendables para la implementación de un SGSI en LEYDE, conforme a ISO/IEC 27001:2022? | Analizar y seleccionar metodologías, herramientas y mejores prácticas internacionales que faciliten la implementación efectiva de un SGSI en LEYDE. | Cualitativa | Metodologías y buenas prácticas | Aplicabilidad de metodologías reconocidas, aceptación por parte del personal | Aplicabilidad de metodologías reconocidas, nivel de aceptación por parte del personal | Revisión documental, entrevistas con expertos |
| ¿Qué recursos (humanos, técnicos y financieros) son necesarios para la implementación efectiva de un SGSI en LEYDE basado en la norma ISO/IEC 27001:2022? | Identificar y definir los recursos humanos, técnicos y financieros necesarios para la implementación efectiva del SGSI en LEYDE. | Cuantitativa | Recursos para la implementación del SGSI | Personal especializado, presupuesto, herramientas tecnológicas | Disponibilidad de personal especializado, presupuesto asignado, herramientas tecnológicas disponibles | Revisión documental, encuestas a stakeholders |
| ¿Qué plan de acción (cronograma, recursos y asignación de responsabilidades) es necesario para implementar efectivamente un SGSI en LEYDE basado en ISO/IEC 27001:2022? | Formular un plan de acción detallado que incluya un cronograma, asignación de recursos y responsabilidades, para la adopción efectiva del SGSI en LEYDE basado en ISO/IEC 27001:2022. | Mixta (Cualitativa y Cuantitativa) | Plan de acción para la implementación del SGSI | Planificación, roles y responsabilidades | Existencia de un cronograma detallado, asignación de roles y responsabilidades | Revisión documental, entrevistas, listas de verificación |

# CAPÍTULO IV. RESULTADOS Y ANÁLISIS

## 4.1 INTRODUCCIÓN

Este capítulo presenta los hallazgos obtenidos durante el proceso investigativo, producto del diagnóstico situacional de la empresa LEYDE en relación con el cumplimiento de los requisitos establecidos en la norma ISO/IEC 27001:2022. A partir de la aplicación de técnicas cualitativas y cuantitativas, se analizaron los elementos clave que afectan la seguridad de la información, incluyendo políticas internas, prácticas actuales, recursos disponibles y nivel de concienciación institucional.

En el presente capítulo se presentan y analizan los datos recopilados a través de los instrumentos utilizados como las entrevistas, encuestas, matriz documental y lista de verificación realizadas a los empleados de la empresa LEYDE. Esta información es la base para dar respuesta a la pregunta de investigación general: ¿Cómo puede implementarse un Sistema de Gestión de Seguridad de la Información (SGSI) en LEYDE, basado en la norma ISO/IEC 27001:2022, con el fin de fortalecer la protección, confidencialidad, integridad y disponibilidad de la información?

Los instrumentos utilizados para la recolección de datos fueron validados mediante juicio de expertos, con el propósito de asegurar su pertinencia, claridad y capacidad de generar información relevante para el diagnóstico del estado de la seguridad de la información en LEYDE. Esta validación fue realizada en conjunto con el maestro guía, M. Sc. Jorge Maradiaga, y el Coordinador de Infraestructura y Comunicaciones en LEYDE el Ing. Edy Parks, con el objetivo de tener un instrumento detallado y entendible para los entrevistados y encuestados y de esta forma obtener la información que aporte valor a la investigación.

## 4.2 EVALUACIÓN DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LEYDE

LEYDE ha demostrado avances importantes en la modernización de su infraestructura tecnológica. Entre estos esfuerzos destaca la migración de sus principales aplicaciones a entornos en la nube, lo cual ha mejorado notablemente la escalabilidad, disponibilidad y resiliencia de sus sistemas. Asimismo, se han implementado medidas técnicas como firewalls de nueva generación, software antivirus actualizado, protección en la capa DNS y autenticación multifactor (MFA). Estas herramientas permiten mitigar riesgos comunes como accesos no autorizados, malware o

ataques de denegación de servicio, representando una base sólida para la seguridad operativa.

No obstante, estos avances tecnológicos no han sido complementados con un marco formal de gestión de la seguridad de la información. Actualmente, LEYDE cuenta con lineamientos básicos para la gestión de accesos, tales como la creación de usuarios con credenciales seguras y ciertas restricciones al uso de dispositivos extraíbles o sitios web no autorizados. Sin embargo, dichos lineamientos carecen de formalización en políticas documentadas, procedimientos estandarizados o procesos de revisión y mejora continua, lo que genera una brecha significativa frente a las mejores prácticas internacionales, particularmente las establecidas en la norma ISO/IEC 27001:2022.

LEYDE aún no cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI) que esté correctamente definido, tampoco está certificado ni alineado formalmente con esta norma internacional. Esto significa que, si bien existen controles técnicos implementados, no hay una estructura de gobernanza ni un enfoque basado en gestión de riesgos que permita asegurar la confidencialidad, integridad y disponibilidad de la información. En consecuencia, la organización se encuentra vulnerable a brechas de seguridad, pérdidas de información crítica y posibles sanciones por incumplimiento normativo.

Para este objetivo se diseñó una Lista de Verificación basada en los 52 controles y requisitos de ISO/IEC 27001:2022. El levantamiento se realizó en el área de IT de LEYDE, con apoyo del equipo técnico a cargo de la infraestructura. Adicionalmente, se condujo una entrevista semiestructurada con el Coordinador de Infraestructura y Comunicaciones, Edy Parks.

### 4.2.1 RECOLECCIÓN Y ANÁLISIS DE DATOS DE LISTA DE VERIFICACIÓN

La matriz de cumplimiento con los controles y requisitos de ISO/IEC 27001:2022 muestra que, de los diez dominios de la norma (cláusulas 4 a 10), únicamente la política de seguridad de la información está definida de manera completa; todo lo demás figura “No” o “Parcial” con riesgos “Altos” o “Medios”.

**Tabla 8: Cumplimiento ISO 27001 – La Organización y Su Contexto**

| 4 | La Organización y su Contexto | Cumple (Sí/No/Parcial) | Riesgo Asociado (Alto/Medio/Bajo) |
|---|---|---|---|
| **4.1** | **Entendiendo la Organización y su contexto** | | |
| 1.- | ¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información? | No | Alto |
| 2.- | ¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información? | Parcial | Alto |
| 3.- | ¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información? | Parcial | Alto |
| **4.2** | **Expectativas de las partes interesadas** | | |
| 1.- | ¿Se han identificado las partes interesadas? | No | Medio |
| 2.- | ¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas? | No | Alto |
| 3.- | ¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales? | No | Alto |
| **4.3** | **Alcance del SGSI** | | |
| 1.- | ¿Se ha determinado el alcance del SGS y se conserva información documentada? | No | Alto |
| **4.4** | **SGS Sistema de Gestión de la Seguridad de la información** | | |
| 1.- | ¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora? | No | Alto |

La tabla 8 evidencia que la organización no ha definido objetivos del SGSI y solo parcialmente ha identificado factores internos, externos y amenazas, lo que representa un riesgo alto. Además, no se han identificado formalmente las partes interesadas, ni sus requisitos de seguridad, incluyendo legales y contractuales, lo que también implica riesgos altos.

No se ha determinado ni documentado el alcance del sistema de gestión, lo que imposibilita saber qué áreas o activos están protegidos. El SGSI no está implementado ni operando, y no existe evidencia de revisión o mejora continua. Este es un hallazgo crítico que refleja que la organización no tiene un sistema funcional de seguridad de la información, exponiéndola a riesgos severos.

**Tabla 9: Cumplimiento ISO 27001 – Liderazgo**

| 5 | Liderazgo | Cumple (Sí/No/Parcial) | Riesgo Asociado (Alto/Medio/Bajo) |
|---|---|---|---|
| **5.1** | **Liderazgo y compromiso** | | |
| 1.- | ¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio? | No | Alto |
| 2.- | ¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI? | No | Medio |
| 3.- | ¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI? | No | Alto |
| **5.2** | **Política de la Seguridad de la Información** | | |
| 1.- | ¿Se ha definido una Política de la Seguridad de la Información? | Si | Alto |
| 2.- | ¿Se ha establecido un marco que permita el establecimiento de objetivos? | Parcial | Medio |
| 3.- | ¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa? | Parcial | Medio |
| 4.- | ¿Se mantiene información documentada de la política del SGSI y de sus objetivos? | Si | Medio |
| **5.3** | **Roles y Responsabilidades** | | |
| 1.- | ¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información? | Parcial | Alto |
| 2.- | ¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información? | No | Medio |

A través de la tabla 9 en la sección 5.1 (Liderazgo y compromiso), se evidencia que no se han establecido objetivos alineados con el negocio, ni se han asignado recursos humanos o materiales adecuados, y tampoco se realiza una revisión efectiva de la eficacia del SGSI por parte de la dirección. En la sección 5.2 (Política de Seguridad de la Información), aunque se reconoce que existe una política formal y documentada, no se ha establecido completamente un marco para definir objetivos, y su comunicación interna y externa es deficiente. Esto debilita la comprensión y apropiación de la política por parte del personal y partes interesadas. En la sección 5.3 (Roles y responsabilidades), las responsabilidades han sido asignadas parcialmente, pero no se han comunicado adecuadamente. Esta falta de claridad puede dar lugar a incumplimientos, elevando

los riesgos de fallos de seguridad constante.

**Tabla 10: Cumplimiento ISO 27001 – Planificación**

| 6 | Planificación | Cumple (Sí/No/Parcial) | Riesgo Asociado (Alto/Medio/Bajo) |
|---|---|---|---|
| **6.1** | **Tratamiento de Riesgos y Oportunidades** | | |
| 1.- | ¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas con relación a la Seguridad de la Información? | No | Alto |
| 2.- | ¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos? | No | Alto |
| 3.- | ¿Se ha definido un proceso de tratamiento de riesgos? | No | Alto |
| 4.- | ¿Se han establecido criterios para elaborar una declaración de aplicabilidad? | No | Medio |
| 5.- | ¿Se mantiene información documentada de los puntos anteriores? | No | Medio |
| **6.2** | **Planificación para consecución de objetivos** | | |
| 1.- | ¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivos del negocio? | Parcial | Medio |
| 2.- | ¿Los objetivos de la Seguridad de la Información están planificados mediante?<br>-Asignación de responsabilidades<br>-Cronograma de ejecución temporal<br>-Método de evaluación | No | Medio |
| 3.- | ¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización teniendo en cuenta las funciones principales dentro de la Organización? | No | Medio |

En esta tabla 10 en la sección 6.1 (Tratamiento de riesgos y oportunidades), se identificó un incumplimiento total en aspectos fundamentales como la consideración de las expectativas de las partes interesadas, la identificación y análisis de riesgos, la definición del tratamiento de riesgos y la elaboración de la declaración de aplicabilidad. En la sección 6.2 (Planificación para la consecución de objetivos), aunque existen algunos intentos parciales por establecer objetivos, estos no son totalmente medibles ni están alineados con los objetivos estratégicos del negocio.

La falta de planificación estructurada y documentada en materia de seguridad de la información deja a la organización expuesta a riesgos sin control, sin rumbo estratégico ni mecanismos claros de mejora continua.

**Tabla 11: Cumplimiento ISO 27001 – Soporte**

| 7 | Soporte | Cumple (Sí/No/Parcial) | Riesgo Asociado (Alto/Medio/Bajo) |
|---|---|---|---|
| **7.1** | **Recursos** | | |
| 1.- | ¿Se identifican y asignan los recursos necesarios para el SGSI? | No | Medio |
| **7.2** | **Competencia** | | |
| 1.- | ¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad? | Parcial | Medio |
| 2.- | ¿Se mantiene información actualizada sobre la competencia del personal? | Parcial | Bajo |
| **7.3** | **Concienciación** | | |
| 1.- | ¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información? | Parcial | Medio |
| 2.- | ¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información? | Parcial | Medio |
| **7.4** | **Comunicación** | | |
| 1.- | ¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno? | Parcial | Medio |
| 2.- | ¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información? | No | Alto |

La tabla 11 evidencia que la organización presenta deficiencias importantes en los elementos de soporte requeridos para el adecuado funcionamiento del Sistema de Gestión de Seguridad de la Información. No se han identificado ni asignado los recursos necesarios y la evaluación de competencias del personal es incompleta. Aunque existe cierto grado de concienciación, el personal no está plenamente informado ni comprometido con su rol en la seguridad de la información. Además, la comunicación sobre políticas y responsabilidades es solo parcial y, de forma crítica, no existe un proceso formal para reportar deficiencias o malas prácticas en seguridad, lo cual representa un riesgo alto. En conjunto, estas debilidades comprometen la capacidad de la organización para mantener un SGSI efectivo, actualizado y alineado con los objetivos de seguridad, y aumentan su vulnerabilidad frente a incidentes y amenazas.

**Tabla 12: Cumplimiento ISO 27001 – Operación**

| 8 | Operación | Cumple (Sí/No/Parcial) | Riesgo Asociado (Alto/Medio/Bajo) |
|---|---|---|---|
| **8.1** | **Control Operacional** | | |
| 1.- | ¿Los procesos de seguridad de la Información están documentados para controlar que se realizan según lo planificado? | No | Medio |
| 2.- | ¿Existe un proceso para evaluar los riesgos en la Seguridad de la Información antes de realizar cambios en el Sistema de Gestión o procesos de Seguridad? | No | Alto |
| 3.- | ¿Se establecen medidas y planes para mitigar los riesgos en la Seguridad de la Información ante cambios realizados? | No | Alto |
| 4.- | ¿Se identifican y controlan los procesos externalizados en cuanto a los riesgos para la Seguridad de la Información? | Parcial | Alto |
| **8.2** | **Análisis de riesgos de la Seguridad de la Información** | | |
| 1.- | ¿Se ha establecido un proceso documentado de análisis y evaluación de riesgos para la Seguridad de la Información donde se identifique?<br>-El propietario del riesgo<br>-La importancia del riesgo o nivel de impacto<br>-La probabilidad de ocurrencia | No | Alto |
| **8.3** | **Tratamiento de riesgos de la Seguridad de la Información** | | |
| 1.- | ¿Se ha implementado un plan de tratamiento de riesgos dónde?<br>-Los propietarios del riesgo están informados y han aprobado el plan<br>-Se documentan los resultados | No | Alto |
| 2.- | ¿Se identifican todos los controles necesarios para mitigar el riesgo justificando su aplicación? | No | Alto |
| 3.- | ¿Se documenta el nivel de aplicación de todos los controles a aplicar? | No | Medio |

La tabla 12 muestra que la organización no cuenta con procesos documentados ni controles operacionales efectivos para gestionar la seguridad de la información. No se evalúan ni mitigan adecuadamente los riesgos antes de realizar cambios en el sistema o procesos, lo que representa un riesgo alto. Tampoco se ha establecido un proceso formal para analizar y evaluar riesgos, ni un plan de tratamiento de riesgos aprobado y documentado. Esta falta de gestión estructurada expone a la organización a vulnerabilidades y amenazas significativas

**Tabla 13: Cumplimiento ISO 27001 – Evaluación del desempeño**

| 9 | Evaluación del desempeño | Cumple (Sí/No/Parcial) | Riesgo Asociado (Alto/Medio/Bajo) |
|---|---|---|---|
| **9.1** | **Seguimiento y medición** | | |
| 1.- | ¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información teniendo en cuenta los controles para la seguridad de la información? | No | Alto |
| 2.- | ¿Se ha establecido un proceso documentado para evaluar los resultados de las mediciones y de que estos resultados son tomados en cuenta por los responsables tanto de los procesos como de la Seguridad de la Información? | No | Medio |
| **9.2** | **Auditorías Internas** | | |
| 1.- | ¿Se ha establecido una programación de Auditorías Internas y asignado responsables? | No | Alto |
| 2.- | ¿Se ha definido el alcance y los requisitos para el informe de auditoría? | No | Medio |
| 3.- | ¿Se consideran acciones correctivas y propuestas de cambio en los informes de auditoría? | No | Alto |
| **9.3** | **Informe de Revisión por la Dirección** | | |
| 1.- | ¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica? | No | Medio |
| 2.- | ¿Se documentan los resultados de los informes y la dirección se implica tanto en su conocimiento como en la toma de decisiones sobre los aspectos cruciales para el SGSI? | No | Alto |

Los resultados obtenidos según la tabla 13 muestra que la organización no ha establecido procesos efectivos para monitorear y medir el desempeño del SGSI, lo que implica un riesgo alto debido a la falta de seguimiento continuo y evaluación de los controles de seguridad. Tampoco existe una programación ni ejecución de auditorías internas, ni se han definido sus alcances, responsabilidades o acciones correctivas, lo que refleja una ausencia total de controles de evaluación interna. Además, no se cuenta con revisiones periódicas documentadas por parte de la alta dirección, ni con un involucramiento activo en la toma de decisiones sobre la mejora del SGSI. Esta falta de evaluación y mejora continua impide detectar fallas, corregir desviaciones y asegurar la eficacia del sistema, aumentando la vulnerabilidad organizacional frente a incidentes de seguridad.

**Tabla 14: Cumplimiento ISO 27001 – Mejora**

| 10 | Mejora | Cumple (Sí/No/Parcial) | Riesgo Asociado (Alto/Medio/Bajo) |
|---|---|---|---|
| **10.1** | **No Conformidades y acciones correctivas** | | |
| 1.- | ¿Existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento? | No | Alto |
| 2.- | ¿Dentro de las acciones correctivas existe una diferenciación entre acciones correctivas sobre la no conformidad y sobre las causas de esta? | No | Medio |
| **10.2** | **Mejora continua** | | |
| 1.- | ¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora? | No | Alto |

La tabla 10 evidencia que la organización no cuenta con un procedimiento documentado para identificar, registrar y tratar las no conformidades, lo que representa un riesgo alto para la capacidad de respuesta ante fallos o incidentes relacionados con la seguridad de la información. Tampoco existen acciones correctivas diferenciadas entre la resolución inmediata de la no conformidad y el abordaje de sus causas raíz, lo que limita la efectividad para evitar recurrencias, con un riesgo medio asociado.

Además, no se ha establecido un proceso formal para asegurar la mejora continua del SGSI, ni para identificar y aprovechar oportunidades de mejora, lo que compromete gravemente la evolución y fortalecimiento del sistema, aumentando la vulnerabilidad y la probabilidad de errores repetidos.

### 4.2.2 RECOLECCIÓN Y ANÁLISIS DE DATOS DE ENTREVISTA

Entrevistado: Edy Parks
Entrevistador: Danilo Josimar Herrera Elvir
Fecha: 16 de mayo de 2025

En el contexto actual, la seguridad de la información es un pilar fundamental para el correcto funcionamiento y protección de los activos digitales de cualquier organización. En esta entrevista, se abordaron aspectos clave relacionados con las prácticas de seguridad implementadas, el control de accesos físicos y digitales, la gestión de incidentes, y la

capacitación del personal en materia de ciberseguridad. La conversación se realizó con Edy Parks, coordinador de TI, quien aportó detalles sobre las políticas internas, el uso de tecnologías de protección, y los desafíos enfrentados para fortalecer la cultura de seguridad dentro de la empresa. Además, se exploró la familiaridad con normas internacionales como la ISO 27001 y la percepción sobre la necesidad de implementar sistemas de gestión de seguridad de la información.
Este análisis permite comprender la situación actual, identificar áreas de mejora y plantear propuestas orientadas a robustecer la protección de datos y sistemas en la organización.

La entrevista permitió identificar diversos elementos clave relacionados con la seguridad de la información, los cuales se detallan a continuación:

#### 4.2.2.1 CONTROL DE DISPOSITIVOS USB Y ALMACENAMIENTO EXTERNO

En la empresa se ha implementado una política de bloqueo general de puertos USB como medida preventiva para evitar la introducción de software malicioso o la extracción no autorizada de información sensible. Sin embargo, Edy explicó que existen equipos específicos que requieren el uso de dispositivos USB, principalmente en áreas de producción donde es necesario transferir datos de maquinaria o sistemas especializados. Estos accesos están estrictamente controlados y los equipos autorizados están plenamente identificados, lo que permite mantener un equilibrio entre la operatividad técnica y la seguridad. A pesar de este control, no se dispone actualmente de herramientas automatizadas para auditar o monitorear de forma centralizada los accesos a estos puertos, lo cual representa un punto de mejora potencial dentro de una estrategia de ciberseguridad más robusta.

#### 4.2.2.2 ACCESO FÍSICO Y RESGUARDO DE HARDWARE

Edy indicó que la empresa sí tiene controles físicos básicos para el acceso a áreas críticas, como el uso de llaves para oficinas cerradas y cámaras de seguridad en puntos estratégicos. Sin embargo, no se describieron medidas adicionales como control por tarjetas magnéticas, lectores biométricos o registro de ingreso y salida. Asimismo, no se mencionaron protocolos específicos para el resguardo de equipos obsoletos o dañados que aún contengan información sensible. Esta área podría reforzarse con mejores prácticas de seguridad física y procedimientos formales de

resguardo y disposición segura de hardware.

#### 4.2.2.3 DETECCIÓN DE AMENAZAS Y USO DE HERRAMIENTAS

La empresa utiliza herramientas antivirus que integran funciones avanzadas, como escaneo mediante inteligencia artificial para identificar comportamientos anómalos en los equipos. Edy mencionó que en algunos casos estas soluciones han generado alertas automáticas cuando se detectan posibles amenazas, lo que indica un nivel básico pero activo de monitoreo. Aunque no se detalló el uso de sistemas más avanzados, como IDS/IPS (sistemas de detección y prevención de intrusos) o firewalls configurables a nivel de red, el enfoque actual permite actuar de forma preventiva en ciertos casos. Aun así, este componente podría fortalecerse con la implementación de un sistema de seguridad más integral, que permita una mayor visibilidad y una respuesta proactiva frente a ciberataques.

#### 4.2.2.4 CAPACITACIÓN EN CIBERSEGURIDAD

Durante la entrevista, se identificó que la empresa realiza esfuerzos de concienciación en ciberseguridad, principalmente mediante comunicaciones internas semanales, como correos enviados los martes con recomendaciones sobre buenas prácticas, por ejemplo, uso adecuado de contraseñas o identificación de posibles amenazas como el phishing. Sin embargo, Edy reconoció que estas acciones no constituyen capacitaciones formales y que el personal de IT debería recibir una formación más robusta y especializada en temas clave de seguridad informática. La falta de entrenamientos técnicos más profundos limita la capacidad del equipo para anticipar, detectar y responder a incidentes de forma efectiva. Invertir en programas de formación estructurados y continuos, tanto para el personal general como para el técnico, sería una medida estratégica para fortalecer la postura de seguridad de la organización.

#### 4.2.2.5 POLÍTICAS Y DOCUMENTACIÓN

Edy señaló que la empresa aún no cuenta con políticas documentadas que regulen el uso de los recursos informáticos, el manejo de información confidencial, la gestión de incidentes o el uso aceptable de internet y correo electrónico. La ausencia de estas directrices puede llevar a la improvisación y a la inconsistencia en la respuesta a problemas de seguridad. El desarrollo de

políticas claras y accesibles es un paso fundamental para establecer una cultura organizacional de seguridad.

#### 4.2.2.6 GESTIÓN DE INCIDENTES DE SEGURIDAD

En caso de un incidente de seguridad, como una infección de malware o pérdida de datos, la empresa no cuenta con un procedimiento estructurado para reportarlo, analizarlo y remediarlo. Edy mencionó que este tipo de situaciones se resuelven en el momento, sin dejar registros ni realizar un análisis posterior. Esto impide aprender de los incidentes y prevenir su repetición. Establecer un proceso formal de gestión de incidentes ayudaría a mejorar la respuesta y reducir el impacto de futuras amenazas.

#### 4.2.2.7 CONOCIMIENTO SOBRE ISO/IEC 27001

Edy indicó que estudió la norma ISO/IEC 27001 hace algún tiempo, pero no está actualizado con la versión más reciente (2022). Esta norma establece los requisitos para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a estándares internacionales. Aunque existe un conocimiento previo, la falta de actualización podría dificultar la alineación de las prácticas actuales de seguridad con los requerimientos vigentes. Retomar el estudio de esta normativa y evaluar el estado actual de la empresa en relación con sus controles sería un paso importante para fortalecer de forma estructurada la ciberseguridad de la organización.

#### 4.2.2.8 ASPECTOS A FORTALECER

- Con base en la entrevista, se pueden identificar varios aspectos que requieren atención prioritaria:
- Formalización de políticas de seguridad y procedimientos.
- Implementación de herramientas de seguridad tecnológica (antivirus, firewalls, monitoreo).
- Desarrollo de un programa de capacitación continua para todo el personal.
- Mejora del control físico de accesos y resguardo de equipos informáticos.
- Creación de un plan de gestión de incidentes con roles y acciones definidas.
- Introducción gradual a marcos normativos como ISO/IEC 27001.

La empresa muestra un buen inicio en la implementación de controles básicos de seguridad y concienciación, pero presenta importantes áreas de mejora en formalización de políticas, documentación de incidentes, y planificación estratégica en ciberseguridad. La adopción de la norma ISO/IEC 27001:2022 podría representar una excelente oportunidad para elevar el nivel de madurez en la gestión de la seguridad de la información.

#### 4.2.2.8 RESUMEN DE ANÁLISIS

La entrevista con Edy Parks, coordinador de TI, permitió identificar el estado actual y los principales retos en la gestión de la seguridad de la información en la empresa. Se confirmó que los puertos USB están bloqueados de forma general, con excepciones controladas para equipos de producción, aunque no existe un monitoreo centralizado de estos accesos. El acceso físico a áreas críticas cuenta con controles básicos, pero faltan medidas más avanzadas para el resguardo de hardware.

La empresa utiliza antivirus con funciones de inteligencia artificial para detección de amenazas, pero carece de sistemas integrales como IDS/IPS o firewalls configurables que permitan una respuesta más proactiva. En cuanto a capacitación, se realizan comunicaciones internas periódicas para concienciar al personal, pero no hay entrenamientos formales, especialmente para el equipo de IT, que requiere formación más especializada.

No existen políticas documentadas sobre seguridad de la información ni procedimientos estructurados para la gestión de incidentes, lo que dificulta la respuesta organizada ante eventos de seguridad. Aunque Edy tiene conocimientos previos sobre la norma ISO/IEC 27001, no está actualizado con la versión vigente, lo que limita la alineación con estándares internacionales.

Como aspectos a fortalecer se destacan la formalización de políticas y procedimientos, mejora en las herramientas tecnológicas de seguridad, capacitación continua, control físico reforzado y la implementación de un plan formal de gestión de incidentes. La adopción de un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001:2022 se ve como una oportunidad clave para mejorar la madurez y protección de la empresa.

## 4.3 REQUISITOS Y LINEAMIENTOS DE ISO/IEC 27001:2022

Se analizó la documentación clave relacionada con el Sistema de Gestión de Seguridad de la Información (SGSI) implementado en la organización, evaluando su relevancia, grado de cumplimiento y su impacto en la gestión integral de la seguridad según la norma ISO/IEC 27001:2022. Los documentos analizados incluyen políticas internas, planes estratégicos y normativas externas que sustentan el control y mejora continua del SGSI.

Para la recopilación de la información documental se utilizó como instrumento una Matriz de Análisis Documental para revisar 4 documentos internos y la norma ISO/IEC 27001:2022, la cual permitió identificar aspectos clave relacionados con el cumplimiento de los requisitos establecidos en la norma ISO/IEC 27001:2022. El levantamiento documental se realizó con el equipo de IT.

**Tabla 15: Matriz Documental - Política de Seguridad de la Información**

| Nombre del Documento | Fuente | Fecha | Aspectos Relevantes | Relevancia para el SGSI |
|---|---|---|---|---|
| Política de Seguridad de la Información | Interno | 30-06-2024 | - Políticas de organización interna.<br><br>- Política de seguridad para el teletrabajo o trabajo remoto.<br><br>- Política de seguridad del recurso humano.<br><br>- Política de uso aceptable de activos.<br><br>-Política de uso de internet.<br>-Política de uso de dispositivos móviles.<br><br>- Política de uso del correo electrónico corporativo.<br><br>- Uso de redes inalámbricas. | -Agrupar todas estas políticas en la Política de Seguridad de la Información crea un punto de referencia para decisiones, auditorías y formación.<br><br>-Al documentar estas políticas y revisarlas periódicamente, se fortalece el ciclo de Planificar – Hacer – Verificar – Actuar, adaptándote a amenazas y cambios tecnológicos.<br><br>-Asegura que se cubre todos los controles de Anexo A de ISO 27001, apoyando la certificación y demostrando diligencia debida ante auditorías o reguladores. |

La tabla 15 nos muestra Política de Seguridad de la Información, cuya última actualización data del 30 de junio de 2024. Este documento agrupa diversas políticas internas fundamentales, tales como el uso aceptable de activos, el uso del correo electrónico corporativo, políticas para el trabajo remoto, políticas de contraseñas, y control de acceso, entre otras. La agrupación de estos lineamientos en una política integral representa un avance importante para el cumplimiento de los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2022. En relación con el objetivo específico número 2 de esta investigación, se concluye que la Política de Seguridad de la Información refleja de manera parcial los lineamientos de la norma. Si bien se abordan múltiples aspectos claves, se recomienda mejorar la trazabilidad documental con respecto a los controles específicos del Anexo A y establecer un mecanismo formal para su actualización y comunicación al personal.

**Tabla 16: Matriz Documental - Plan de Continuidad de Negocios**

| Nombre del Documento | Fuente | Fecha | Aspectos Relevantes | Relevancia para el SGSI |
|---|---|---|---|---|
| Plan de Continuidad de Negocios | Interno | 30-09-2024 | -Asegurar la protección de los activos clave de la empresa.<br><br>-Minimizar la interrupción de servicios y operaciones críticas.<br><br>-Minimizar la interrupción de servicios y operaciones críticas. | -Garantiza la disponibilidad de activos críticos.<br><br>-Reduce el riesgo operacional<br><br>-Protege la reputación y mantiene la confianza de clientes, socios |

La Tabla 16 nos muestra el análisis del Plan de Continuidad de Negocios, evidenciando que este documento interno, con fecha del 30 de septiembre de 2024, contempla aspectos clave como la protección de activos críticos y la minimización de interrupciones en los servicios y operaciones esenciales de la organización. Estos elementos son fundamentales para cumplir con los requisitos establecidos en la norma ISO/IEC 27001:2022, específicamente en el control 17.1, relacionado con la continuidad de la seguridad de la información.

La existencia de este plan es una evidencia importante del compromiso de la organización

con la seguridad de la información y la gestión de la continuidad del negocio, alineándose con el enfoque de mejora continua propuesto por el ciclo PDCA (Planificar, Hacer, Verificar, Actuar).

Sin embargo, es necesario verificar si el plan incluye componentes como el análisis de impacto al negocio (BIA), las estrategias de recuperación, y los mecanismos de prueba y actualización periódica, para asegurar su efectividad ante eventos disruptivos.

**Tabla 17: Matriz Documental - Plan de Respuesta a Incidentes**

| Nombre del Documento | Fuente | Fecha | Aspectos Relevantes | Relevancia para el SGSI |
|---|---|---|---|---|
| Plan de Respuesta a Incidentes | Interno | 09-12-2024 | -Detectar y clasificar los incidentes.<br><br>- Limitar el impacto del incidente para evitar su propagación.<br><br>- Eliminar las causas subyacentes del incidente.<br><br>- Restaurar los sistemas y servicios a su estado normal y minimizar el tiempo de inactividad.<br><br>- Evaluar la respuesta al incidente y mejorar los procesos de seguridad para el futuro. | - Cumplir con la cláusula 16 de ISO/IEC 27001, asegurando que se tienes roles, procedimientos y criterios de clasificación claros.<br><br>-Aprender de cada incidente, cerrando el ciclo de mejora continua (PDCA) y reforzando controles preventivos y correctivos. |

La Tabla 17 evidencia el contenido del Plan de Respuesta a Incidentes, un documento interno actualizado el 09 de diciembre de 2024, el cual contempla acciones esenciales como la detección y clasificación de incidentes, la contención y eliminación de causas, la restauración de los servicios afectados y la evaluación post-incidente con miras a mejorar continuamente los procesos de seguridad.

Este plan está directamente alineado con la cláusula 16 de la norma ISO/IEC 27001:2022, que establece la necesidad de contar con un proceso estructurado para gestionar los incidentes de seguridad de la información.

Desde la perspectiva del Sistema de Gestión de Seguridad de la Información (SGSI), este plan fortalece la capacidad de respuesta organizacional y demuestra un compromiso con el ciclo

de mejora continua PDCA, al permitir el aprendizaje a partir de eventos pasados y la mejora de controles preventivos y correctivos.

**Tabla 18: Matriz Documental - Políticas de Uso Datacenter**

| Nombre del Documento | Fuente | Fecha | Aspectos Relevantes | Relevancia para el SGSI |
|---|---|---|---|---|
| Políticas de Uso Datacenter | Externo | 18-01-2024 | -Uso del Datacenter y sala de equipos<br>-Normas de Evacuación<br>-Solicitud de Acceso al Datacenter<br>-Mantenimientos | -Relacionado con el control A.11.1.1 (Controles de acceso físico).<br>-A.17.1.1 (Continuidad de la seguridad de la información).<br>-Reduce el riesgo de intrusiones o actividades no autorizadas.<br>-Se relaciona con A.11.2.4 (Mantenimiento de equipos). |

La Tabla 18 presenta el análisis del documento externo titulado Políticas de Uso del Datacenter, con fecha del 18 de enero de 2024. Este documento establece lineamientos claros sobre el uso del Datacenter y la sala de equipos, incluye normas de evacuación, procedimientos para la solicitud de acceso y pautas para el mantenimiento de los equipos críticos. El contenido de este documento se relaciona directamente con varios controles del Anexo A de la norma ISO/IEC 27001:2022. En particular, se vincula con el control A.11.1.1, que aborda los controles de acceso físico a instalaciones, y con el control A.11.2.4, que trata sobre el mantenimiento seguro de los equipos. Asimismo, guarda relación con el control A.17.1.1, enfocado en garantizar la continuidad de la seguridad de la información ante eventos disruptivos. Se observa que la existencia de estas políticas permite reducir los riesgos asociados a accesos no autorizados, mantener la seguridad física del entorno tecnológico y asegurar la operación continua del Datacenter. Esto resulta fundamental para preservar la disponibilidad, integridad y confidencialidad de los activos de información alojados en dicho entorno

## 4.4 RECURSOS HUMANOS, TÉCNICOS Y FINANCIEROS

Como parte del análisis para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa LEYDE, basado en la norma ISO/IEC 27001:2022, se realizó una encuesta dirigida a 15 colaboradores de distintas áreas funcionales de la organización, incluyendo IT, Finanzas, Contabilidad, Producción y Administración. El objetivo de esta encuesta fue evaluar la percepción interna sobre los actuales controles, conocimientos y preparación de la empresa en materia de seguridad de la información. Cabe destacar que más del 38% de los encuestados pertenecen al área de IT, considerada crítica por su rol central en la gestión y protección de los activos de información.

### 4.4.3 PERFIL DEL PERSONAL ENCUESTADO

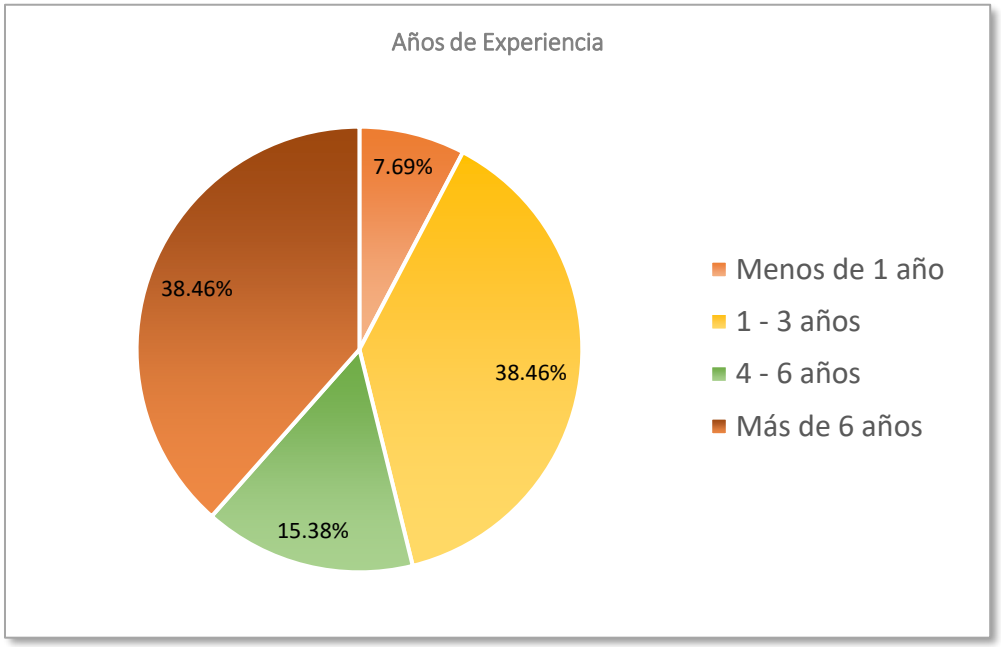



**Figura 11: Encuesta - Años de experiencia empleados**

La experiencia laboral de los colaboradores es un factor relevante al evaluar el nivel de madurez y comprensión de los procesos relacionados con la seguridad de la información. Un equipo con mayor antigüedad en la organización suele tener un conocimiento más profundo de la infraestructura tecnológica, los procedimientos internos y los riesgos específicos del entorno de trabajo, lo que puede facilitar la implementación de medidas de seguridad efectivas.

Se observó un equilibrio positivo en la antigüedad del personal, destacando dos grupos significativos: colaboradores con entre 1 a 3 años de experiencia y aquellos con más de 6 años. Esta combinación permite contar tanto con una base de personal con experiencia consolidada como

con empleados más recientes que pueden aportar nuevas perspectivas y apertura al cambio. **Solo una pequeña proporción de empleados cuenta con menos de un año en la organización, lo que indica estabilidad laboral y retención del talento.**

Particularmente en el área de Tecnologías de la Información (IT), se identificó una mayor concentración de empleados con entre 4 a 6 años de experiencia. Este grupo representa un recurso estratégico, ya que su conocimiento acumulado sobre la infraestructura tecnológica, los sistemas en uso y las necesidades del negocio los posiciona como actores clave para liderar o apoyar procesos de fortalecimiento en ciberseguridad. Además, su tiempo en la organización les permite comprender mejor las dinámicas internas y posibles resistencias al cambio, lo cual puede ser aprovechado para facilitar la adopción de un Sistema de Gestión de Seguridad de la Información (SGSI).

Este perfil de experiencia, bien aprovechado, puede ser una ventaja significativa para el desarrollo de estrategias de seguridad sostenibles y alineadas con la cultura organizacional.

### 4.4.4 CONOCIMIENTO SOBRE LA NORMA ISO/IEC 27001

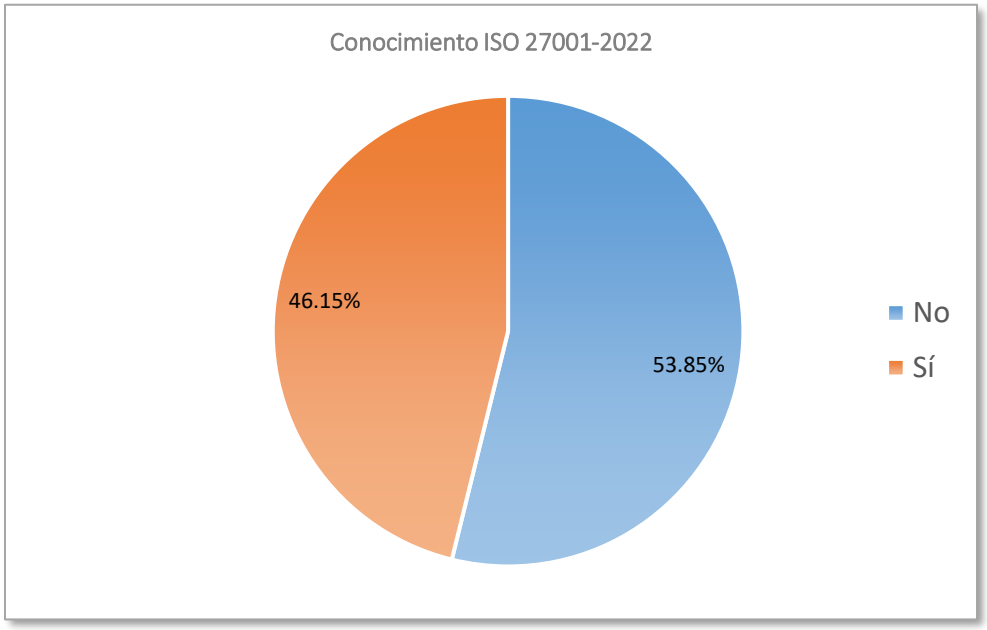



**Figura 12: Encuesta - Conocimiento sobre ISO 27001**

Con respecto al nivel de conocimiento sobre la norma ISO/IEC 27001:2022, se identificó que más del 50% de los encuestados manifestaron no tener conocimiento sobre dicha normativa. Este resultado refleja una importante brecha en la familiaridad con los estándares internacionales

que rigen la gestión de la seguridad de la información.

El desconocimiento es aún más pronunciado en el área de Tecnologías de la Información (IT), donde el 60% de los colaboradores indicaron no estar familiarizados con la norma. Esta situación resulta especialmente crítica, considerando que el personal de IT desempeña un rol central en la implementación, mantenimiento y monitoreo de los controles de seguridad establecidos por un Sistema de Gestión de Seguridad de la Información (SGSI).

**La ausencia de conocimiento técnico sobre la norma ISO/IEC 27001 limita la capacidad de la organización para alinear sus prácticas con marcos reconocidos a nivel global**, lo cual puede traducirse en debilidades en la protección de la información sensible, en el cumplimiento regulatorio y en la respuesta ante incidentes. Por tanto, este hallazgo representa una oportunidad crítica de mejora, que debe abordarse mediante programas de capacitación específicos para los equipos clave, particularmente aquellos involucrados en la gestión tecnológica y la gobernanza de la seguridad. Fortalecer este conocimiento no solo aumentará la eficacia de cualquier futura implementación de un SGSI, sino que también contribuirá a elevar la madurez general en ciberseguridad dentro de LEYDE.

### 4.4.5 POLÍTICAS Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

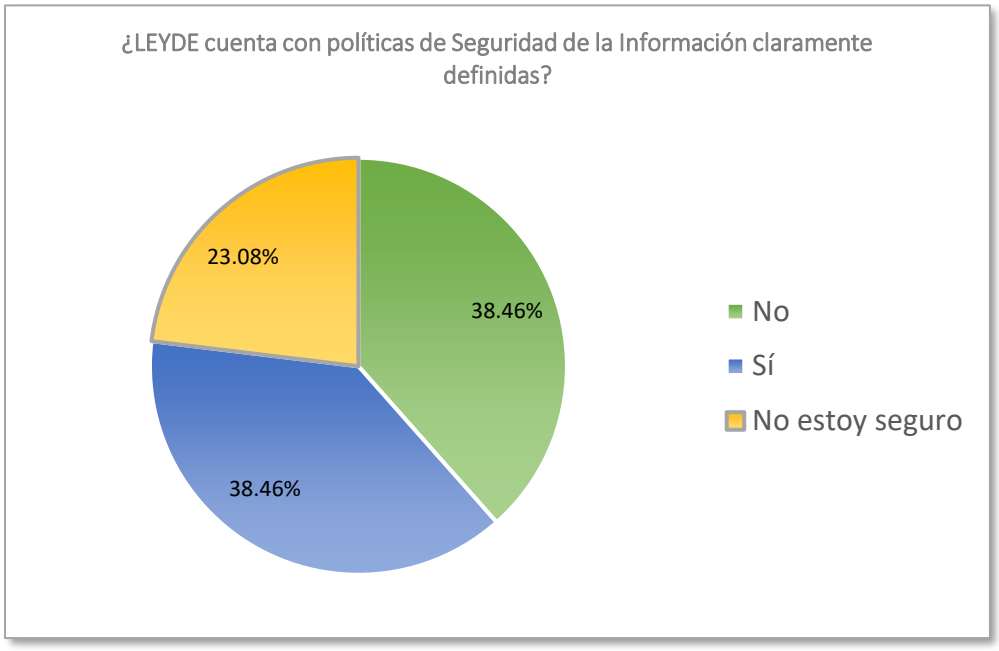



**Figura 13: Encuesta - Políticas de seguridad en LEYDE**

Una de las preguntas realizadas en la encuesta fue: ***"¿La empresa cuenta con políticas de seguridad de la información claramente definidas?".*** Los resultados revelaron una distribución equitativa entre quienes consideran que sí existen dichas políticas (38.46%) y quienes opinan lo contrario (38.46%). Además, un 23.08% de los encuestados manifestó no estar seguro al respecto. Esta división en las respuestas refleja una importante falta de claridad y comunicación interna en torno a los lineamientos actuales de seguridad de la información dentro de la organización.

**La percepción ambigua o contradictoria sobre la existencia de políticas claras puede indicar que, aunque las políticas pudieran estar documentadas,** no han sido debidamente socializadas ni interiorizadas por el personal. Esto genera un riesgo significativo, ya que el desconocimiento o la falta de comprensión de las políticas compromete su efectividad y dificulta la adopción de comportamientos seguros por parte de los colaboradores.

Este hallazgo subraya la necesidad de reforzar no solo la formalización de políticas de seguridad, sino también su divulgación y capacitación continua, de forma que todos los niveles de la organización tengan una comprensión clara y actualizada de los lineamientos que deben seguirse para proteger los activos de información.

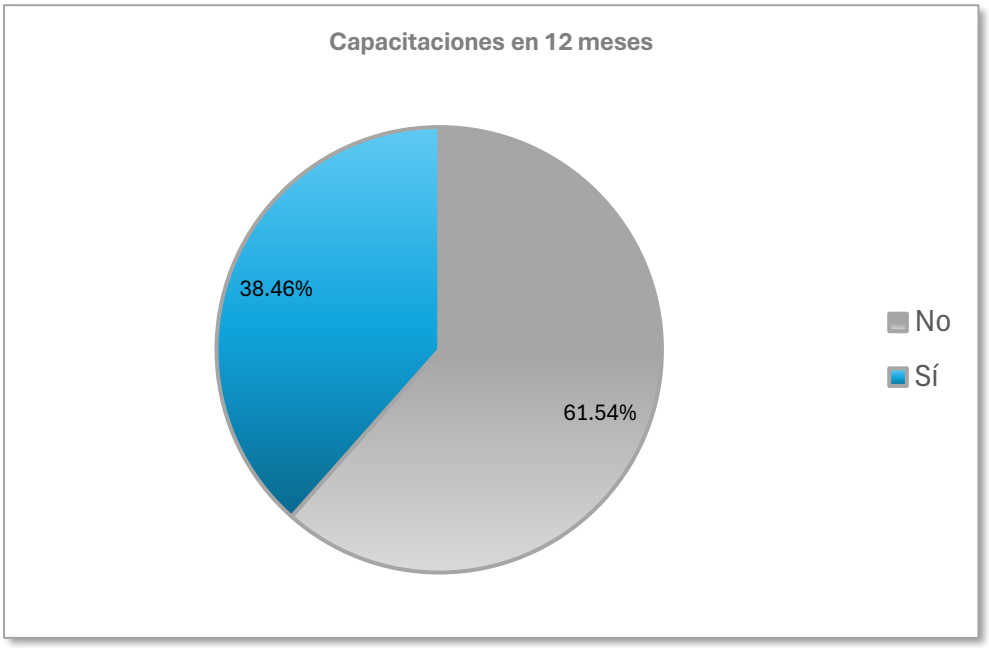



**Figura 14: Encuesta – Capacitaciones**

Un aspecto preocupante revelado en los resultados de la encuesta es la limitada formación del personal en temas de seguridad de la información. En concreto, el 61% de los colaboradores indicó no haber recibido ningún tipo de capacitación en los últimos 12 meses relacionada con buenas prácticas de ciberseguridad, tales como la prevención de ataques de phishing, el uso adecuado de contraseñas o la protección de datos sensibles.

**Este escenario se agrava aún más en áreas estratégicas como IT, Finanzas y Contabilidad, donde el 100% de los encuestados señaló no haber recibido formación reciente en este ámbito.** Esta falta de preparación representa un riesgo crítico, ya que dichos departamentos gestionan información confidencial, recursos financieros y sistemas esenciales para el funcionamiento de la empresa, convirtiéndolos en objetivos prioritarios para posibles amenazas cibernéticas.

La ausencia de programas de capacitación continua limita la capacidad de respuesta del personal ante incidentes de seguridad y debilita la cultura organizacional en torno a la protección de la información. Por tanto, establecer planes formativos periódicos y diferenciados por perfil de riesgo sería un paso clave para fortalecer la postura de seguridad de la organización.

### 4.4.6 PERCEPCIÓN SOBRE LA GESTIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN

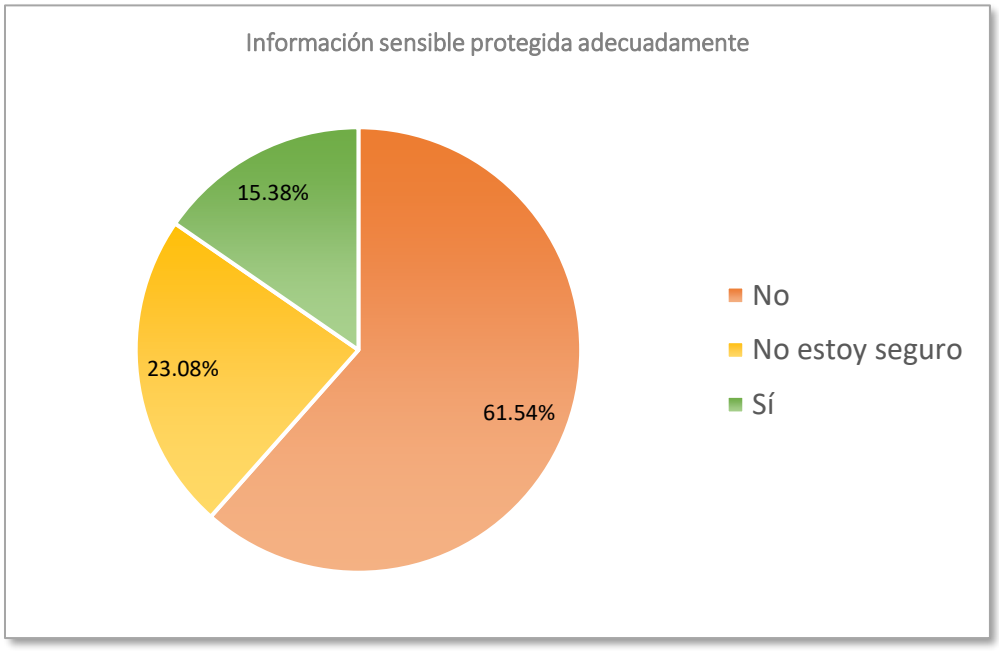



**Figura 15: Encuesta - Información sensible**

Al evaluar la percepción general del personal respecto a la protección de la información sensible dentro de la empresa, solo el 15% de los encuestados consideró que la organización gestiona adecuadamente la seguridad de sus datos. Este resultado pone de manifiesto **una brecha significativa entre las expectativas del personal y las prácticas actuales en materia de ciberseguridad.**

Una percepción tan baja de efectividad en los controles de seguridad puede estar relacionada con múltiples factores, como la falta de comunicación interna sobre las medidas existentes, la ausencia de políticas claras, la falta de capacitación formal o la escasez de herramientas tecnológicas visibles por parte de los usuarios. En cualquier caso, este nivel de desconfianza representa una vulnerabilidad organizacional, ya que puede traducirse en menor compromiso del personal con las políticas de seguridad, o en un reporte de incidentes o comportamientos sospechosos.

Este indicador refuerza la importancia de establecer un Sistema de Gestión de Seguridad

de la Información (SGSI) basado en estándares reconocidos como la ISO/IEC 27001, que no solo mejore los controles técnicos y administrativos, sino que también aumente la transparencia, la confianza interna y la cultura organizacional en torno a la protección de la información.

### 4.4.7 RECURSOS NECESARIOS PARA LA IMPLEMENTACIÓN DE UN SGSI

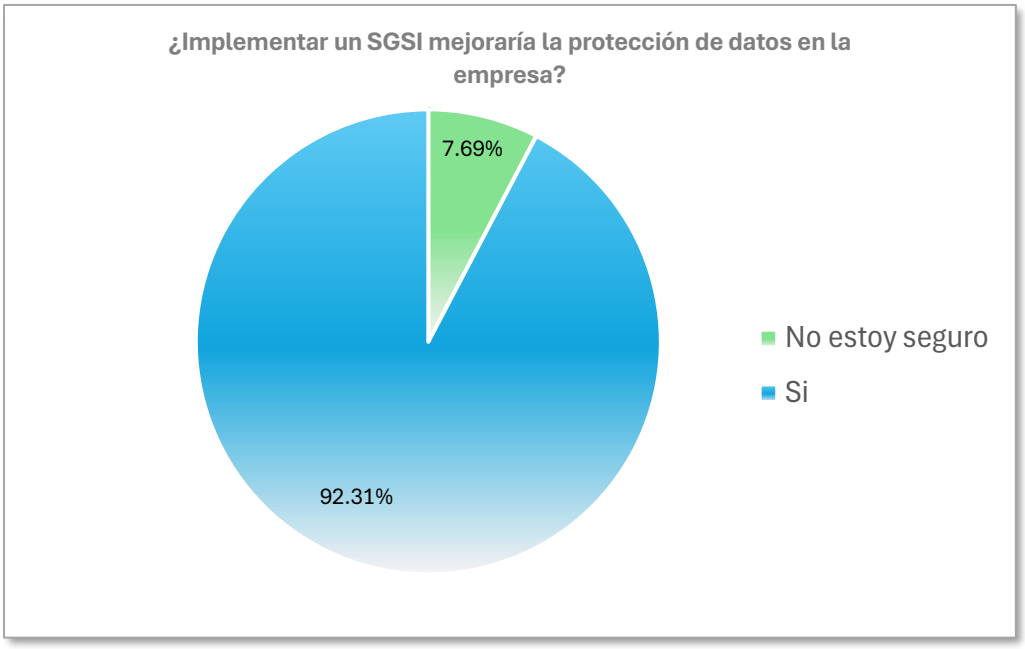



**Figura 16: Encuesta - Implementación de un SGSI**

Uno de los hallazgos más significativos de la encuesta fue la alta aceptación por parte del personal respecto a la implementación de un **Sistema de Gestión de Seguridad de la Información (SGSI)**. Más del **90% de los encuestados** manifestaron estar de acuerdo con que la adopción de un sistema formal de este tipo **mejoraría significativamente los indicadores de seguridad dentro de la empresa**.

Este dato refleja una **actitud positiva y receptiva hacia el cambio organizacional** en materia de ciberseguridad. El alto nivel de aceptación sugiere que existe un entendimiento, al menos general, de que los riesgos actuales requieren una gestión más estructurada y proactiva, respaldada por políticas, procedimientos y tecnologías alineadas con estándares internacionales como la norma **ISO/IEC 27001**.

Además, esta disposición del personal puede facilitar notablemente el proceso de

implementación de un SGSI, ya que el éxito de dicho sistema no solo depende de la infraestructura tecnológica o de las políticas escritas, sino también del **compromiso de las personas que lo operan y lo cumplen a diario**. La aceptación inicial es un activo importante para impulsar iniciativas de cambio, programas de concientización, capacitaciones y la adopción de controles nuevos sin enfrentar una fuerte resistencia cultural.

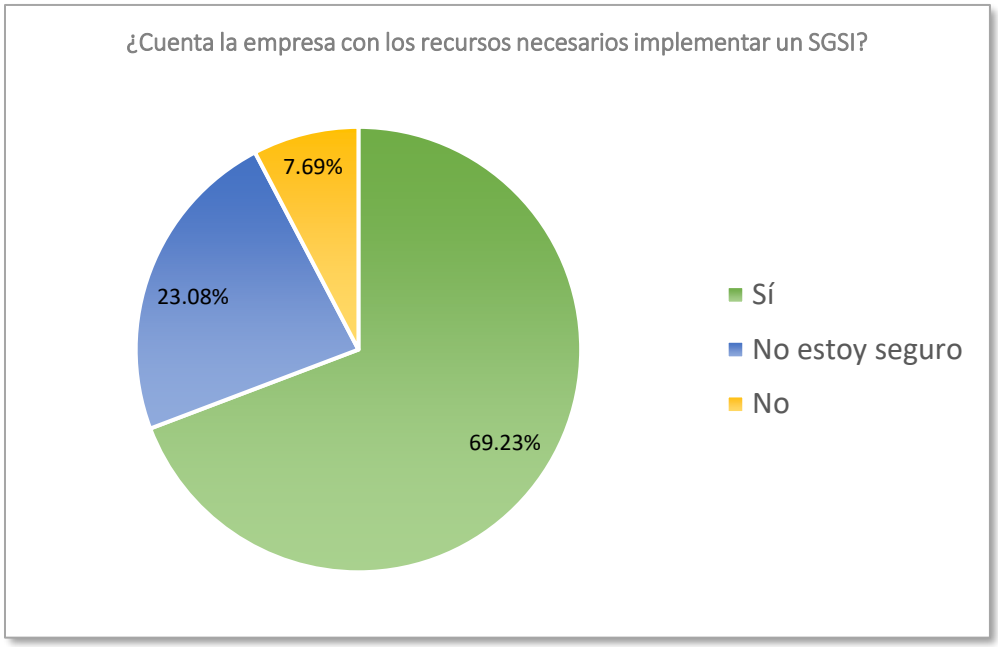



**Figura 17: Encuesta - Recursos para implementar un SGSI**

Otro hallazgo relevante de la encuesta fue la percepción general sobre la disponibilidad de recursos para llevar a cabo la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). El 69% de los encuestados manifestó que considera que la empresa cuenta con los recursos necesarios para este propósito.

Este porcentaje refleja una opinión mayoritaria positiva sobre la capacidad actual de la organización para asumir los retos que implica la adopción de un SGSI**. La percepción de contar con recursos adecuados puede referirse a aspectos como infraestructura tecnológica, herramientas de seguridad, presupuesto asignado, así como el capital humano disponible.**

De manera más destacada, en las áreas consideradas críticas para la seguridad, como Tecnologías de la Información (IT) y Finanzas, el 100% de los colaboradores encuestados afirmó que se dispone de los elementos necesarios para emprender esta iniciativa. Esto es particularmente relevante porque estos departamentos suelen ser los más involucrados en la gestión de

información sensible y en la operación de controles de seguridad.

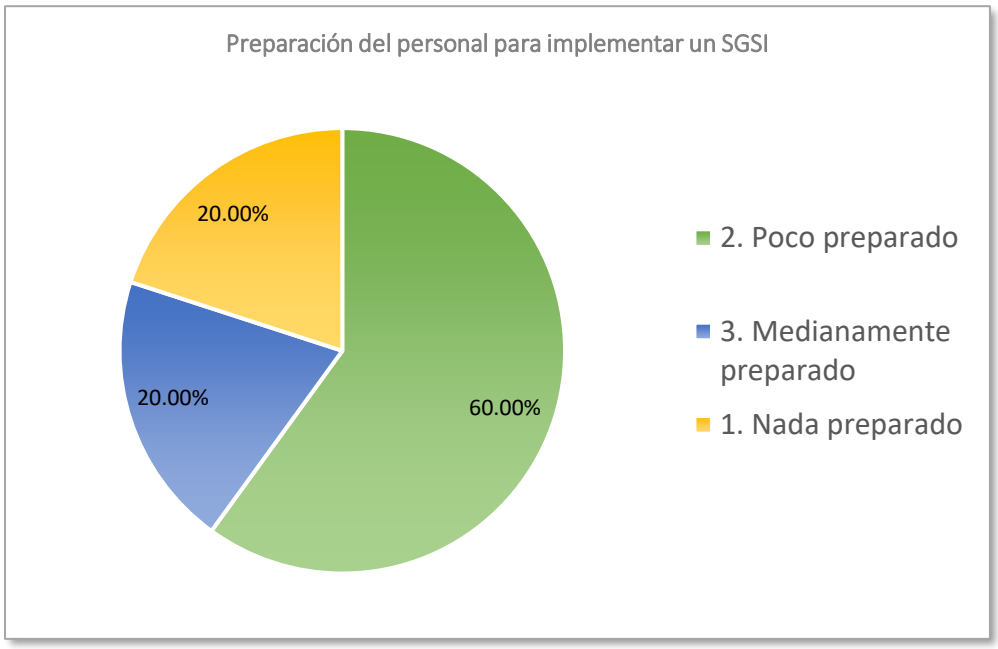



**Figura 18: Encuesta - Preparación del personal para implementar un SGSI**

Dentro del personal de IT se evaluó la preparación actual para afrontar un proyecto de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). La gran mayoría manifestó no sentirse adecuadamente preparada, lo que evidencia una brecha importante en conocimientos y habilidades necesarios para liderar y ejecutar este tipo de iniciativas. Este hallazgo refuerza la necesidad de diseñar e implementar intervenciones estratégicas para fortalecer al equipo y asegurar el éxito del proyecto.

En este contexto, los encuestados señalaron dos áreas principales de mejora:

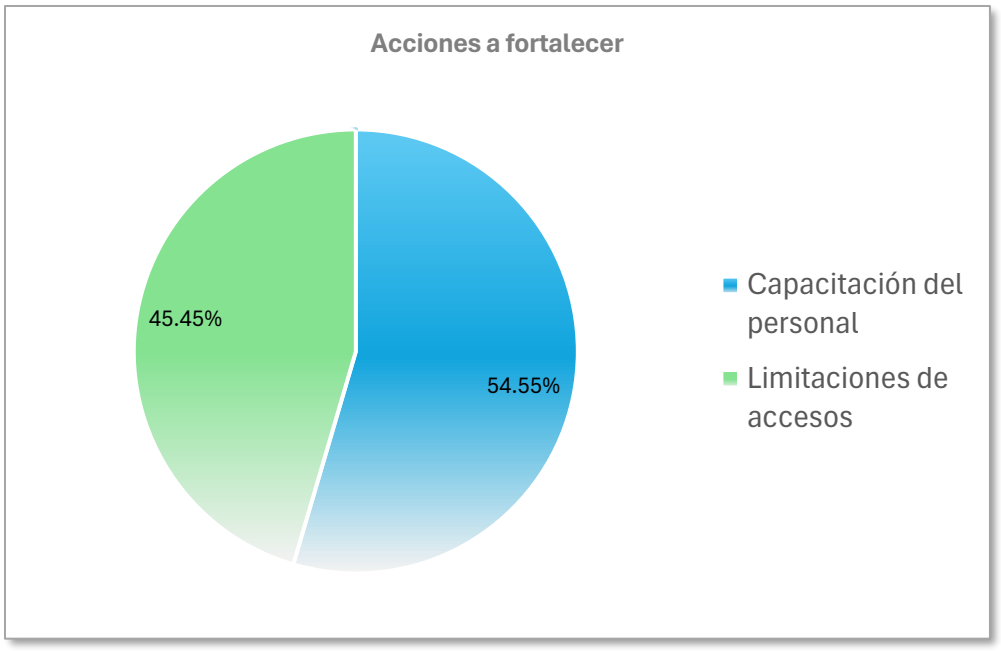



**Figura 19: Encuesta - Acciones a fortalecer**

El 54% de los encuestados consideró que la **capacitación del personal en temas de seguridad de la información** es una prioridad fundamental para fortalecer la postura de ciberseguridad de la empresa. Esta percepción refleja la importancia de contar con colaboradores capacitados que comprendan los riesgos, las mejores prácticas y los procedimientos para proteger los activos de información.

De manera similar, una proporción comparable de participantes destacó la necesidad de **establecer mejores mecanismos de control de acceso para los usuarios**. Este aspecto es crucial para garantizar que únicamente el personal autorizado pueda acceder a recursos sensibles, minimizando así la superficie de ataque y facilitando una gestión efectiva del riesgo.

Ambas prioridades —la formación continua del personal y el control riguroso de accesos— constituyen pilares esenciales para la implementación exitosa de un Sistema de Gestión de Seguridad de la Información (SGSI), contribuyendo a la protección integral de la organización frente a amenazas cibernéticas.

En resumen, los resultados muestran que la empresa reconoce la importancia de mejorar la seguridad de la información, especialmente en la capacitación del personal y el control de accesos. Aunque hay recursos disponibles, es necesario fortalecer la preparación del equipo para avanzar hacia una gestión más segura y efectiva.

# CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

## 5.1 CONCLUSIONES

1. **Limitaciones en la política de seguridad y en la gestión documental:**

   El diagnóstico reveló que, aunque la política de seguridad de LEYDE está formalmente documentada, esta no cubre adecuadamente los dominios esenciales exigidos por la norma ISO/IEC 27001:2022. Por ejemplo, no se evidencia la aplicación de un proceso formal de evaluación y tratamiento de riesgos conforme a la cláusula 6.1.2, tampoco se especifican criterios claros de aceptación de riesgos según la cláusula 6.1.3. Asimismo, la política carece de mecanismos de revisión y actualización periódica, lo que contraviene la cláusula 5.1 sobre liderazgo y compromiso, y la cláusula 10.1 relacionada con la mejora continua.

   Adicionalmente, no se contemplan controles del Anexo A fundamentales para una gestión efectiva de la seguridad de la información, como:

   - **A.5.12**: Clasificación de la información,
   - **A.5.15**: Gestión de acceso basada en roles y necesidades,
   - **A.5.24**: Gestión de incidentes de seguridad de la información, y
   - **A.5.30**: Registro de eventos y monitoreo.

   Tampoco se evidencia una planificación estructurada de auditorías internas conforme a la cláusula 9.2, lo que impide el establecimiento de un ciclo efectivo de mejora continua, limitando la capacidad de la organización para identificar, corregir y prevenir vulnerabilidades de manera oportuna. Sumado a ello, se identificó que el 57% de los colaboradores no conoce los lineamientos de la norma ni ha recibido capacitación reciente, lo que profundiza la brecha de conocimiento y la falta de conciencia organizacional sobre la importancia de la seguridad de la información. (Barker, 2024)

2. **Desalineación significativa entre prácticas actuales y requisitos normativos:**

   La comparación entre las prácticas implementadas en LEYDE y los requerimientos de ISO/IEC 27001:2022 evidencia un desfase importante. No se cuenta con una definición clara del contexto interno y externo, ni con una identificación formal de las partes

interesadas y sus expectativas. Asimismo, el alcance del SGSI está mal delimitado y carece de objetivos de seguridad específicos y medibles. La ausencia de documentación detallada sobre los controles y la falta de mecanismos formales para revisar periódicamente su cumplimiento limitan la capacidad para garantizar la efectividad y actualización continua del sistema. Estas deficiencias dificultan la alineación de los procesos internos con los estándares internacionales y representan un riesgo para la preparación frente a auditorías externas.

3. **Necesidad de herramientas y metodologías para una gestión integral:**

   El análisis de mejores prácticas y estándares internacionales subraya la importancia de adoptar modelos como ISO 31000 para la gestión de riesgos, y la implementación de plataformas centralizadas para el registro, seguimiento y control de riesgos, incidentes y auditorías. Actualmente, la falta de un sistema integrado para consolidar esta información obstaculiza la trazabilidad y dificulta el control y la generación de evidencias. La incorporación de soluciones GRC (Governance, Risk & Compliance) o similares es fundamental para fortalecer la gestión, facilitar reportes claros y demostrar conformidad con la norma, promoviendo así una mayor transparencia y eficacia en la administración de la seguridad de la información.

4. **Déficit en la definición de roles y en la capacitación continua del personal:**

   Si bien existe una percepción positiva respecto a la disponibilidad de recursos técnicos y financieros para implementar el SGSI, se identificó una carencia relevante en la asignación clara de roles estratégicos, tales como gestores de riesgos, responsables de procesos y coordinadores de auditorías. Además, la falta de un programa de formación continua especializada en seguridad de la información limita el desarrollo de competencias necesarias para sostener el SGSI. Esta combinación de factores implica que, a pesar de contar con infraestructura, el factor humano representa un punto débil que podría poner en riesgo la correcta implementación y operación del sistema en el mediano plazo.

5. **Ausencia de un plan de implementación estructurado y detallado:**

   La falta de un plan de acción formal que establezca cronogramas, hitos, asignación de recursos y responsables específicos para cada etapa del proyecto genera un alto riesgo de

desorganización y retrasos. Sin una planificación clara que abarque desde el diagnóstico inicial y la gestión de brechas hasta la elaboración de documentación, capacitación, auditorías y revisiones directivas, la implementación del SGSI puede perder foco y momentum. Este vacío estratégico compromete la eficiencia del proceso y la sostenibilidad de la gestión de seguridad en el largo plazo, haciendo imprescindible la definición de una hoja de ruta clara y consensuada.

## 5.2 RECOMENDACIONES

1. **Identificar y documentar asuntos internos y externos, partes interesadas y alcance de la certificación.**

   **Ejemplo:** Realizar una sesión de análisis con los líderes de cada área para identificar factores como la rotación del personal (interno) o cambios regulatorios en la industria alimentaria (externo). Documentar que el alcance del SGSI incluye la planta de producción, el sistema ERP y el correo corporativo. Incluir como partes interesadas al proveedor de servicios de nube, a los clientes que exigen seguridad contractual y a los entes reguladores.

2. **Ampliar la política existente incluyendo objetivos, responsabilidades definidas, revisiones anuales y mecanismos de comunicación interna.**

   **Ejemplo:** Modificar la política de seguridad para establecer como objetivo reducir incidentes de phishing en un 50% en un año. Designar al jefe de IT como responsable de coordinar revisiones. Comunicarla trimestralmente vía correo y reuniones departamentales. Publicarla en el portal interno de la empresa.

3. **Adoptar ISO 31000 u OCTAVE para evaluar, tratar y monitorear riesgos de seguridad; definir criterios de aceptación y elaborar la Declaración de Aplicabilidad.**

   **Ejemplo:** Aplicar el método OCTAVE para identificar que el riesgo de pérdida de información por USBs no cifradas es alto, y definir como tratamiento la desactivación de puertos USB en equipos críticos. Incluir este control en la Declaración de Aplicabilidad (SoA) junto con la justificación de su implementación.

4. **Crear y gestionar procedimientos para todos los procesos críticos (gestión de accesos, incidentes, cambios, continuidad), almacenándolos en un repositorio accesible y**

**versionado.**

**Ejemplo:** Elaborar un procedimiento paso a paso para la gestión de incidentes, desde la detección hasta la resolución. Guardarlo en SharePoint con control de versiones. Establecer que se debe revisar cada 12 meses y capacitar al personal sobre su uso.

5. **Diseñar un programa de formación regular (seminarios, e-learning) dirigido a todo el personal, con especial foco en TI, finanzas y dirección, midiendo la eficacia con evaluaciones y simulacros**.

   **Ejemplo:** Implementar cursos virtuales sobre phishing, gestión de contraseñas y clasificación de la información usando plataformas como Moodle o Microsoft Learn. Para el área de TI, incluir talleres sobre gestión de incidentes y recuperación ante desastres. Realizar simulacros de phishing cada 3 meses y aplicar pruebas de comprensión para medir efectividad.

6. **Definir roles y responsabilidades claros (gestores de riesgos, responsables de procesos), y asegurar la disponibilidad de presupuesto para herramientas y auditorías.**

   **Ejemplo**: Nombrar a un Oficial de Seguridad de la Información como responsable del SGSI. Asignar un presupuesto anual para adquirir herramientas como antivirus corporativo, firewalls y contratar una auditoría externa de ciberseguridad.

7. **Establecer indicadores clave (tiempo de respuesta a incidentes, porcentaje de no conformidades cerradas, nivel de cumplimiento de controles) y un programa de auditorías internas anuales con informes a la alta dirección.**

   **Ejemplo:** Medir el tiempo promedio de respuesta a incidentes (meta: menos de 4 horas), y el porcentaje de controles implementados. Programar auditorías internas cada 6 meses, reportando hallazgos directamente al Comité de Dirección.

8. **Aplicar el ciclo Plan–Do–Check–Act en todos los procesos del SGSI: actualizar el análisis de riesgos tras incidentes, revisar políticas y procesos, implementar acciones correctivas y preventivas.**

   **Ejemplo:** Tras detectar un incidente de pérdida de datos, revisar el procedimiento de respaldo (Plan), actualizarlo (Do), verificar que se siga correctamente (Check) e introducir

mejoras (Act), como el cifrado de los respaldos.

9. **Desarrollar un cronograma con hitos (definición de alcance, elaboración de documentación, formación, auditoría inicial, revisión de la dirección), asignando recursos y responsables para cada actividad.**

   **Ejemplo:** Definir hitos como: diagnóstico inicial (mes 1), elaboración de documentación (meses 2-3), formación (mes 4), auditoría interna (mes 5) y auditoría externa de certificación (mes 6). Usar herramientas como Microsoft Project o Trello para dar seguimiento.

10. **Evaluar soluciones de GRC (Governance, Risk & Compliance) para automatizar el seguimiento de controles, gestión documental y generación de reportes, facilitando el mantenimiento y la auditoría del SGSI.**

    **Ejemplo:** Implementar una solución como ISMS.online o LogicManager para centralizar evidencias, automatizar reportes de cumplimiento y recibir alertas sobre vencimientos de auditorías o controles vencidos.

# CAPÍTULO VI. APLICABILIDAD

Este capítulo presenta la aplicabilidad de la propuesta de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en LEYDE, conforme a la norma ISO/IEC 27001:2022. Se detallan los elementos clave para su ejecución, incluyendo la gestión de la integración, alcance, requisitos, cronograma, costos, recursos, riesgos, análisis FODA y el plan de implementación basado en el ciclo PDCA. Esta estructura permite visualizar de forma clara y ordenada cómo se llevará a cabo la propuesta, garantizando su viabilidad técnica, organizacional y económica.

## 6.1 PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO/IEC 27001:2022 EN LEYDE.

### 6.1.1 PLANTEAMIENTO DEL PROBLEMA

En el contexto actual de transformación digital, las organizaciones enfrentan una creciente exposición a amenazas cibernéticas que comprometen la confidencialidad, integridad y disponibilidad de la información. En los últimos años, LEYDE ha dado pasos importantes hacia la modernización tecnológica, como la migración de sus sistemas a la nube y la implementación de herramientas básicas de seguridad. Sin embargo, estos esfuerzos no han sido suficientes para enfrentar los crecientes riesgos asociados a la ciberseguridad. Actualmente, la empresa no cuenta con un sistema formal que le permita gestionar de manera integral la seguridad de su información. No existen políticas documentadas, los procedimientos son informales y no se realiza una evaluación sistemática de riesgos. Además, no hay un plan estructurado para responder a incidentes ni mecanismos de auditoría o mejora continua.

Esta situación deja a la organización expuesta a múltiples amenazas, desde accesos no autorizados hasta pérdidas de información crítica. También limita su capacidad para cumplir con normativas internacionales y responder de forma efectiva ante auditorías o requerimientos de clientes. En un entorno donde los ataques cibernéticos son cada vez más frecuentes y sofisticados, no contar con un SGSI representa un riesgo real para la continuidad del negocio, la reputación de la empresa y la confianza de sus partes interesadas.

Por tanto, se recomienda de manera proactiva establecer un sistema que permita gestionar

de forma adecuada los riesgos y garantice la confidencialidad, integridad y disponibilidad de los datos, alineado con buenas prácticas y estándares internacionales como la norma ISO/IEC 27001:2022.

### 6.1.2 JUSTIFICACIÓN DEL PROYECTO

Implementar un SGSI en LEYDE, alineado con la norma ISO/IEC 27001:2022, es una decisión estratégica que responde tanto a necesidades internas como a exigencias del entorno. Desde el punto de vista operativo, permitirá establecer políticas claras, definir responsabilidades, gestionar riesgos de forma estructurada y proteger los activos de información más críticos. También facilitará la detección oportuna de amenazas, la respuesta ante incidentes y la mejora continua de los controles de seguridad.

Desde una perspectiva organizacional, el proyecto contribuirá a fortalecer la cultura de seguridad dentro de la empresa, promoviendo la capacitación del personal y la colaboración entre áreas. Además, al adoptar un estándar reconocido internacionalmente, LEYDE podrá demostrar su compromiso con la protección de la información, lo que mejora su imagen ante clientes, socios y autoridades regulatorias.

Por otro lado, el SGSI también representa una inversión inteligente. Al reducir la probabilidad de incidentes de seguridad, se minimizan los costos asociados a interrupciones operativas, pérdidas de datos o sanciones legales. Asimismo, contar con un sistema bien estructurado permite tomar decisiones más informadas, optimizar recursos y alinear la seguridad con los objetivos estratégicos del negocio. Finalmente, el proyecto se alinea con los principios de la mejora continua (PDCA), asegurando que la seguridad evolucione junto con el crecimiento de la empresa.

### 6.1.1 COBERTURA DE CLÁUSULAS ISO/IEC 27001:2022

Con base en el diagnóstico realizado a la organización, se identificaron diversas brechas en la gestión de la seguridad de la información. Estas brechas afectan directamente la conformidad con varios requisitos de la norma ISO/IEC 27001:2022, por lo que el Sistema de Gestión de Seguridad de la Información (SGSI) propuesto tiene como finalidad establecer un marco formal y estructurado que permita cerrar dichas brechas y fortalecer la postura de ciberseguridad de la empresa.

En este contexto, se detallan a continuación los elementos de las cláusulas 4 a la 10 de la norma ISO/IEC 27001:2022 que serán abordados por la presente propuesta, indicando claramente si su cobertura será total o parcial, en función de los hallazgos identificados:

- **CLÁUSULA 4: CONTEXTO DE LA ORGANIZACIÓN**

  Se abordará completamente. Se establecerá un análisis detallado del contexto interno y externo de la organización, identificando las partes interesadas relevantes y sus requerimientos en materia de seguridad. Se definirá con precisión el alcance del SGSI y sus límites, permitiendo alinear los controles con las necesidades reales del negocio.

- **CLÁUSULA 5: LIDERAZGO**

  Se cumplirá en su totalidad. El compromiso de la alta dirección será formalizado mediante la emisión de una política de seguridad, la definición de responsabilidades, y el establecimiento de roles claves para la operación del SGSI, fomentando la integración de la seguridad en la cultura organizacional.

- **CLÁUSULA 6: PLANIFICACIÓN**

  Se implementará completamente. Se diseñará un proceso de gestión de riesgos basado en la metodología OCTAVE, lo cual permitirá identificar, analizar y tratar los riesgos asociados a los activos de información. Además, se establecerán acciones concretas para abordar riesgos y oportunidades, garantizando un enfoque preventivo y estructurado.

- **CLÁUSULA 7: APOYO**

  Su cobertura será parcial. Si bien se establecerán procesos para la gestión documental, comunicación interna y provisión de recursos necesarios, el componente relacionado con la concientización y formación de todo el personal será implementado de forma gradual. Esto se debe a que el diagnóstico identificó que una parte significativa de los colaboradores aún no tiene conocimientos sobre los principios básicos de seguridad de la información, lo cual requerirá un plan progresivo de capacitación.

- **CLÁUSULA 8: OPERACIÓN**

  Será cubierta completamente. La propuesta incluye la planificación, implementación, control y evaluación continua de los procesos operativos del SGSI, así como la respuesta

ante eventos y la ejecución de controles de seguridad basados en los riesgos identificados.

- **CLÁUSULA 9: EVALUACIÓN DEL DESEMPEÑO**

  Se abordará en su totalidad. Se establecerán indicadores de desempeño, procesos de auditoría interna, y revisiones de gestión que permitan monitorear la eficacia del sistema. Esto permitirá identificar áreas de mejora y asegurar el cumplimiento de los objetivos del SGSI.

- **CLÁUSULA 10: MEJORA**

  Será cubierta completamente. Se implementará un enfoque de mejora continua basado en la detección de no conformidades, acciones correctivas, y lecciones aprendidas. Esto permitirá la evolución constante del sistema y la adaptación a nuevas amenazas y requisitos regulatorios.

## 6.2 GESTIÓN DE LA INTEGRACIÓN

### 6.2.1 ACTA DE CONSTITUCIÓN DEL PROYECTO

| Nombre del proyecto | Siglas |
|---|---|
| Propuesta de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 en LEYDE. | PISGSILEYDE |

| **Propósito del proyecto** | |
|---|---|
| Desarrollar una propuesta de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en LEYDE, basado en la norma ISO/IEC 27001:2022, y gestionado conforme a la Guía PMBOK, con el fin de fortalecer la protección, confidencialidad, integridad y disponibilidad de la información. | |
| **Objetivos del proyecto** | |
| **Objetivos** | **Criterio de éxito** |

| | |
|---|---|
| Evaluar el estado actual de la seguridad de la información en LEYDE, identificando las brechas existentes en relación con los requisitos de la norma ISO/IEC 27001:2022. | Informe de diagnóstico que identifique las brechas entre el estado actual y los requisitos de la norma, validado por personal interno del área de IT. |
| Identificar y analizar los requisitos y lineamientos establecidos en la norma ISO/IEC 27001:2022 para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). | Análisis de los requisitos de la norma, con mapeo de controles aplicables a LEYDE, aprobado por la dirección del proyecto. |
| Analizar y seleccionar metodologías, herramientas y mejores prácticas internacionales que faciliten la implementación efectiva de un SGSI en LEYDE. | Matriz comparativa de metodologías y herramientas, alineada con las necesidades de LEYDE. |
| Identificar y definir los recursos humanos, técnicos y financieros necesarios para la implementación efectiva del SGSI en LEYDE. | Documento de planificación de recursos que incluya perfiles requeridos, tecnologías necesarias y estimación de costos, validado por la gerencia. |
| Formular un plan de acción detallado que incluya un cronograma, asignación de recursos y responsabilidades, para la adopción efectiva del SGSI en LEYDE basado en ISO/IEC 27001:2022. | Plan de implementación estructurado con cronograma y entregables definidos, aprobado por los usuarios clave. |
| Identificar los desafíos y riesgos potenciales durante la implementación de la plataforma digital para la gestión empresarial y desarrollar estrategias para mitigarlos, siguiendo las mejores prácticas de la guía PMBOK. | Plan con estrategias viables aprobado por interesados para mitigar riesgos. |
| **Definición de requisitos del proyecto** | |
| – Capacitación y sensibilización del personal | |
| – Gestión de recursos. | |
| – Sistema de comunicación interna | |

| |
|---|
| – Indicadores de desempeño. |
| – Cumplimiento normativo |
| – Documentación clara y estructurada |
| – Gestión del cambio |
| – Soporte técnico y mantenimiento |
| – Evaluación y mejora continua. |
| **Descripción general del proyecto, límites y entregables claves** |
| El proyecto consiste en el desarrollo de una propuesta para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa LEYDE, tomando como base los lineamientos de la norma ISO/IEC 27001:2022 y gestionado bajo la metodología PMBOK. Esta iniciativa tiene como propósito fortalecer la protección de los activos de información de la organización, optimizar los procesos relacionados con la seguridad, y fomentar una cultura organizacional orientada a la gestión de riesgos. Con el propósito establecer una hoja de ruta clara y estructurada que permita a LEYDE avanzar hacia una gestión más segura, eficiente y alineada con estándares internacionales. |
| **Riesgos generales del proyecto: describir los riesgos generales del proyecto.** |
| Falta de apoyo de la alta dirección<br>Falta de conocimientos técnicos especializados<br>Limitaciones presupuestarias<br>Resistencia al cambio.<br>La falta de motivación del personal.<br>La falta de alineación con las necesidades de las empresas |
| **Cronograma de hitos del proyecto** |

| Hitos | Fechas programadas | |
|---|---|---|
| 1. Aprobación del Acta de Constitución del Proyecto. | 12/08/2025 | 19/08/2025 |
| 2. Investigación y Recolección de Requisitos. | 20/08/2025 | 19/09/2025 |
| 3. Diseño Conceptual de la Propuesta. | 22/09/2025 | 05/12/2025 |
| 4. Revisión y Validación de la Propuesta. | 08/12/2025 | 13/01/2026 |

| | | |
|---|---|---|
| 5. Finalización de la propuesta de Implementación del SGSI en LEYDE. | 14/01/2026 | 25/02/2026 |
| 7. Presentación final a interesados y entrega del informe del proyecto. | 27/02/2026 | |
| Recursos financieros del proyecto: mencionar los recursos financieros asignados al proyecto. | | |
| **Concepto** | **Monto** | |
| Consultoría | Lps 134,000 | |
| Servidores \| Software \| Licencias | Lps 543,005 | |
| Lista de interesados clave | | |
| Alta Dirección de LEYDE.<br>Gerente de Tecnología.<br>Responsable de Seguridad.<br>Equipo de desarrollo del proyecto.<br>Gerente del Proyecto<br>Usuarios Finales. | | |
| Requisitos de aprobación del proyecto | | |
| Cumplimiento de los objetivos planteados.<br>Aprobación de los interesados clave.<br>Validación del cumplimiento normativo.<br>Presentación formal del proyecto.<br>Aceptación formal del entregable final. | | |
| Criterios de culminación del proyecto | | |
| – Finalización de los entregables claves. | | |
| – Aprobación de la propuesta. | | |
| – Cumplimiento de los objetivos. | | |
| – Entrega de informe final. | | |
| Designación del director de proyecto | | |
| Nombre | Carlos Quiróz | Nivel de autoridad |

| | | | |
|---|---|---|---|
| Reporta a | Christian Nehring | Alto | |
| Supervisa a | Equipo del proyecto. | | |
| Patrocinador que autoriza el proyecto: mencionar al patrocinador del proyecto, así como la entidad a la que pertenece, el cargo que ocupa y la fecha de elaboración del acta de constitución del proyecto. | | | |
| Nombre | Empresa | Cargo | Fecha |
| Carlos Quiróz | LEYDE | Gerente de Tecnología | 19 de agosto 2025 |
| | | | |
| | | | |

### 6.2.2 MATRIZ DE LOS INTERESADOS

| Nombre del Interesado | Rol en el Proyecto | Interés | Influencia | Estrategia de Gestión |
|---|---|---|---|---|
| Alta Dirección de LEYDE | Patrocinador | Asegurar el cumplimiento normativo y la protección de la información | Alta | Involucrar activamente y mantener informada |
| Gerente de TI | Responsable Técnico | Implementar mejoras en la seguridad de la infraestructura tecnológica | Alta | Consultar y coordinar decisiones técnicas |
| Personal Administrativo | Usuarios Finales | Afectados por los nuevos procedimientos y controles de seguridad | Media | Capacitar y sensibilizar |
| Departamento Legal | Asesor Legal | Verificar cumplimiento con normativas y regulaciones | Media | Consultar en temas de cumplimiento |
| Consultor Externo | Asesor del Proyecto | Apoyar en el diseño de la propuesta y alineación con ISO/IEC 27001:2022 | Alta | Involucrar en fases clave del proyecto |
| Departamento de Recursos Humanos | Apoyo en Gestión del Cambio | Facilitar la comunicación y capacitación del personal | Media | Coordinar actividades de formación y comunicación |
| Auditor Interno | Evaluador | Verificar la | Alta | Incluir en |

| | | | | |
|---|---|---|---|---|
| | | calidad y cumplimiento de la propuesta | | revisiones y validaciones |
| Usuarios Finales (colaboradores) | Afectados por el SGSI | Utilizarán los procedimientos y herramientas del SGSI | Baja | Informar, capacitar y recoger retroalimentación |

## 6.3 GESTIÓN DEL ALCANCE

| CONTROL DE VERSIONES | | | | | |
|---|---|---|---|---|---|
| ***Versión*** | ***Hecha por*** | ***Revisada por*** | ***Aprobada por*** | ***Fecha*** | ***Motivo*** |
| 1.0 | Equipo proyecto Propuesta SGSI ISO 27001:2022 Leyde | | Dirección de proyecto | | Creación de documento inicial |

### 6.3.1 PLAN DE GESTIÓN DEL ALCANCE

| NOMBRE DEL PROYECTO | SIGLAS DEL PROYECTO |
|---|---|
| Propuesta de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 en LEYDE. | PISGSILEYDE |

| PROCESO DE DEFINICIÓN DEL ALCANCE |
|---|
| El alcance del proyecto será definido a partir del análisis de riesgos y necesidades internas identificadas en la empresa Leyde. Este proceso incluirá la recopilación de información |

mediante encuestas y entrevistas con personal clave, permitiendo delimitar los activos de información, procesos críticos y áreas prioritarias para la implementación del SGSI. La definición del alcance se desarrollará durante la fase de planificación, utilizando metodologías reconocidas como ISO/IEC 27001 y OCTAVE, y será validada por el equipo técnico y la alta dirección de la organización.

**DIAGRAMA DE PROCESO DE DEFINICIÓN DE ALCANCE**

Este diagrama muestra las etapas para definir el alcance del SGSI en Leyde, desde la revisión de requisitos y activos críticos hasta la validación final por la dirección, siguiendo los lineamientos de la norma ISO/IEC 27001:2022.

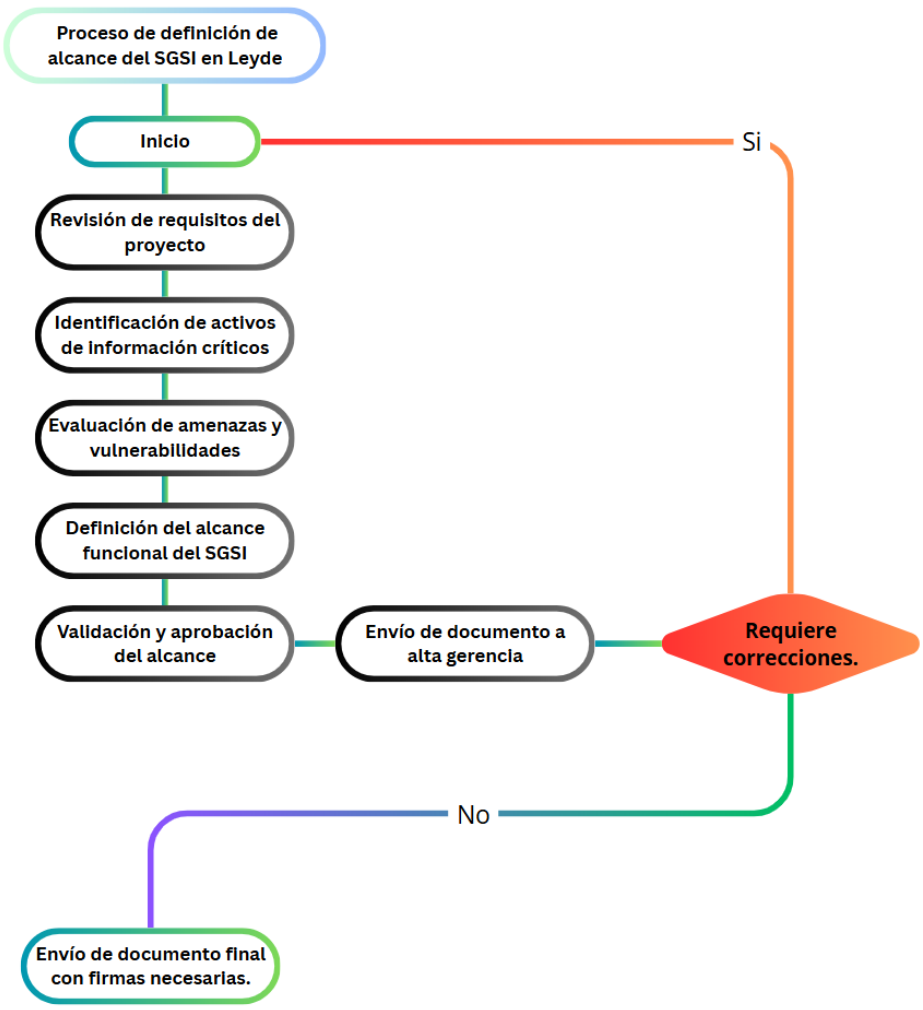
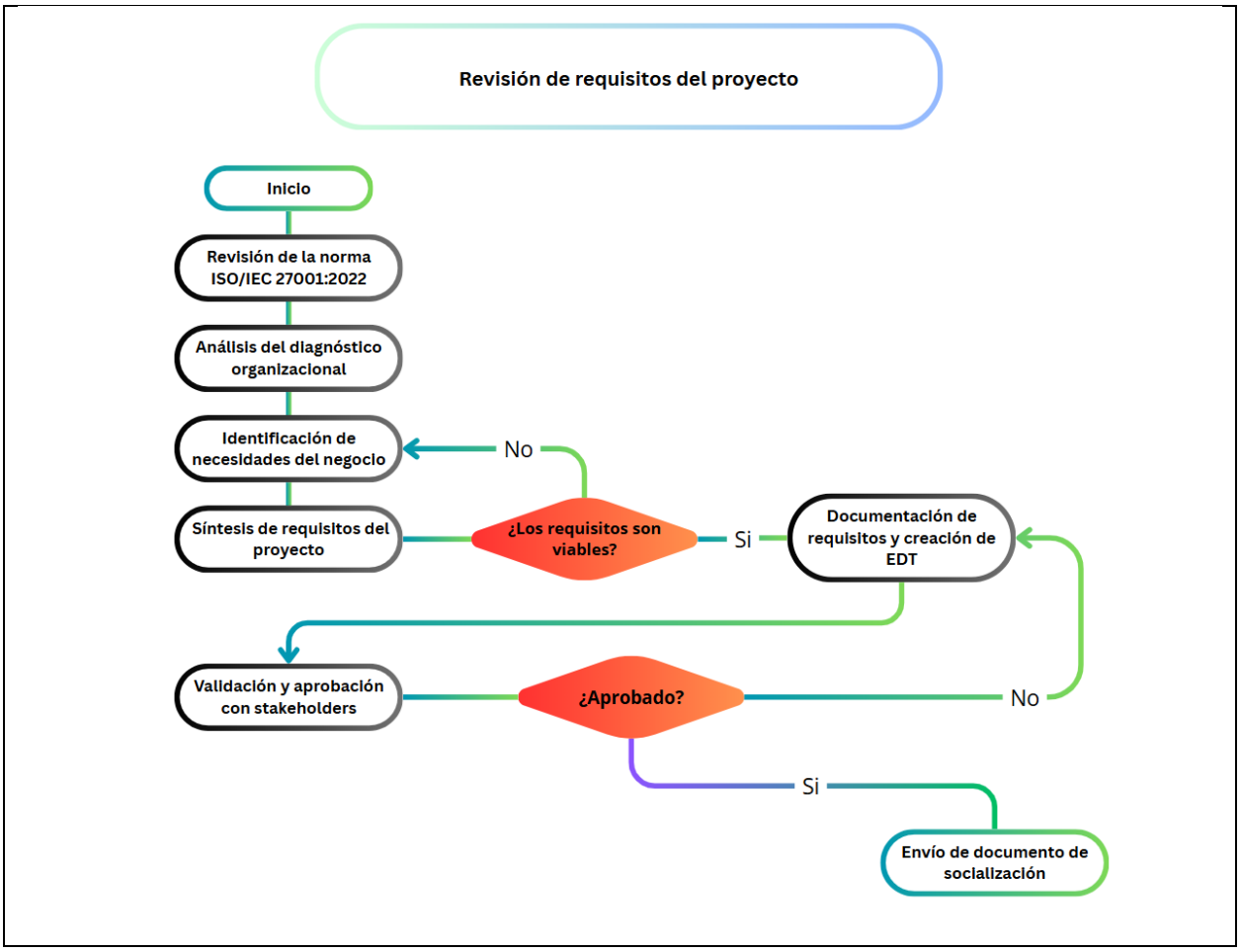
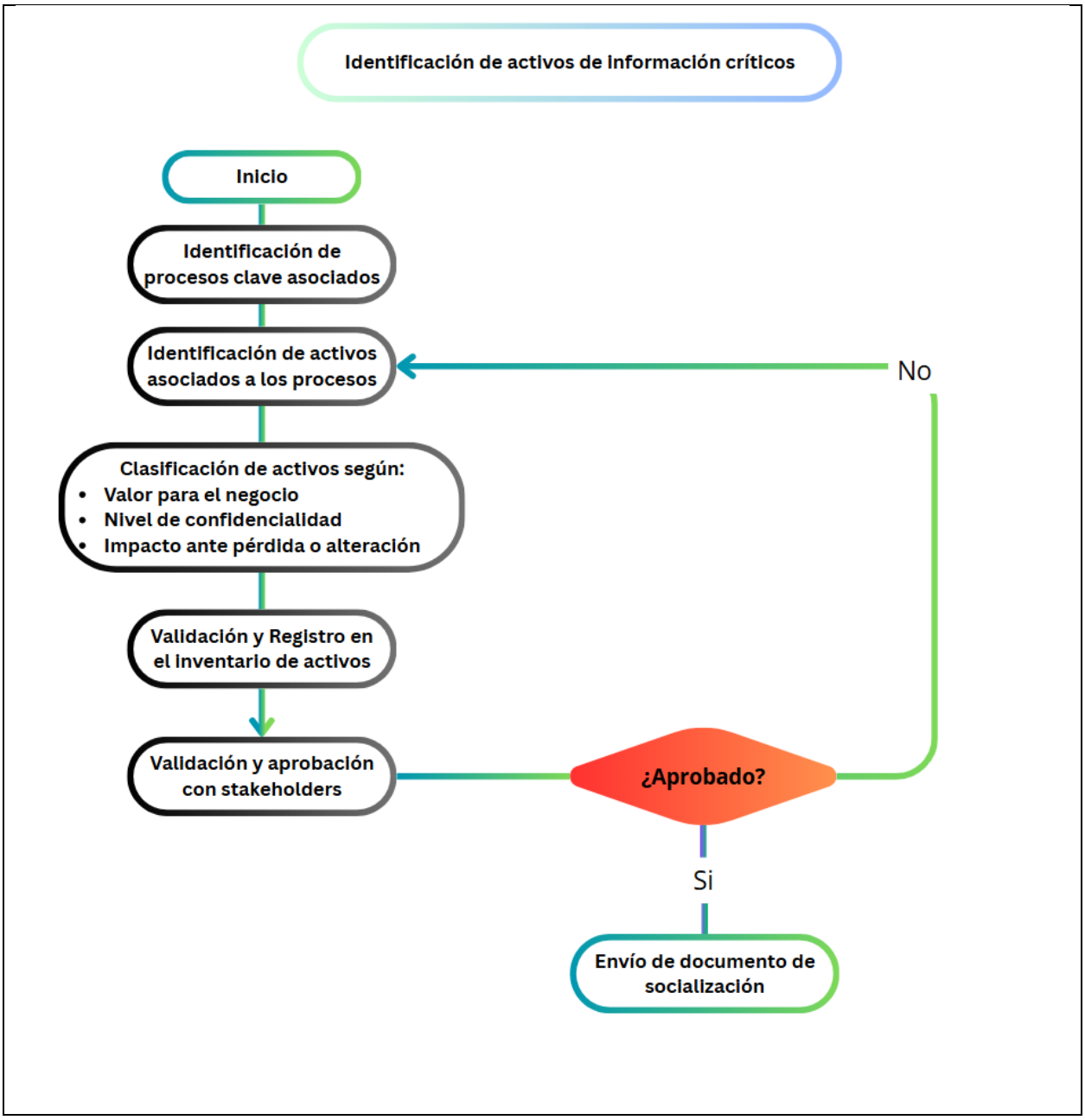



**DIAGRAMA DE REVISIÓN DE REQUISITOS DEL PROYECTO**

Este diagrama ilustra el flujo de actividades involucradas en la revisión de requisitos del proyecto para la implementación del SGSI en Leyde. Inicia con la revisión de la norma ISO/IEC 27001:2022, y por el análisis del diagnóstico organizacional, seguido por algunos elementos de documentación necesaria, elaboración de un EDT y validación de requisitos con los stakeholders. Incluye puntos de decisión clave para asegurar la viabilidad y aprobación de los requisitos antes de su socialización final.




| **DIAGRAMA DE IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN CRÍTICOS** |
| --- |
| Este diagrama detalla el proceso de identificación de criticidad de activos y procesos importantes en los que se utilizan, así mismo, se propone la clasificación de los mismos y su respectivo registro en el inventario de activos de información. |




| **DIAGRAMA DE IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES (OCTAVE)** |
| --- |
| Este gráfico representa el flujo de actividades claves dentro de la metodología OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), enfocándose en la identificación de escenarios de riesgo y el análisis de impacto a la organización. El proceso inicia con la preparación del análisis, continúa con la identificación de activos, |

amenazas y vulnerabilidades, y culmina con la evaluación del impacto de los riesgos identificados y la definición de planes de acción priorizados para mitigar dichos riesgos.

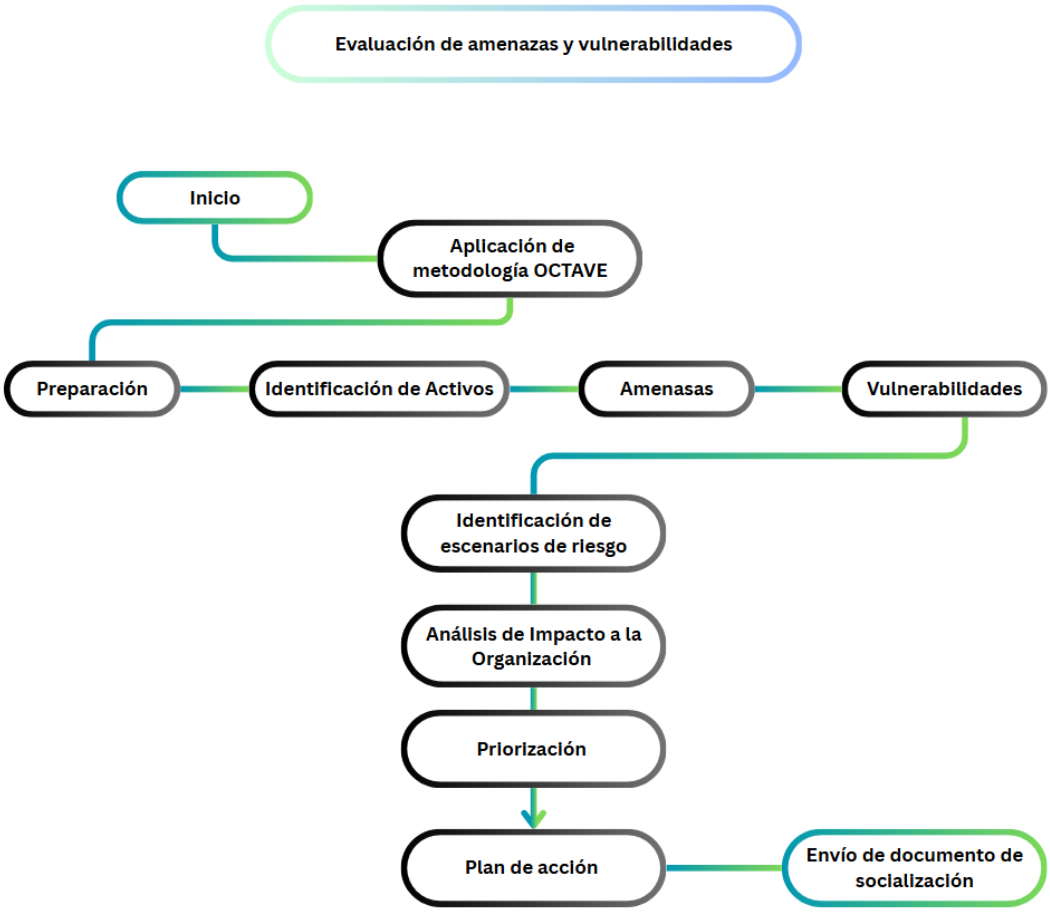



**DIAGRAMA DE DEFINICIÓN DEL CALCANCE FUNCIONAL DEL SGSI**

El Siguiente gráfico muestra los elementos clave considerados en la definición del alcance funcional del Sistema de Gestión de Seguridad de la Información (SGSI). Se representan las áreas organizativas, activos y procesos que se incluyen dentro del alcance, así como las exclusiones justificadas que quedan fuera por razones técnicas, operativas o estratégicas. Además, se incluyen los criterios utilizados para tomar decisiones sobre qué incluir o excluir, y se destaca la importancia de la validación del alcance por las partes interesadas relevantes.

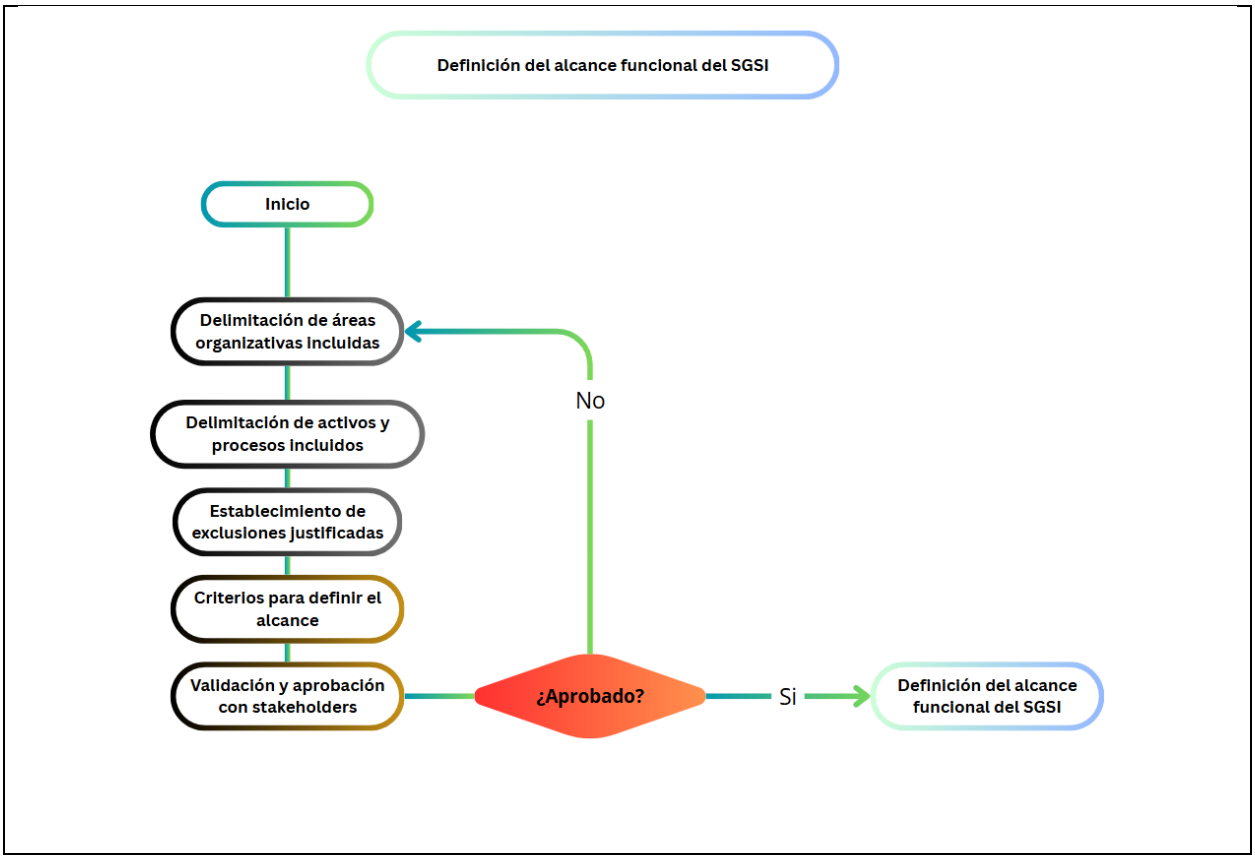
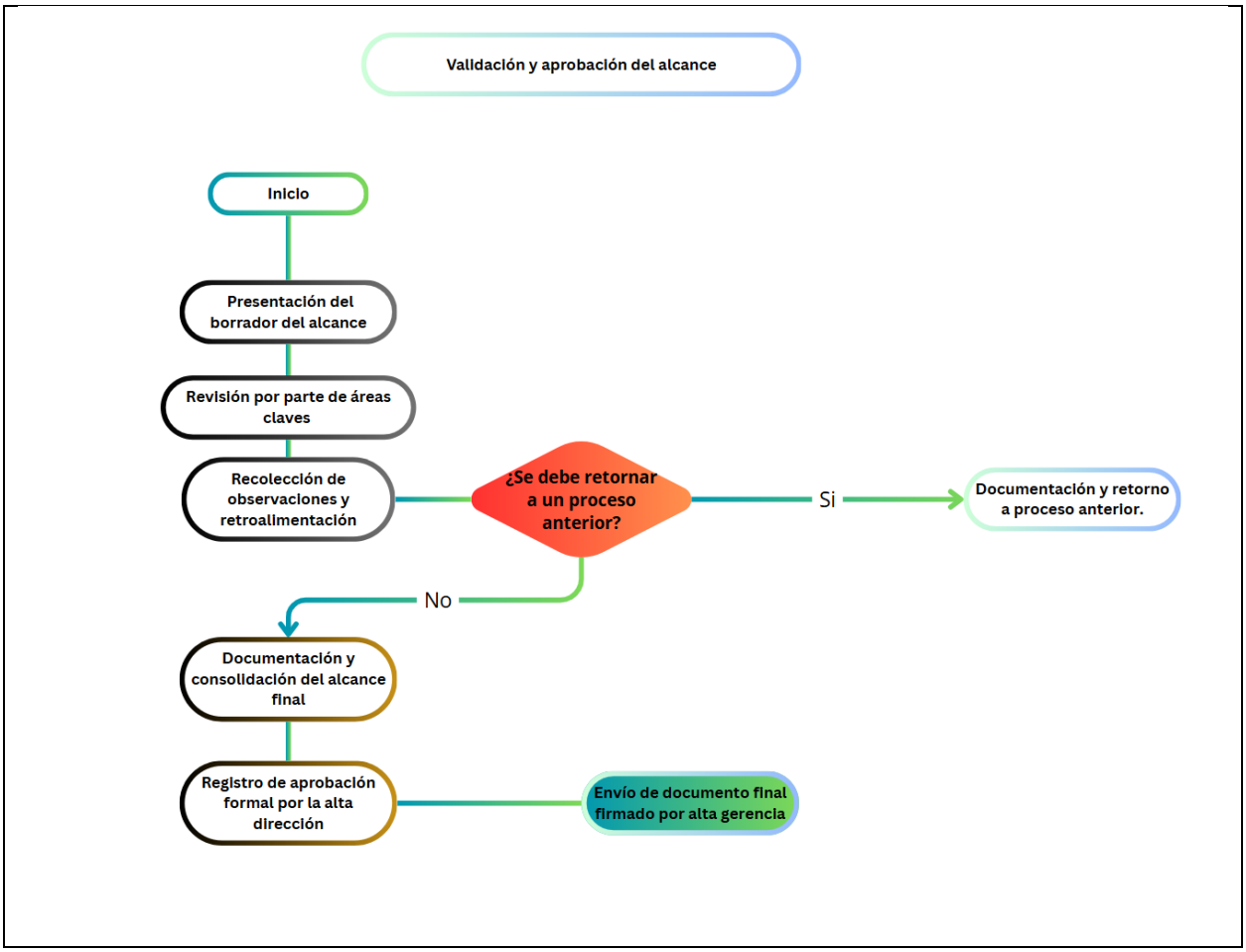



**DIAGRAMA DE VALIDACIÓN Y APROBACIÓN DEL ALCANCE**

El gráfico representa el proceso de presentación, revisión y aprobación del borrador del alcance funcional del Sistema de Gestión de Seguridad de la Información (SGSI). Incluye la elaboración inicial del borrador, la identificación de las partes interesadas clave, la revisión por parte de las áreas involucradas, la recopilación de observaciones, y la incorporación de ajustes necesarios. Finalmente, se muestra la validación y aprobación formal por la alta dirección, asegurando el compromiso organizacional y la alineación estratégica del alcance del SGSI. Este proceso garantiza que el alcance sea preciso, consensuado y aplicable a la realidad de la organización.




## 6.4 GESTIÓN DE REQUISITOS

| CONTROL DE VERSIONES | | | | | |
|---|---|---|---|---|---|
| ***Versión*** | ***Hecha por*** | ***Revisada por*** | ***Aprobada por*** | ***Fecha*** | ***Motivo*** |
| 1.0 | Equipo proyecto Propuesta SGSI ISO 27001:2022 Leyde | | Dirección de proyecto | | Creación de documento inicial |

### 6.4.1 PLAN DE GESTIÓN DE LOS REQUISITOS

| NOMBRE DEL PROYECTO | SIGLAS DEL PROYECTO |
|---|---|
| Propuesta de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 en LEYDE. | PISGSILEYDE |

| ACTIVIDADES DE REQUISITOS |
|---|
| Las actividades relacionadas con los requisitos estarán enfocadas en identificar, documentar y validar las necesidades clave de la empresa Leyde para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), de acuerdo con la norma ISO/IEC 27001:2022.<br><br>Estas actividades se realizarán mediante:<br><br>• **Planificación:** Recolección inicial de información mediante encuestas, entrevistas y revisión documental con personal clave de áreas como IT, Finanzas, Contabilidad, Recursos Humanos y otras áreas operativas.<br><br>• **Monitoreo:** Seguimiento del progreso en la definición de requisitos, mediante sesiones semanales de revisión con el equipo responsable del proyecto, para validar avances y realizar ajustes necesarios.<br><br>• **Reporte:** Elaboración de un informe consolidado que contenga los requisitos funcionales (políticas, controles, procedimientos) y no funcionales (capacitación, cultura organizacional, recursos) necesarios para la implementación efectiva del SGSI. |
| |
| **ACTIVIDADES DE GESTIÓN DE LA CONFIGURACIÓN** |
| Cualquier modificación en los requisitos identificados durante el desarrollo de la propuesta será gestionada mediante un proceso estructurado, que garantice el control y trazabilidad de los cambios: |

- **Inicio del Cambio:** Cualquier parte interesada podrá proponer ajustes a los requisitos a través de un formulario estandarizado de solicitud de cambio.
- **Análisis del Impacto:** El equipo del proyecto evaluará el impacto de cada solicitud en la planificación, alcance y objetivos de la implementación del SGSI.
- **Aprobación**: Los cambios serán aprobados por el líder del proyecto, en coordinación con los responsables de las áreas clave involucradas.
- **Rastreo:** Todas las solicitudes y cambios serán registrados y controlados mediante una hoja de seguimiento en Excel, la cual será actualizada periódicamente.
- **Reporte**: Los cambios aceptados serán incorporados en versiones actualizadas del documento de requisitos, y se socializarán con las partes interesadas.

**PROCESO DE PRIORIZACIÓN DE REQUISITOS**

Los requisitos serán priorizados utilizando una matriz de valoración basada en criterios como:

- **Impacto en la seguridad de la información**
- **Cumplimiento normativo**
- **Urgencia operativa**
- **Viabilidad técnica y organizacional**

Durante las sesiones con los responsables de área, se aplicará el modelo **MoSCoW**, clasificando cada requisito en las siguientes categorías:

- **Must have (Debe tener)**
- **Should have (Debería tener)**
- **Could have (Podría tener)**
- **Won't have (No tendrá por ahora)**

Este enfoque permitirá enfocar los esfuerzos en los elementos más críticos para el éxito

| |
|---|
| de la implementación del SGSI. |
| **Estructura de Trazabilidad** |
| Los atributos capturados en la matriz de trazabilidad incluirán el ID del requisito, su descripción, prioridad asignada, estado (pendiente, en progreso, completado) y el origen del requisito (entrevistas, encuestas, normativa ISO/IEC 27001:2022, etc.). La trazabilidad se establecerá en relación con documentos clave del proyecto como el enunciado del alcance, la Estructura de Desglose del Trabajo (EDT) y los entregables planificados.<br><br>Esta trazabilidad permitirá verificar que cada requisito esté correctamente alineado con los objetivos del SGSI y sus componentes, facilitando así el monitoreo, control y gestión de cambios durante el desarrollo del proyecto. |

### 6.4.2 DOCUMENTACIÓN DE REQUISITOS

| **CONTROL DE VERSIONES** | | | | | |
|---|---|---|---|---|---|
| ***Versión*** | ***Hecha por*** | ***Revisada por*** | ***Aprobada por*** | ***Fecha*** | ***Motivo*** |
| 1.0 | Equipo proyecto Propuesta SGSI ISO 27001:2022 Leyde | | Dirección de proyecto | | Creación de documento inicial |

| **NOMBRE DEL PROYECTO** | **SIGLAS DEL PROYECTO** |
|---|---|
| Propuesta de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 en LEYDE | PISGSILEYDE |

| REQUISITOS DEL NEGOCIO | | | |
|---|---|---|---|
| Código | Descripción del Requisito | Fuente | Prioridad |
| RN-01 | Establecer un SGSI para proteger la información sensible de la empresa | Dirección General | Must Have |
| RN-02 | Cumplir con requisitos regulatorios y contractuales en materia de seguridad | Departamento Legal | Must Have |
| RN-03 | Mejorar la confianza de los colaboradores, clientes y proveedores respecto al manejo de su información | Entrevistas ejecutivas | Should Have |

| REQUISITOS DE LOS INTERESADOS | | | |
|---|---|---|---|
| Código | Descripción del Requisito | Fuente | Prioridad |
| RI-01 | Capacitación al personal sobre políticas de seguridad | Encuesta interna | Must Have |
| RI-02 | Definir roles y responsabilidades claras en seguridad de la información | Área de RR. HH. | Should Have |
| RI-03 | Accesos limitados y controlados a sistemas de información | Departamento de IT | Must Have |
| RI-04 | Documentación accesible sobre los procedimientos de seguridad | Personal operativo | Could Have |

| REQUISITOS DE SOLUCIONES | | | |
|---|---|---|---|
| Código | Descripción del Requisito | Fuente | Prioridad |
| *3.1 Requisitos funcionales: Elementos que describen lo que debe hacer el sistema o la solución.* | | | |
| RS-01 | Implementar un sistema de control de accesos por perfiles y permisos | Revisión de normativa | Must Have |
| RS-02 | Establecer una plataforma para el registro y seguimiento de incidentes de seguridad | Análisis comparativo | Should Have |

| | | | |
|---|---|---|---|
| RS-03 | Incorporar autenticación multifactor en sistemas críticos | Mejores prácticas ISO | Must Have |
| RS-04 | Sistema automatizado de respaldo de información sensible | Departamento de TI | Could Have |
| RS-05 | Desarrollar una política de control de dispositivos extraíbles (USB, discos externos) | Encuestas internas | Should Have |
| RS-06 | Crear una base de conocimiento interna sobre procedimientos de seguridad | Entrevistas a usuarios clave | Could Have |
| RS-07 | Implementar herramientas de monitoreo y alertas sobre accesos no autorizados | Departamento de IT | Must Have |
| RS-08 | Establecer mecanismos de validación de integridad para archivos sensibles | Buenas prácticas de seguridad | Could Have |
| RS-09 | Automatizar el registro de logs de eventos y accesos | Revisión técnica | Must Have |
| RS-10 | Implementar políticas de cambio de contraseñas con complejidad definida | Departamento de RRHH / TI | Should Have |
| *3.2 Requisitos no funcionales: Describen cómo debe comportarse el sistema o las condiciones en las que opera, incluyendo seguridad, rendimiento, disponibilidad, etc.* | | | |
| RS-11 | Configurar una red segmentada para sistemas críticos | Auditoría técnica | Should Have |
| RS-12 | Configurar acceso remoto seguro mediante VPN corporativa con control de dispositivos | Requerimiento operativo | Should Have |
| RS-13 | La solución debe ser compatible con los sistemas operativos y plataformas existentes en la organización, incluyendo servidores Windows y Linux. | Revisión técnica interna | Should Have |
| RS-14 | Toda la información generada por el SGSI debe almacenarse durante al menos 2 años, cumpliendo con políticas internas y requisitos | Políticas internas / Auditoría | Must Have |

| | | | |
|---|---|---|---|
| | legales. | | |

| REQUISITOS DE TRANSICIÓN Y PREPARACIÓN | | | |
|---|---|---|---|
| Código | Descripción del Requisito | Fuente | Prioridad |
| RT-01 | Capacitar al personal clave sobre la nueva estructura y objetivos del SGSI | Encuestas internas | Must Have |
| RT-02 | Migrar los registros existentes de seguridad a la nueva estructura documental del SGSI | Departamento de IT | Should Have |
| RT-03 | Establecer un calendario de transición de políticas y procedimientos vigentes | Comité de Seguridad | Must Have |
| RT-04 | Comunicar oficialmente a toda la organización el inicio de la implementación del SGSI | Dirección General | Must Have |

| REQUISITOS DEL PROYECTO | | | |
|---|---|---|---|
| Código | Descripción del Requisito | Fuente | Prioridad |
| RP-01 | Definir un cronograma detallado con fases, entregables y responsables | Coordinación del proyecto | Must Have |
| RP-02 | Asignar recursos humanos con experiencia en ciberseguridad y gestión de riesgos | Dirección / RR. HH. | Must Have |
| RP-03 | Disponer de presupuesto para adquisición de herramientas tecnológicas específicas | Coordinación del proyecto/Finanzas | Should Have |
| RP-04 | Realizar reuniones periódicas de seguimiento del plan de implementación | Planificación interna | Must Have |

| REQUISITOS DE CALIDAD |
|---|

| Código | Descripción del Requisito | Fuente | Prioridad |
|---|---|---|---|
| RQ-01 | Verificar que todos los controles establecidos cumplan con los objetivos del Anexo A de ISO/IEC 27001:2022 | Auditoría interna | Must Have |
| RQ-02 | Realizar pruebas de validación de políticas y procedimientos antes de su liberación final | Comité de Calidad | Should Have |
| RQ-03 | Documentar evidencias de cumplimiento en cada fase del proyecto | Manual de Calidad Leyde | Must Have |
| RQ-04 | Garantizar que los documentos generados sean revisados y aprobados antes de su publicación | Normativa interna | Must Have |

### 6.4.3 MATRIZ DE TRAZABILIDAD DE REQUISITOS

| ATRIBUTOS DE REQUISITOS | | | | | TRAZABILIDAD HACIA | |
|---|---|---|---|---|---|---|
| Código | Descripción | Sustentado por | Prioridad | Estado | Objetivos del proyecto | Alcance del proyecto |
| RS-02 | Registrar incidentes de seguridad con clasificación y detalle | ISO/IEC 27001:2022 / Usuarios | A | IP | Fortalecer el control y seguimiento de incidentes | Incorpora funciones clave del SGSI |
| RS-03 | Autenticación multifactor para sistemas críticos | Buenas prácticas ISO / Auditoría | A | P | Aumentar protección de accesos no autorizados | Aplicable a sistemas sensibles y de alto riesgo |
| RT-01 | Capacitación al personal | Encuestas internas | A | IP | Preparar al personal para la | Aplicable a personal de |

| | | | | | | |
|---|---|---|---|---|---|---|
| | clave sobre objetivos del SGSI | | | | transición | áreas estratégicas |
| RP-01 | Definir cronograma detallado con entregables y responsables | Coordinación del proyecto | A | C | Planificar ordenadamente la implementación del SGSI | Fase de planificación del proyecto |
| RS-12 | Acceso remoto seguro mediante VPN corporativa con control de dispositivos autorizados | Requerimiento operativo | M | P | Minimizar riesgos por trabajo remoto | Aplica a usuarios con privilegios fuera de planta |
| RQ-03 | Documentar evidencias de cumplimiento en cada fase del proyecto | Manual de calidad interno | A | IP | Facilitar auditorías y validación del proyecto | Durante ejecución y cierre del proyecto |
| | | | | | | |
| | | | | | | |

**SIMBOLOGÍA**

| Estado Actual | |
|---|---|
| Código | Descripción |
| P | Pendiente |
| IP | En progreso |
| C | Completado |

| Prioridad | |
|---|---|
| Código | Descripción |
| A | Alta |
| M | Media |
| B | Baja |

| CONTROL DE VERSIONES | | | | | |
|---|---|---|---|---|---|
| ***Versión*** | ***Hecha por*** | ***Revisada por*** | ***Aprobada por*** | ***Fecha*** | ***Motivo*** |
| 1.0 | Equipo proyecto Propuesta SGSI ISO 27001:2022 Leyde | | Dirección de proyecto | | Creación de documento inicial |

| **NOMBRE DEL PROYECTO** | **SIGLAS DEL PROYECTO** |
|---|---|
| Propuesta de implementación de un sistema de gestión de seguridad de la información (SGSI) basado en ISO/IEC 27001:2022 en Leyde. | Propuesta SGSI ISO 27001:2022 Leyde |

| **DEFINICIÓN DEL ALCANCE DEL PROYECTO** |
|---|
| El alcance del proyecto se limita a la planificación e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa Leyde, conforme a los lineamientos establecidos por la norma ISO/IEC 27001:2022.<br><br>Este alcance comprende la identificación de activos de información críticos, evaluación de riesgos, diseño e implementación de controles de seguridad, elaboración de políticas y procedimientos, y capacitación del personal en temas relacionados con la gestión de la seguridad de la información.<br><br>El proyecto se centrará en las áreas operativas, administrativas y tecnológicas que manejan información sensible, excluyendo por el momento sedes externas o procesos que no involucren el tratamiento directo de información digital o documental. |

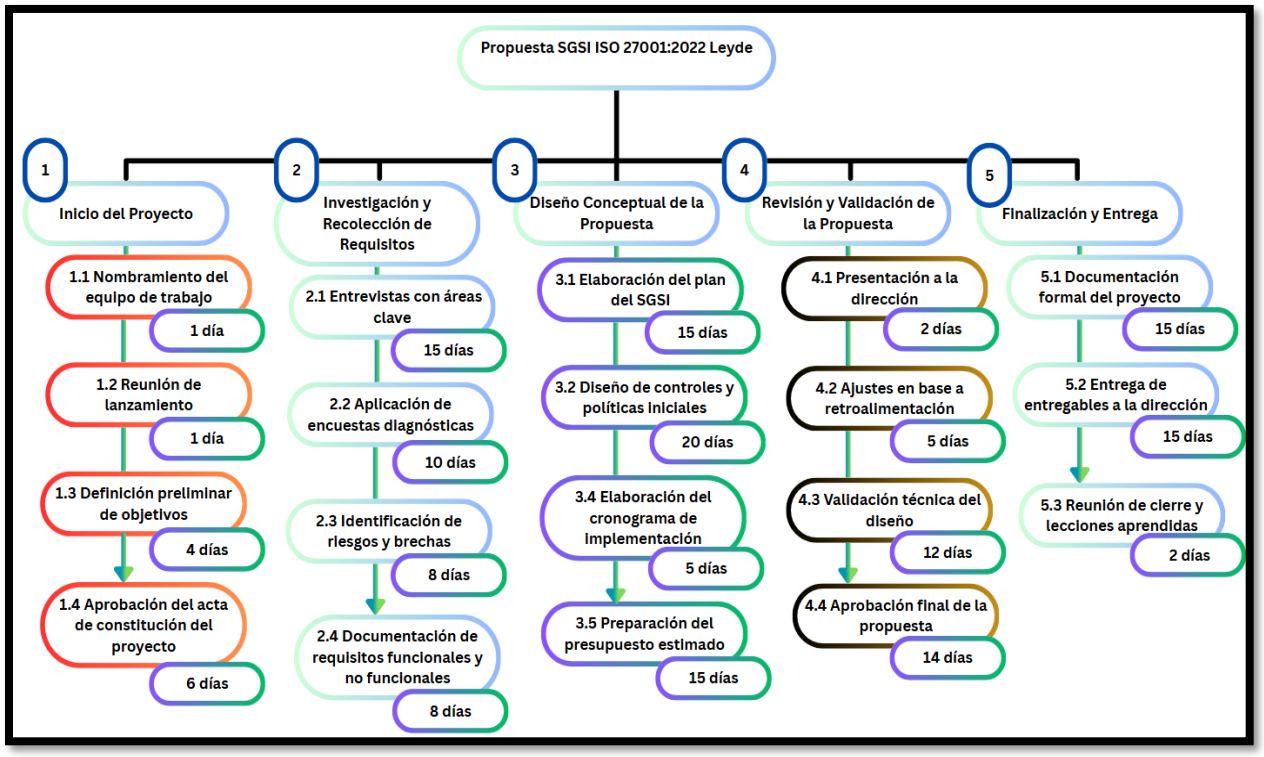
| | |
|---|---|
| Cualquier integración con otras normas o sistemas de gestión (por ejemplo, ISO 9001 o ISO 22301) quedará fuera del alcance de este proyecto inicial. | |
| **ENTREGABLES DEL PROYECTO** | |
| **Etapas del proyecto** | **Entregables del proyecto** |
| **Inicio y diagnóstico** | Informe diagnóstico de seguridad de la información actual en Leyde |
| **Planificación del SGSI** | Plan de trabajo detallado, análisis de riesgos, plan de tratamiento, política SGSI inicial |
| **Diseño de controles y documentación** | Manuales, políticas, procedimientos y matriz de controles alineados a ISO/IEC 27001:2022 |
| **Implementación inicial** | Evidencias de ejecución de controles, configuraciones técnicas, sesiones de capacitación |
| **Seguimiento y evaluación** | Informes de auditoría interna, plan de acciones correctivas, lista de lecciones aprendidas |
| **Cierre del proyecto** | Documento final de cierre, presentación ejecutiva, entrega formal del SGSI documentado |
| **CRITERIOS DE ACEPTACIÓN DEL PROYECTO** | |
| **Entregable** | **Criterios de Aceptación** |
| **Informe diagnóstico de seguridad de la información** | • Debe incluir identificación de activos, brechas de seguridad y resumen ejecutivo.<br>• Validado por el área de IT y aprobado por la dirección. |

| | |
|---|---|
| **Plan de trabajo y planificación del SGSI** | • Debe incluir cronograma, responsables, alcance, riesgos y objetivos específicos.<br>• Aprobado por el comité del proyecto. |
| **Análisis de riesgos y plan de tratamiento** | • Debe aplicar una metodología aceptada (como OCTAVE).<br>• Debe contener clasificación de activos, amenazas, vulnerabilidades y plan de acciones. |
| **Políticas y procedimientos SGSI** | • Documentos deben estar alineados con los controles del Anexo A de ISO/IEC 27001:2022.<br>• Revisión aprobada por la Alta Dirección y publicada internamente. |
| **Evidencias de implementación** | • Capturas, informes técnicos, actas de reuniones y registros de actividades realizadas.<br>• Revisados por el líder del proyecto y el área de seguridad. |
| **Registros de capacitación** | • Listas de asistencia, material entregado y evaluaciones de conocimiento realizadas.<br>• Al menos el 80% del personal objetivo debe haber participado. |
| **Informe de auditoría interna** | • Realizado según procedimiento definido.<br>• Identifica no conformidades y |

| | |
|---|---|
| | oportunidades de mejora documentadas |
| **Documento de cierre del proyecto** | • Incluye resumen de logros, cumplimiento del alcance, entregables y lecciones aprendidas.<br>• Firmado por el líder del proyecto y aceptado por la Alta Dirección. |

### 6.4.4 ESTRUCTURA DE DESGLOSE DE TRABAJO (EDT)

El siguiente diagrama de Estructura de Desglose del Trabajo (EDT) presenta la organización jerárquica de las principales actividades necesarias para la realización del proyecto de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa Leyde, basado en la norma ISO/IEC 27001:2022. Esta herramienta permite visualizar de forma estructurada las fases, entregables y tareas específicas del proyecto, facilitando su planificación, control y seguimiento.



### 6.4.5 DICCIONARIO DE LA EDT

El Diccionario de la EDT complementa el diagrama de estructura del proyecto, proporcionando una descripción detallada de cada componente. Incluye actividades, entregables, criterios de aceptación, recursos, duración y costos asociados. Su objetivo es asegurar claridad en la ejecución y control del proyecto de implementación del SGSI en Leyde, conforme a la norma ISO/IEC 27001:2022.

| **INICIO DEL PROYECTO** | |
|---|---|
| **ELEMENTO** | **DETALLE** |
| **Descripción** | Inicio formal del proyecto, definición del equipo, alcance preliminar y objetivos generales. |
| **Criterio de Aceptación** | Acta de constitución firmada y equipo de trabajo definido. |
| **Entregables** | Acta del proyecto, estructura del equipo, plan preliminar de trabajo. |
| **Supuestos** | Alta dirección aprueba el proyecto; disponibilidad de personal clave. |
| **Recursos Asignados** | Director del Proyecto, Gerente de Seguridad, Dirección General. |
| **Duración Estimada** | 10 días. |
| **Hitos** | Aprobación del proyecto y primera reunión oficial del equipo. |
| **Costos** | Tiempo del personal directivo y administrativo. |
| Firma del director del Proyecto | |

| **INVESTIGACIÓN Y RECOLECCIÓN DE REQUISITOS** |
|---|

| ELEMENTO | DETALLE |
|---|---|
| **Descripción** | Recopilación de información sobre el estado actual, necesidades, brechas y requisitos funcionales. |
| **Criterio de Aceptación** | Documento validado de requerimientos funcionales y no funcionales. |
| **Entregables** | Informe de diagnóstico, matriz de requisitos, lista de activos críticos. |
| **Supuestos** | Acceso a la información y disponibilidad del personal para entrevistas y encuestas. |
| **Recursos Asignados** | Analistas de seguridad, Líder Técnico, Usuarios clave. |
| **Duración Estimada** | 40 días. |
| **Hitos** | Entrega del informe diagnóstico y validación por stakeholders. |
| **Costos** | Tiempo del equipo técnico, herramientas de encuestas, análisis de datos. |
| Firma del director del Proyecto | |

| DISEÑO CONCEPTUAL DE LA PROPUESTA | |
|---|---|
| **ELEMENTO** | **DETALLE** |
| **Descripción** | Definición del diseño técnico y organizativo del SGSI, controles a implementar y recursos necesarios. |
| **Criterio de Aceptación** | Documento de propuesta aprobado por dirección y stakeholders. |
| **Entregables** | Plan del SGSI, diseño de controles, cronograma de implementación, presupuesto estimado. |

| | |
|---|---|
| **Supuestos** | Disponibilidad para revisión y aporte de áreas técnicas y administrativas. |
| **Recursos Asignados** | Equipo de Seguridad, Analistas TI, Consultor ISO. |
| **Duración Estimada** | 40 días. |
| **Hitos** | Aprobación formal del diseño conceptual. |
| **Costos** | Análisis técnico, tiempo del equipo, reuniones de validación. |
| Firma del director del Proyecto | |

| **REVISIÓN Y VALIDACIÓN DE LA PROPUESTA** | |
|---|---|
| **ELEMENTO** | **DETALLE** |
| **Descripción** | Presentación de la propuesta a la dirección, revisión por expertos y ajustes según retroalimentación. |
| **Criterio de Aceptación** | Validación formal del diseño del SGSI y controles propuestos. |
| **Entregables** | Acta de aprobación, versión final de la propuesta, listado de ajustes realizados. |
| **Supuestos** | Retroalimentación clara y participación activa de los revisores. |
| **Recursos Asignados** | Comité de Proyecto, Dirección General, Consultores externos (opcional). |
| **Duración Estimada** | 20 días. |
| **Hitos** | Validación del diseño final del SGSI. |
| **Costos** | Tiempo de revisión, ajustes técnicos, sesiones de retroalimentación. |
| Firma del director del | |

| | |
|---|---|
| Proyecto | |

| **FINALIZACIÓN Y ENTREGA** | |
|---|---|
| **ELEMENTO** | **DETALLE** |
| **Descripción** | Consolidación de entregables, documentación final, reunión de cierre y presentación ejecutiva. |
| **Criterio de Aceptación** | Entregables aprobados y firmados por la dirección; cierre documentado del proyecto. |
| **Entregables** | Informe final del proyecto, documentos del SGSI, acta de cierre. |
| **Supuestos** | No se requieren cambios mayores de último momento. |
| **Recursos Asignados** | Director del Proyecto, Equipo Técnico, Dirección General. |
| **Duración Estimada** | 20 días. |
| **Hitos** | Cierre formal del proyecto. |
| **Costos** | Tiempo administrativo, edición final de documentos, logística de presentación. |
| Firma del director del Proyecto | |

## 6.5 GESTIÓN DE LAS COMUNICACIONES DEL PROYECTO

### 6.5.1 MATRIZ DE COMUNICACIONES DEL PROYECTO

| Elemento de la EDT | Objetivo | Usuario | Responsabilidad | Tiempo |
|---|---|---|---|---|
| **Inicio del Proyecto** | Informar el inicio formal del proyecto y establecer roles | Alta Dirección, Gerente de Proyecto | Gerente de Proyecto | Primera semana del proyecto |
| **Investigación y Recolección de Requisitos** | Recopilar información clave y validar necesidades | Usuarios Clave, Departamento TI | Analista de Requisitos | Durante la fase de levantamiento |

| | | | | |
|---|---|---|---|---|
| **Diseño Conceptual de la propuesta** | Presentar el diseño preliminar del SGSI | Gerente de Proyecto, Consultores | Equipo de Diseño | Una vez finalizado el análisis de requisitos |
| **Revisión y Validación de la Propuesta** | Obtener retroalimentación y aprobación de la propuesta | Alta Dirección | Gerente de Proyecto | Después del diseño conceptual |
| **Finalización y entrega** | Entregar la propuesta final y cerrar el proyecto | Alta Dirección, Usuarios Finales | Gerente de Proyecto | Última semana del proyecto |

## 6.6 GESTIÓN DEL CRONOGRAMA

### 6.6.1 PLAN DE GESTIÓN DEL CRONOGRAMA

| CONTROL DE VERSIONES | | | | | |
|---|---|---|---|---|---|
| ***Versión*** | ***Hecha por*** | ***Revisada por*** | ***Aprobada por*** | ***Fecha*** | ***Motivo*** |
| 1.0 | Equipo Proyecto PISGSILEYDE | | Dirección Proyecto | | Creación inicial del documento |

| NOMBRE DEL PROYECTO | SIGLAS DEL PROYECTO |
|---|---|
| Propuesta de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 en LEYDE. | PISGSILEYDE |

| DESARROLLO DEL MODELO DE PROGRAMACIÓN DEL PROYECTO |
|---|
| El desarrollo del proyecto se guiará mediante una planificación secuencial, utilizando un enfoque de cascada, ya que las fases del proyecto desde el diagnóstico inicial hasta la elaboración de la propuesta final siguen una lógica progresiva y dependiente. Para la planificación, seguimiento y control de las actividades se empleará Microsoft Project, herramienta que facilitará la asignación de responsabilidades, la identificación de relaciones entre tareas, el control de plazos y la visibilidad del avance del proyecto en tiempo real. |
| |
| **PERIODO DE LANZAMIENTO E ITERACIÓN** |

El proyecto no contempla un ciclo de vida adaptativo, ya que su enfoque es lineal y estructurado. A continuación, se presenta el cronograma general propuesto para su desarrollo:

- Inicio del proyecto: 2 semanas (Aprobación del acta).
- Investigación y recolección de requisitos: 4 semanas.
- Diseño conceptual de la propuesta: 11 semanas.
- Revisión y validación de la propuesta: 5 semanas.
- Entrega final: 6 semanas.

**NIVEL DE EXACTITUD**

Se adoptará un nivel de precisión del ±10%, lo cual permitirá realizar estimaciones razonables sobre la duración de las actividades, considerando posibles desviaciones menores ante eventuales retrasos.

**UNIDADES DE MEDIDA**

| *RECURSO* | *UNIDAD DE MEDIDA* |
|---|---|
| Equipo técnico | Horas de trabajo (HH). |
| Consultor en SGSI | Horas de consultoría (HH) |
| Herramientas de software | Licencias anuales |
| Actividades del proyecto | Días laborales |
| Infraestructura tecnológica | Días de uso |

**ENLACES CON LOS PROCEDIMIENTOS DE LA ORGANIZACIÓN**

Este plan de gestión del cronograma se encuentra alineado con el Plan de Gestión del Alcance, dado que las actividades programadas derivan directamente de los entregables establecidos. Asimismo, guarda relación con el Plan de Gestión de Requisitos, ya que la identificación y validación de las necesidades de los interesados impacta directamente en la definición y secuencia de las tareas del cronograma.

**MANTENIMIENTO DEL MODELO DE PROGRAMACIÓN DEL PROYECTO**

El cronograma será gestionado y actualizado semanalmente por el gerente del proyecto a través de Microsoft Project. En las reuniones de seguimiento, se revisará el progreso de las actividades y se documentarán posibles desviaciones, permitiendo realizar los ajustes necesarios en la planificación.

**UMBRALES DE CONTROL.**

Se define un umbral de control del 10% sobre las variaciones en las actividades programadas. En caso de superarse este límite, se analizará el impacto en el cronograma global y se implementarán las medidas correctivas correspondientes.

| **REGLAS PARA LA MEDICIÓN DEL DESEMPEÑO** | | |
|---|---|---|
| ***REGLAS PARA ESTABLECER EL % COMPLETADO.*** | ***TÉCNICAS PARA MEDIR EL VALOR GANADO.*** | ***MEDIDAS DE DESEMPEÑO DEL CRONOGRAMA.*** |
| Las actividades se consideran completas al 100% cuando se validan los entregables conforme a los criterios de aceptación definidos | Se utiliza la planificación basada en hitos y entregables aprobados por el equipo de proyecto y partes interesadas. | SPI (Índice de Desempeño del Cronograma). |
| Los avances parciales se registran en función del porcentaje de duración ejecutada respecto a la duración total planificada. | El Valor Ganado (EV) se calcula comparando el trabajo completado con el Valor Planeado (PV) hasta la fecha de reporte. | Variación del Cronograma (SV) para identificar adelantos o retrasos en el proyecto |
| Las actividades que dependen de terceros o proveedores externos deben incluirse con sus tiempos reales de entrega para evitar desviaciones | El análisis de tendencias se realiza semanalmente para detectar posibles riesgos de retrasos. | Reportes semanales de avance que comparan valores planificados vs reales para toma de decisiones |

| **FORMATOS DE LOS INFORMES** | |
|---|---|
| **INFORME** | **FRECUENCIA DE PRESENTACIÓN** |
| Informe de progreso semanal | Semanalmente |
| Informe de desviaciones del cronograma | Mensualmente o según sea necesario |
| Informe de riesgos | Mensualmente |
| Informe de gestión de cambios | Cada vez que se apruebe un cambio |
| Informe de recursos | Mensualmente |
| Informe final del proyecto | Al cierre del proyecto. |

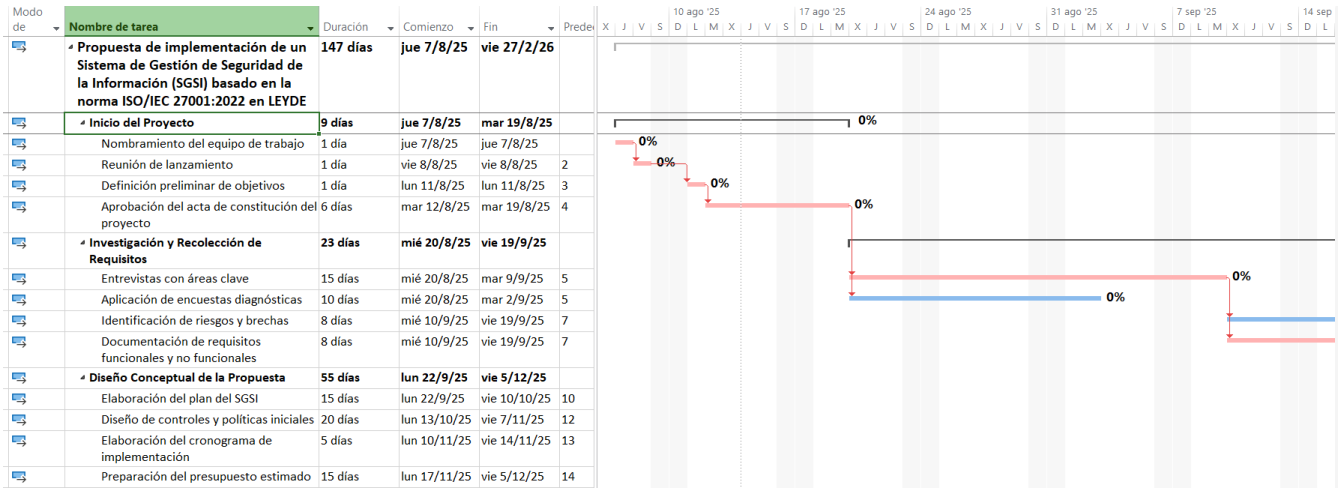
### 6.6.2 IDENTIFICACIÓN Y SECUENCIACIÓN DE ACTIVIDADES

| NOMBRE DEL PROYECTO | SIGLAS DEL PROYECTO |
|---|---|
| Propuesta de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 en LEYDE. | PISGSILEYDE |

| Paquete de Trabajo | | Actividad del Paquete de Trabajo | | Restricciones o Supuestos | Persona Responsable | Tipo de Actividad |
|---|---|---|---|---|---|---|
| **Código EDT** | **Nombre** | **Código** | **Nombre** | | | |
| 1.1 | Inicio del Proyecto | 1.1.1 | Nombramiento del equipo de trabajo | El equipo debe estar completo y alineado. | Gerente de Proyecto | Documentación |
| 1.1 | Inicio del Proyecto | 1.1.2 | Reunión de lanzamiento | Todos los participantes deben estar disponibles. | Gerente de Proyecto | Reunión |
| 1.1 | Inicio del Proyecto | 1.1.3 | Definición preliminar de objetivos | Los objetivos deben alinearse con la visión de la empresa. | Gerente de Proyecto | Planificación |
| 1.1 | Inicio del Proyecto | 1.1.4 | Aprobación del acta de constitución del proyecto | Requiere validación por parte de la alta dirección. | Dirección General | Aprobación |
| 1.2 | Investigación y Recolección de Requisitos | 1.2.1 | Entrevistas con áreas clave | Disponibilidad de los entrevistados. | Analista de Requisitos | Investigación |
| 1.2 | Investigación y Recolección de Requisitos | 1.2.2 | Aplicación de encuestas diagnósticas | Participación de los colaboradores. | Analista de Requisitos | Investigación |

| | | | | | | |
|---|---|---|---|---|---|---|
| 1.2 | Investigación y Recolección de Requisitos | 1.2.3 | Identificación de riesgos y brechas | Acceso a información histórica y procesos actuales. | Especialista en Seguridad | Análisis |
| 1.2 | Investigación y Recolección de Requisitos | 1.2.4 | Documentación de requisitos funcionales y no funcionales | Requiere validación por parte de usuarios clave. | Analista de Requisitos | Documentación |
| 1.3 | Diseño Conceptual de la Propuesta | 1.3.1 | Elaboración del plan del SGSI | Basado en los requisitos identificados y la norma ISO/IEC 27001:2022. | Consultor en SGSI | Planificación |
| 1.3 | Diseño Conceptual de la Propuesta | 1.3.2 | Diseño de controles y políticas iniciales | Deben alinearse con los objetivos de seguridad de la organización. | Consultor en SGSI | Diseño |
| 1.3 | Diseño Conceptual de la Propuesta | 1.3.3 | Elaboración del cronograma de implementación | Debe considerar recursos y tiempos realistas. | Gerente de Proyecto | Planificación |
| 1.3 | Diseño Conceptual de la Propuesta | 1.3.4 | Preparación del presupuesto estimado | Basado en costos históricos y cotizaciones actuales. | Analista Financiero | Estimación |
| 1.4 | Finalización y Entrega | 1.4.1 | Documentación formal del proyecto | Debe cumplir con los lineamientos académicos y organizacionales. | Gerente de Proyecto | Documentación |
| 1.4 | Finalización y Entrega | 1.4.2 | Entrega de entregables a la dirección | Requiere aprobación formal. | Gerente de Proyecto | Entrega |
| 1.4 | Finalización y Entrega | 1.4.3 | Reunión de cierre y lecciones aprendidas | Participación de todos los miembros clave del proyecto. | Gerente de Proyecto | Reunión |

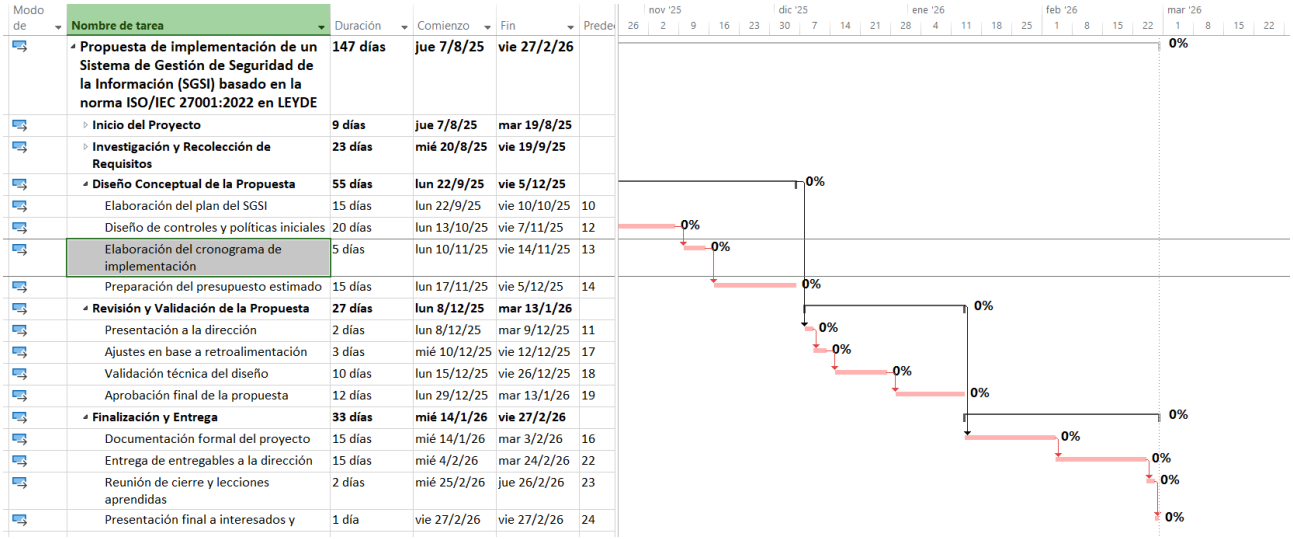
## 6.6.3 CRONOGRAMA DE IMPLEMENTACIÓN



| Modo de | Nombre de tarea | Duración | Comienzo | Fin | Prede |
|---|---|---|---|---|---|
| | **Propuesta de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 en LEYDE** | **147 días** | **jue 7/8/25** | **vie 27/2/26** | |
| | **Inicio del Proyecto** | **9 días** | **jue 7/8/25** | **mar 19/8/25** | |
| | Nombramiento del equipo de trabajo | 1 día | jue 7/8/25 | jue 7/8/25 | |
| | Reunión de lanzamiento | 1 día | vie 8/8/25 | vie 8/8/25 | 2 |
| | Definición preliminar de objetivos | 1 día | lun 11/8/25 | lun 11/8/25 | 3 |
| | Aprobación del acta de constitución del proyecto | 6 días | mar 12/8/25 | mar 19/8/25 | 4 |
| | **Investigación y Recolección de Requisitos** | **23 días** | **mié 20/8/25** | **vie 19/9/25** | |
| | Entrevistas con áreas clave | 15 días | mié 20/8/25 | mar 9/9/25 | 5 |
| | Aplicación de encuestas diagnósticas | 10 días | mié 20/8/25 | mar 2/9/25 | 5 |
| | Identificación de riesgos y brechas | 8 días | mié 10/9/25 | vie 19/9/25 | 7 |
| | Documentación de requisitos funcionales y no funcionales | 8 días | mié 10/9/25 | vie 19/9/25 | 7 |
| | **Diseño Conceptual de la Propuesta** | **55 días** | **lun 22/9/25** | **vie 5/12/25** | |
| | Elaboración del plan del SGSI | 15 días | lun 22/9/25 | vie 10/10/25 | 10 |
| | Diseño de controles y políticas iniciales | 20 días | lun 13/10/25 | vie 7/11/25 | 12 |
| | Elaboración del cronograma de implementación | 5 días | lun 10/11/25 | vie 14/11/25 | 13 |
| | Preparación del presupuesto estimado | 15 días | lun 17/11/25 | vie 5/12/25 | 14 |



**Figura 20: Cronograma de implementación del proyecto**



| Modo de | Nombre de tarea | Duración | Comienzo | Fin | Prede |
|---|---|---|---|---|---|
| | **Propuesta de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 en LEYDE** | **147 días** | **jue 7/8/25** | **vie 27/2/26** | |
| | **Inicio del Proyecto** | **9 días** | **jue 7/8/25** | **mar 19/8/25** | |
| | **Investigación y Recolección de Requisitos** | **23 días** | **mié 20/8/25** | **vie 19/9/25** | |
| | **Diseño Conceptual de la Propuesta** | **55 días** | **lun 22/9/25** | **vie 5/12/25** | |
| | Elaboración del plan del SGSI | 15 días | lun 22/9/25 | vie 10/10/25 | 10 |
| | Diseño de controles y políticas iniciales | 20 días | lun 13/10/25 | vie 7/11/25 | 12 |
| | Elaboración del cronograma de implementación | 5 días | lun 10/11/25 | vie 14/11/25 | 13 |
| | Preparación del presupuesto estimado | 15 días | lun 17/11/25 | vie 5/12/25 | 14 |
| | **Revisión y Validación de la Propuesta** | **27 días** | **lun 8/12/25** | **mar 13/1/26** | |
| | Presentación a la dirección | 2 días | lun 8/12/25 | mar 9/12/25 | 11 |
| | Ajustes en base a retroalimentación | 3 días | mié 10/12/25 | vie 12/12/25 | 17 |
| | Validación técnica del diseño | 10 días | lun 15/12/25 | vie 26/12/25 | 18 |
| | Aprobación final de la propuesta | 12 días | lun 29/12/25 | mar 13/1/26 | 19 |
| | **Finalización y Entrega** | **33 días** | **mié 14/1/26** | **vie 27/2/26** | |
| | Documentación formal del proyecto | 15 días | mié 14/1/26 | mar 3/2/26 | 16 |
| | Entrega de entregables a la dirección | 15 días | mié 4/2/26 | mar 24/2/26 | 22 |
| | Reunión de cierre y lecciones aprendidas | 2 días | mié 25/2/26 | jue 26/2/26 | 23 |
| | Presentación final a interesados y | 1 día | vie 27/2/26 | vie 27/2/26 | 24 |



**Figura 21: Cronograma de implementación del proyecto**

## 6.7 GESTIÓN DE LOS COSTOS

| CONTROL DE VERSIONES | | | | | |
|---|---|---|---|---|---|
| ***Versión*** | ***Hecha por*** | ***Revisada por*** | ***Aprobada por*** | ***Fecha*** | ***Motivo*** |
| 1.0 | Equipo proyecto Propuesta SGSI ISO 27001:2022 Leyde | | Dirección de proyecto | | Creación de documento inicial |

### 6.7.1 PLAN DE GESTIÓN DE COSTOS

### 6.7.2 ESTIMACIÓN DE COSTOS

| **NOMBRE DEL PROYECTO** | **SIGLAS DEL PROYECTO** |
|---|---|
| Propuesta de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 en LEYDE. | PISGSILEYDE |

| CLASIFICACIÓN DE RECURSOS | |
|---|---|
| TIPO DE RECURSO | UNIDADES DE MEDIDA |
| Tipo de recurso | Unidades de medida |
| Humano | Horas/hombre, por tarea o servicio contratado |
| Materiales | Licencias, herramientas digitales, manuales |
| Financieros | Estimación en Lempiras (HNL), clasificado por rubros |
| METODO DE ESTIMACIÓN | |

| TIPO DE ESTIMACIÓN | MODO DE FORMULACIÓN | NIVEL DE PRECISIÓN |
|---|---|---|
| ANALOGICA | Basada en proyectos similares de implementación de SGSI | Dos cifras significativas |
| PARAMÉTRICA | Basada en métricas como costo por hora promedio | Al entero más próximo |
| NIVELES DE EXACTITUD | | |
| TIPO DE ESTIMACIÓN | MODO DE FORMULACIÓN | NIVEL DE PRECISIÓN |
| Paramétrica | En función del costo unitario estimado | ±10% del cálculo de actividades |
| ENLACES Y PROCEDIMIENTOS | | |
| El plan de gestión de los costos estará vinculado a los procedimientos contables existentes en Leyde. Las estimaciones, registros y reportes de costos se integrarán con los sistemas administrativos internos, con el objetivo de garantizar una gestión financiera alineada a los estándares de control establecidos por la organización. | | |
| UMBRALES DE CONTROL<br>PROCESO CONTROLAR | | |
| ALCANCE:<br>PROYECTO/FASE/ENTREGABLE | VARIACIÓN PERMITIDA | ACCIÓN PARA TOMAR SI LA<br>VARIACIÓN EXCEDE LO PERMITIDO |
| Preparación del Proyecto | 10% para ajustes menores | Revisar justificación y aprobar recursos adicionales |
| Diseño Conceptual | 15% por iteraciones y validaciones necesarias | Evaluar impacto en entregables y ajustar presupuesto |
| Capacitación y Entrega | 10% en caso de ampliación de sesiones o soporte | Aprobar reprogramación de recursos |

| **REGLAS PARA LA MEDICIÓN DEL DESEMPEÑO CONTROL** | | |
|---|---|---|
| ***ALCANCE*** | ***MÉTODO DE MEDICIÓN*** | ***MODO DE MEDICIÓN*** |
| Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) completo, conforme a la norma ISO/IEC 27001:2022. | Valor ganado, medición de presupuesto con relación a lo avanzado en cronograma | Los responsables del proyecto realizarán **revisiones mensuales** durante reuniones virtuales programadas, en las cuales se actualizará el estado de los entregables y se analizará el avance financiero. |
| **SALIDAS DE CONTROL DE COSTO** | | |
| ***FORMATO DE GESTIÓN DE COSTOS*** | ***DESCRIPCIÓN: QUÉ, QUIÉN, CÓMO, CUÁNDO, DÓNDE, CON QUÉ*** | |
| Informe de Costo Estimado | El **Informe de Costo Estimado** consistirá en la consolidación inicial de los costos planificados para la implementación del Sistema de Gestión de Seguridad de la Información en Leyde. Será elaborado por el **equipo del proyecto**, utilizando una **plantilla estructurada** en Microsoft Excel que incluya rubros por fases, recursos y contingencias. Este informe se preparará **al inicio del proyecto**, y será **presentado y validado** en la primera reunión de planificación. Se almacenará en **plataformas colaborativas** como One Drive o SharePoint, y servirá como base de comparación frente a los costos reales. El documento será elaborado **con base en cotizaciones, referencias de mercado y horas estimadas de trabajo** | |
| Registro de Costos Reales | El **Registro de Costos Reales** documentará de forma sistemática los gastos ejecutados durante la implementación del SGSI. Este control será responsabilidad del **líder del proyecto**, quien realizará **registros semanales** en una hoja de cálculo digital, con respaldo en **facturas, órdenes de compra o reportes de tiempo trabajado**. La información se gestionará **en línea** y estará disponible para el equipo mediante herramientas colaborativas como Microsoft Excel. Este registro será fundamental para identificar desviaciones frente al presupuesto estimado, facilitando decisiones correctivas en reuniones mensuales de control. | |
| **DETALLES ADICIONALES DE LA GESTIÓN DE COSTOS** | | |
| **SELECCIÓN DE FINANCIAMIENTO** | | |
| El financiamiento del proyecto será cubierto de manera integral con el presupuesto interno aprobado por la empresa Leyde, sin requerir apoyo de fuentes externas ni financiamiento adicional. | | |
| **FLUCTUACIONES EN LOS TIPOS DE CAMBIO** | | |
| El proyecto no contempla costos en moneda extranjera, por lo que no se consideran riesgos asociados a fluctuaciones cambiarias. | | |

| REGISTRO DE LOS COSTOS |
| --- |
| Todos los costos serán registrados de forma semanal por el líder del proyecto, utilizando un formato estándar previamente definido, el cual se integrará con el sistema contable interno de Leyde para asegurar un control financiero adecuado y alineado a los procesos institucionales. |

### 6.7.3 PRESUPUESTO

| NOMBRE DEL PROYECTO | SIGLAS DEL PROYECTO |
| --- | --- |
| Propuesta de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 en LEYDE. | PISGSILEYDE |

| ESTIMACIÓN DE COSTOS | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Entregable** | **Actividad** | **Tipo de Recurso** | **Nombre del Recurso** | **Unidades** | **Cantidad** | **Costo Unitario (HNL)** | **Costo Total (HNL)** |
| Inicio del Proyecto | Reunión de lanzamiento | Humano | Coordinador de Proyecto | Hora/Hombre | 5 | L - | L - |
| Investigación y Recolección | Entrevistas a áreas clave | Humano | Analista de Seguridad | Hora/Hombre | 10 | L - | L - |
| Diagnóstico Inicial | Gap Analysis vs ISO 27001 | Humano | Consultor ISO | Hora/Hombre | 40 | L 1,700.00 | L 68,000.00 |
| Diseño Conceptual | Apoyo en diseño del SGSI | Humano | Consultor ISO | Hora/Hombre | 80 | L 550 | L 44,000.00 |
| Validación de Propuesta | Revisión con stakeholders | Humano | Jefe de TI | Hora/Hombre | 6 | L - | L - |
| Finalización y Entrega | Presentación y entrega informe | Humano | Documentador Técnico | Hora/Hombre | 4 | L - | L - |
| Soporte Técnico y Control | Configuración de herramienta | Máquina / No consumible | Licencia de Software SIEM (IBM QRadar) | Licencia | 1 | L 157,290.00 | L 157,290.00 |
| Protección de Información | Cifrado de disco duro | Máquina / No consumible | Software de Cifrado BitLocker | Licencia | 10 | L - | L - |
| Capacitación | Formación en ISO 27001 para el personal | Humano | Consultor ISO | Sesión | 2 | L 11,000.00 | L 22,000.00 |
| Registro y Monitoreo | Registro centralizado de logs | Máquina / No consumible | Servidor virtual en la nube | Mes | 3 | L 3,500.00 | L 10,500.00 |
| Protección de Endpoints y Redes | Licencia Sophos Endpoint Protection | Máquina / No consumible | Sophos Endpoint Protection | Licencia | 10 | L 686.00 | L 6,860.00 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Auditoría y Evaluación | Licencia GRC Tool (RSA Archer / ServiceNow) | Máquina / No consumible | Licencia GRC Tool | Licencia | 1 | L 65,000.00 | L 65,000.00 |
| Auditoría de Vulnerabilidades | Escáner Nessus / OpenVAS | Máquina / No consumible | Licencia Nessus | Licencia | 1 | L 68,355.00 | L 68,355.00 |

| DETALLES ADICIONALES DE ESTIMACIÓN DE COSTOS |
|---|
| Los costos de implementación de herramientas pueden variar según licencias acordadas entre el proveedor y la empresa Leyde. |

| REFERENCIAS DE COSTOS | |
|---|---|
| Licencia de Software SIEM (IBM QRadar) | https://www.midlandinfosys.com/ibm-qradar-pricing |
| Sophos Endpoint Protection | https://underdefense.com/blog/sophos-pricing-intercept-x-endpoint-protection-cost |
| Licencia GRC Tool (RSA Archer / ServiceNow) | https://www.scrut.io/post/zengrc-vs-rsa-archer-vs-scrut |
| Escáner Nessus / OpenVAS | https://www.trustradius.com/products/tenable-nessus/pricing |

| BENEFICIOS ESPERADOS ROI | |
|---|---|
| Herramienta / Recurso | Costo Total (HNL) |
| IBM QRadar (SIEM) | L 157,290.00 |
| BitLocker (Cifrado de discos) | L - |
| Servidor Virtual (3 meses) | L 10,500.00 |
| Sophos Endpoint Protection (10 usuarios) | L 6,860.00 |
| Nessus (Escáner de vulnerabilidades) | L 68,355.00 |
| RSA Archer (estimación conservadora) | L 300,000.00 |
| Consultor ISO 2001 | L 134,000.00 |
| Total inversión aproximada: | L 677,005.00 |
| Beneficio estimado | Monto estimado (HNL / Año) |
| Reducción de incidentes de seguridad (menos paros operativos) | L 180,000.00 |
| Ahorro en sanciones o multas regulatorias | L 100,000.00 |
| Mayor productividad por monitoreo automatizado | L 60,000.00 |
| Reducción de gastos por ataques a endpoints (virus/malware) | L 40,000.00 |
| Optimización de gestión de riesgos con GRC | L 50,000.00 |
| Total ahorro/beneficio anual estimado | 430,000 HNL / año |
| Año | Recuperación acumulada (HNL) |

| | | |
|---|---|---|
| 1 | L | 43,0000 |
| 2 | L | 86,0000 |
| 3 | L | 1,290,000 |

| DETALLES ADICIONALES DE BENEFICIOS ESPERADOS |
|---|
| Debido a que los costos de pueden variar según lo acordado con proveedor, los beneficios tendrán alteración con relación al mismo.<br><br>Los beneficios podrían variar según escenarios que se encuentren durante la ejecución del SGSI lo cual alteraría también el ROI. |

## 6.8 GESTIÓN DE LOS RECURSOS

| NOMBRE DEL PROYECTO | SIGLAS DEL PROYECTO |
|---|---|
| Propuesta de implementación de un sistema de gestión de seguridad de la información (SGSI) basado en ISO/IEC 27001:2022 en Leyde. | Propuesta SGSI ISO 27001:2022 Leyde |

| IDENTIFICACIÓN DE LOS RECURSOS | |
|---|---|
| Equipo técnico | |
| Rol / Recurso | Función Principal |
| Coordinador del proyecto SGSI | Planificación, control de cronograma y comunicación con partes interesadas |
| Consultor ISO 27001 | Experto en la norma, diseña e implementa los controles requeridos |
| Analista de Seguridad Informática | Realiza análisis de riesgos, auditorías, y define políticas de seguridad |
| Administrador de sistemas | Apoya en implementación técnica de herramientas de seguridad |
| Auditor interno | Evalúa el cumplimiento de los controles antes de la auditoría externa |
| Soporte TI | Apoya con infraestructura, red, servidores, respaldos y mantenimiento |
| Documentador Técnico | Elabora políticas, manuales y documentación obligatoria del SGSI |
| Legal / Compliance Officer | Verifica cumplimiento con leyes, contratos y normativas de protección de datos |

| Herramientas Digitales | |
|---|---|
| Herramienta | Función / Justificación |
| SIEM (QRadar, Splunk, OSSIM) | Monitoreo de seguridad, correlación de eventos, detección de amenazas |
| Cifrado (BitLocker, VeraCrypt) | Protección de información en equipos y discos |
| Escáner de vulnerabilidades (Nessus, OpenVAS) | Identifica puntos débiles en la infraestructura |
| GRC Tool (RSA Archer, ServiceNow GRC) | Gestión de riesgos, auditorías y cumplimiento |
| Antivirus / EDR (Sophos, CrowdStrike) | Protección de endpoints, detección y respuesta ante incidentes |
| Herramientas de backup | Aseguran recuperación de información crítica |
| Power BI / Tableau / Grafana | Visualización de métricas, KPIs y eficacia del SGSI |
| Repositorio documental (SharePoint, Google Drive, Confluence) | Gestión de políticas, actas, reportes y evidencia |
| Firewall / Control de red | Supervisión de tráfico y prevención de accesos no autorizados |
| Herramientas de autenticación | Control de accesos (ej. MFA, Active Directory, LDAP) |

### 6.8.1 PLAN DE GESTIÓN DE LOS RECURSOS

| IDENTIFICACIÓN DE LOS RECURSOS | |
|---|---|
| Equipo técnico | |
| Rol / Recurso | Función Principal |
| Coordinador del proyecto SGSI | Planificación, control de cronograma y comunicación con partes interesadas |
| Consultor ISO 27001 | Experto en la norma, diseña e implementa los controles requeridos |
| Analista de Seguridad Informática | Realiza análisis de riesgos, auditorías, y define políticas de seguridad |
| Administrador de sistemas | Apoya en implementación técnica de herramientas de seguridad |
| Auditor interno | Evalúa el cumplimiento de los controles antes de la auditoría externa |
| Soporte TI | Apoya con infraestructura, red, servidores, respaldos y mantenimiento |
| Documentador Técnico | Elabora políticas, manuales y documentación obligatoria del SGSI |
| Legal / Compliance Officer | Verifica cumplimiento con leyes, contratos y normativas de protección de datos |

| Herramientas Digitales | |
|---|---|
| Herramienta | Función / Justificación |
| SIEM (QRadar, Splunk, OSSIM) | Monitoreo de seguridad, correlación de eventos, detección de amenazas |
| Cifrado (BitLocker, VeraCrypt) | Protección de información en equipos y discos |
| Escáner de vulnerabilidades (Nessus, OpenVAS) | Identifica puntos débiles en la infraestructura |
| GRC Tool (RSA Archer, ServiceNow GRC) | Gestión de riesgos, auditorías y cumplimiento |
| Antivirus / EDR (Sophos, CrowdStrike) | Protección de endpoints, detección y respuesta ante incidentes |
| Herramientas de backup | Aseguran recuperación de información crítica |
| Power BI / Tableau / Grafana | Visualización de métricas, KPIs y eficacia del SGSI |
| Repositorio documental (SharePoint, Google Drive, Confluence) | Gestión de políticas, actas, reportes y evidencia |
| Firewall / Control de red | Supervisión de tráfico y prevención de accesos no autorizados |
| Herramientas de autenticación | Control de accesos (ej. MFA, Active Directory, LDAP) |

### 6.8.2 ESTIMACIÓN DE LOS RECURSOS

| Categoría | Recurso / Herramienta | Unidad | Cantidad Estimada |
|---|---|---|---|
| Equipo Técnico | Coordinador del proyecto | Persona | 1 |
| | Consultor ISO 27001 | Persona | 1 |
| | Analista de Seguridad | Persona | 1 |
| | Auditor interno | Persona | 1 (parcial) |
| | Documentador Técnico | Persona | 1 (parcial) |
| | | | |
| Herramientas Digitales | SIEM (IBM QRadar / OSSIM) | Licencia | 1 |
| | Cifrado de discos (BitLocker) | Licencia | 10 |
| | Antivirus / EDR (Sophos) | Licencia | 10 |
| | Escáner de vulnerabilidades (Nessus) | Licencia | 1 |
| | Plataforma GRC (RSA Archer / alternativa) | Licencia | 1 |
| Reuniones Virtuales | Plataforma de videollamadas (Zoom / Teams) | Cuenta | 1 (equipo) |
| | Actas y documentación digital | Carpeta/Gestor | 1 compartido |

### 6.8.3 ADQUISICIÓN DE RECURSOS

Este proceso tiene como objetivo documentar y facilitar el control de los recursos que serán requeridos a lo largo de la implementación del SGSI, organizados por tipo, responsables de adquisición, proveedores potenciales, costos estimados y estado actual del proceso de obtención.

| Recurso / Herramienta | Tipo de Recurso | Justificación / Uso | Unidad | Cantidad | Costo Unitario (HNL) | Costo Total (HNL) | Responsable | Estado | Fuente / Proveedor | Observaciones |
|---|---|---|---|---|---|---|---|---|---|---|
| IBM QRadar | Herramienta Digital | SIEM para monitoreo de seguridad | Licencia | 1 | 157,290 | 157,290 | Jefe de TI | Pendiente | IBM / Partner local | Requiere cotización oficial |
| BitLocker | Herramienta Digital | Cifrado de discos | Licencia | 10 | 0 | 0 | Soporte TI | Pendiente | Microsoft | Incluido en Win Pro |
| Sophos Endpoint | Herramienta Digital | Protección de endpoints | Licencia | 10 | 686 | 6,860 | Seguridad Informática | Pendiente | Sophos / Reseller | Se debe pedir demo |
| Consultor ISO 27001 | Recurso Humano | Diseño del SGSI | Hora | 15 | 1,000 | 15,000 | Coordinador SGSI | Pendiente | Contrato externo | |
| Plataforma de Reuniones (Teams) | Herramienta de Comunicación | Gestión remota del proyecto | Licencia | 1 | 2,000 | 2,000 | Coordinador SGSI | Pendiente | Microsoft | Plan incluido en Office365 |

## 6.9 GESTIÓN DE LOS RIESGOS

La gestión de riesgos durante la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001:2022 es crucial para anticipar y mitigar posibles obstáculos que puedan afectar el éxito del proyecto. Identificar y evaluar los riesgos asociados permite tomar decisiones oportunas, asignar recursos adecuados y asegurar que las actividades se desarrollen dentro de los plazos y costos establecidos. Este enfoque proactivo contribuye a garantizar la correcta adopción del SGSI en Leyde, minimizando impactos negativos y fortaleciendo la capacidad de la organización para proteger su información de manera eficiente.

| Nombre | Frecuencia inherente | Impacto inherente | Frecuencia residual | Impacto residual | Riesgo inherente | Riesgo residual | Plan de acción | Responsable |
|---|---|---|---|---|---|---|---|---|
| Fallas en la recuperación ante incidentes y desastres | Improbable | Catastrófico | Improbable | Catastrófico | Alto | Medio | Desarrollar un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP), realizar pruebas semestrales de recuperación simulada y capacitar al personal clave en respuesta ante incidentes. | Coordinador de TI |
| Insuficiente monitoreo y medición del desempeño del SGSI | Posible | Moderado | Posible | Moderado | Medio | Bajo | Establecer KPIs e indicadores de cumplimiento para controles y procesos, implementar herramientas como dashboards en Power BI y realizar revisiones mensuales de resultados con el equipo de SGSI. | Coordinador SGSI |
| Incapacidad para mantener la mejora continua del SGSI | Posible | Moderado | Posible | Moderado | Medio | Bajo | Aplicar el ciclo PDCA de forma trimestral con seguimiento de acciones correctivas, | Calidad |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | implementar un sistema de gestión de hallazgos y oportunidades de mejora, y asignar un responsable del seguimiento de mejoras. | |
| Deficiencias en la gestión de cambios | Probable | Moderado | Probable | Moderado | Alto | Medio | Diseñar un procedimiento formal de gestión de cambios, crear un comité de evaluación de cambios y establecer una matriz de impacto de cambios. | Encargado de Gestión de Cambios. |
| Falta de integración del SGSI con otros sistemas de gestión | Posible | Menor | Posible | Menor | Bajo | Bajo | Realizar un mapeo de procesos comunes entre SGSI y otros sistemas, establecer controles y registros compartidos donde sea posible e incorporar el SGSI en las reuniones de revisión de otros sistemas de gestión. | Coordinador de Sistemas de Gestión |
| Deficiencias en la planificación y ejecución de auditorías internas | Posible | Moderado | Posible | Moderado | Medio | Medio | Crear un calendario anual de auditorías internas, formar auditores internos certificados y diseñar listas de verificación alineadas a ISO/IEC 27001. | Calidad |
| Resistencia al cambio por parte del personal | Probable | Moderado | Probable | Moderado | Alto | Medio | Realizar sesiones informativas sobre beneficios del SGSI, incluir al personal en la definición de políticas y procedimientos, y establecer un canal de comunicación y sugerencias. | Recursos Humanos |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Insuficiente presupuesto y recursos para el SGSI | Probable | Mayor | Probable | Mayor | Alto | Medio | Preparar un caso de negocio basado en riesgos y beneficios, presentar el plan de adquisición de recursos con ROI esperado e identificar fuentes de financiamiento alternativas si es necesario | Finansas |
| Deficiente gestión de proveedores y terceras partes | Ocasional | Moderado | Ocasional | Moderado | Medio | Bajo | Crear un procedimiento de evaluación de proveedores, establecer contratos con cláusulas de seguridad de la información y aplicar auditorías o revisiones a terceros críticos. | Seguridad de la Información |
| Incumplimiento de requisitos legales y normativos | Posible | Catastrófico | Posible | Catastrófico | Alto | Medio | Contratar asesores legales para revisar el marco regulatorio aplicable, implementar un registro de cumplimiento legal actualizado y diseñar controles que aseguren trazabilidad ante auditorías. | Oficial de Cumplimiento |
| Deficiencias en el diseño e implementación de controles de seguridad | Probable | Mayor | Probable | Mayor | Alto | Medio | Utilizar el Anexo A de ISO/IEC 27001 como referencia base, validar los controles mediante evaluaciones técnicas (vulnerabilidad, pruebas) y establecer una matriz de controles aplicables con responsables asignados. | Analista de Seguridad de la Información |
| Falta de concienciación y capacitación del personal | Frecuente | Moderado | Frecuente | Moderado | Alto | Medio | Diseñar un programa de capacitación anual obligatorio, implementar cursos en línea y talleres | Recursos Humanos / SGSI. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | presenciales y evaluar el nivel de conocimiento mediante quizzes o simulacros. | |
| Insuficiente análisis de riesgos de seguridad de la información | Posible | Mayor | Posible | Mayor | Medio | Bajo | Aplicar metodologías cualitativas o mixtas como ISO 31000, OCTAVE o Pirani, revisar el análisis de forma semestral o cuando haya cambios importantes y documentar claramente riesgos, impactos, controles y responsables. | Analista de Riesgos |
| Inadecuada clasificación y gestión de activos | Ocasional | Moderado | Ocasional | Moderado | Medio | Bajo | Identificar activos mediante entrevistas y revisión documental, asignar propietarios de activos y establecer niveles de clasificación, y crear una base de datos centralizada de activos con control de acceso. | Seguridad de la Información |
| Falta de compromiso de la alta dirección | Probable | Mayor | Probable | Mayor | Alto | Medio | Realizar sesiones de sensibilización enfocadas en el impacto estratégico del SGSI, presentar casos de estudio o experiencias de otras empresas e incluir al menos un directivo en el Comité de Seguridad de la Información. | Coordinador del SGSI y Alta Dirección. |

En la siguiente imagen se puede ver el mapa de calor relacionado a la gestión de riesgo de la implementación del proyecto.

Los números en los recuadros, son indicativos de la cantidad de riesgos por tipo, por ejemplo: Frecuenta/Moderado, existe solo 1 riesgo el cual es *Falta de concienciación y capacitación del personal*.

## 6.10 PLAN DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN USANDO LA METODOLOGÍA CICLO PDCA (PLAN-DO-CHECK-ACT)

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en LEYDE representa un reto importante tanto a nivel técnico como organizacional. Este tipo de iniciativa requiere una planificación cuidadosa, una ejecución ordenada y un compromiso institucional que garantice su sostenibilidad en el tiempo. Para abordar este proceso de manera estructurada, se ha optado por aplicar el ciclo PDCA (Planificar, Hacer, Verificar, Actuar), una metodología ampliamente utilizada en sistemas de gestión que permite avanzar de forma progresiva y controlada hacia la mejora continua.

El enfoque PDCA facilita la organización del proyecto en cuatro etapas fundamentales, cada una con objetivos y actividades específicas que se retroalimentan entre sí. En el caso de LEYDE, esta metodología permite establecer una base sólida para el diseño e implementación de un SGSI alineado con los requisitos de la norma ISO/IEC 27001:2022, asegurando que cada fase contribuya al fortalecimiento de la seguridad de la información y al cumplimiento de los objetivos estratégicos de la empresa.

### 6.10.1 FASE PLAN

**Objetivo**: Establecer el contexto, los requisitos y la planificación estratégica para la implementación del SGSI en LEYDE.

**Tareas**:

- Realizar diagnóstico de la situación actual de seguridad de la información.
- Identificar brechas respecto a la norma ISO/IEC 27001:2022.
- Definir el alcance del SGSI y los objetivos de seguridad.
- Elaborar la política de seguridad de la información.
- Planificar los recursos, cronograma y presupuesto del proyecto.

**Entregables:**

- Informe de diagnóstico.

- Análisis de brechas.

- Documento de alcance y objetivos del SGSI.

- Política de seguridad de la información.

- Plan de proyecto (cronograma, recursos, presupuesto).

### 6.10.2 FASE DO

**Objetivo**: Ejecutar las acciones planificadas para implementar los controles y procedimientos del SGSI.

**Tareas:**

- Implementar controles de seguridad definidos en el plan.

- Capacitar al personal en políticas y procedimientos del SGSI.

- Establecer mecanismos de comunicación y gestión documental.

- Operar el SGSI conforme a lo planificado.

**Entregables:**

- Registros de implementación de controles.

- Reportes de capacitación y asistencia.

- Manuales y procedimientos operativos.

- Evidencias de operación del SGSI.

### 6.10.3 FASE CHECK

**Objetivo**: Verificar el desempeño del SGSI y evaluar su conformidad con los requisitos establecidos.

**Tareas:**

- Realizar auditorías internas del SGSI.

- Evaluar el cumplimiento de los controles implementados.

- Analizar los resultados de auditoría y desempeño.

- Identificar no conformidades y oportunidades de mejora.

**Entregables:**

- Informes de auditoría interna.

- Reportes de evaluación de desempeño.

- Registro de no conformidades.

- Planes de acción correctiva.

### 6.10.4 FASE ACT

**Objetivo**: Tomar acciones para mejorar continuamente el SGSI con base en los resultados de la fase de verificación.

**Tareas:**

- Revisar la eficacia de las acciones correctivas.

- Actualizar políticas, procedimientos y controles según resultados.

- Promover la mejora continua del SGSI.

- Comunicar los cambios a las partes interesadas.

**Entregables:**

- Informe de revisión de acciones correctivas.

- Documentación actualizada del SGSI.

- Plan de mejora continua.

- Comunicaciones internas de actualización.

## 6.11 MAPEO ENTRE ISO 27001 | PMBOK | OCTAVE

Este mapeo busca alinear los enfoques de **ISO/IEC 27001:2022**, **PMBOK 6ª edición** y la **metodología OCTAVE** para integrar la gestión de la seguridad de la información con buenas prácticas de gestión de proyectos y análisis de riesgos. Así, se facilita una implementación más estructurada y estratégica del SGSI.

| Área/Proceso | ISO/IEC 27001:2022 | PMBOK | OCTAVE |
|---|---|---|---|
| Contexto y alcance del SGSI | Cláusula 4: Contexto de la organización | Iniciación: análisis de stakeholders, alcance del proyecto | Fase 1: identificación de activos y áreas críticas |
| Liderazgo y gobernanza | Cláusula 5: Liderazgo y compromiso | Gestión de stakeholders y comunicaciones | Roles del equipo evaluador y propietarios de activos |
| Evaluación de riesgos | Cláusula 6.1.2 (Evaluación) y 6.1.3 (Tratamiento) | Gestión de riesgos: planificación, análisis y respuesta | Fase 2: evaluación de amenazas, impacto y priorización |
| Planificación de objetivos de seguridad | Cláusula 6.2: Objetivos y planificación operativa | Planificación del proyecto: definición de entregables y cronogramas | Diseño del plan de acción según riesgos priorizados |
| Implementación de controles | Sección A (Anexo A): selección de controles | Ejecución del proyecto: despliegue de entregables | Fase 3: implementación de mitigaciones y controles |
| Monitoreo y seguimiento | Cláusula 9.1: Monitoreo, medición, análisis | Monitoreo y control: seguimiento de indicadores | Revisión continua de efectividad, Maßnahmen adjustments |
| Auditorías internas y revisión directiva | Cláusulas 9.2 y 9.3 | Informes de desempeño, transferencia a la alta dirección | Revisión de resultados e implicaciones para mitigaciones |
| Mejora continua (PDCA) | Cláusula 10.1: Mejora continua | Control integrador: actualizaciones del plan | Retroalimentación para actualizaciones del SGSI |
| Gestión de incidentes | A.5.24: Gestión de incidentes | Aspecto específico dentro de vigilancia y riesgos | Detección y documentación de incidentes según activos críticos |

# BIBLIOGRAFÍA


Aguilar Antonio, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciber amenazas a la seguridad nacional y política exterior. *Estudios internacionales (Santiago)*, *53*(198), 169-197. https://doi.org/10.5354/0719-3769.2021.57067

*Amenazas a la Seguridad de la Información | Departamento de Seguridad Informática*. (2024). https://www.seguridadinformatica.unlu.edu.ar/?q=node/12

Antequera, C. (2023, junio 19). Protección de datos en los países de Latinoamérica. *ClarkeModet*. https://www.clarkemodet.com/articulos/proteccion-de-datos-en-los-paises-de-latinoamerica/

Ardanza, A. (2022, enero 10). Ciclo PDCA de gestión de la ISO 27001. *GlobalSuite Solutions*. https://www.globalsuitesolutions.com/es/ciclo-pdca-iso-27001/

Arias Odón, F. (2023). Investigación documental, investigación bibliométrica y revisiones sistemáticas. *REDHECS: Revista electrónica de Humanidades, Educación y Comunicación Social*, *31*(22), 9-28.

Ayerdi, A. (2024). *¿Qué es la Gestión Documental?* https://start.docuware.com/es/blog/que-es-la-gestion-documental

Barrera, J. (2024). *Operación de Claro en Centroamérica fue afectada por un caso de ransomware*. www.revistaeyn.com. https://www.revistaeyn.com/empresasymanagement/operacion-de-claro-en-centroamerica-fue-afectada-por-un-caso-de-ransomware-AB17340257

BSI. (2011). *Casos de éxito de Gestión de ISO/IEC 27001*. https://www.bsigroup.com/es-

CL/seguridad-de-la-informacion-isoiec-27001-/casos-de-exito-de-gestion-de-isoiec-27001/

Cano, J. (2021). *2021 Volume 3 Organizational Culture for Information Security*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/organizational-culture-for-information-security

Centeno, C. M. R. (2018). La brecha existente en la ciberseguridad en Honduras. *Innovare: Revista de ciencia y tecnología*, *6*(2), 58-73. https://doi.org/10.5377/innovare.v6i2.5571

Certification, G., & Webmaster, A. (2021, marzo 16). Gestión de riesgos de Seguridad de la Información. *Global Standards*. https://www.globalstd.com/blog/blog-analisis-riesgos-seguridad-informacion/

*Constitución de la República de Honduras*. (2021). https://www.tsc.gob.hn/biblioteca/index.php/leyes/177-constitucion-de-la-republica-de-honduras

*Convention on Cybercrime—Cybercrime—Www.coe.int*. (2001). Cybercrime. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Coyne, I. T. (1997). Sampling in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries? *Journal of Advanced Nursing*, *26*(3), 623-630. https://doi.org/10.1046/j.1365-2648.1997.t01-25-00999.x

Cruz, H. de la. (2021, septiembre 9). Metodología OCTAVE para el análisis de riesgos en SGSI. *PMG SSI - ISO 27001*. https://www.pmg-ssi.com/2021/09/metodologia-octave-para-el-analisis-de-riesgos-en-sgsi/

Daniels, K. (2023). *Vulnerabilidad en Ciberseguridad: Tipos y Medidas de Protección*. https://widefense.com/blog/vulnerabilidad-ciberseguridad

DataGuard. (2023). *ISO 27001 requirement 7.1: Identify and allocate resources for ISMS*. https://www.dataguard.com/knowledge/iso-27001/clause-7-1-resources-for-isms/

Díaz-Bravo, L., Torruco-García, U., Martínez-Hernández, M., & Varela-Ruiz, M. (2013). La entrevista, recurso flexible y dinámico. *Investigación en educación médica*, *2*(7), 162-167.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *4*(2), Article 2. https://doi.org/10.4236/jis.2013.42011

Dulzaides Iglesias, M. E., & Molina Gómez, A. M. (2004). Análisis documental y de información: Dos componentes de un mismo proceso. *ACIMED*, *12*(2), 1-1.

El Periódico de la Energía. (2023, abril 14). *Un grupo prorruso bloquea durante horas la web de la eléctrica canadiense Hydro-Québec*. El Periódico de la Energía. https://elperiodicodelaenergia.com/grupo-prorruso-bloquea-durante-horas-web-electrica-canadiense-hydro-quebec/

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), Article 1. https://doi.org/10.11648/j.ajtas.20160501.11

Europea. (2025). *Protección de Datos conforme al reglamento RGPD*. Your Europe. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

Fernández, A. E. P., Santamaría, L. I. S., & Chacón, J. H. G. (2021). *Aplicar la Metodología OCTAVE de Identificación de Amenazas y Vulnerabilidades en una Entidad Bancaria*.

García Romero, C. (2020). *Diseño e Implementación de un Analizador de Vulnerabilidades*. http://rua.ua.es/dspace/handle/10045/107803

*General Data Protection Regulation (GDPR) – Legal Text*. (2018). General Data Protection Regulation (GDPR). https://gdpr-info.eu/

GlobalSuite. (2021, septiembre 3). Estándares y normas ISO para mejorar la ciberseguridad. *GlobalSuite Solutions*. https://www.globalsuitesolutions.com/es/normas-iso-para-mejorar-la-ciberseguridad/

González, G. (2020, mayo 11). *Fuentes primarias: Características y ejemplos*. Lifeder. https://www.lifeder.com/fuentes-primarias/

González, H. (2016, agosto 25). GAP ANALISIS PARA IMPLEMENTACIÓN DE ISO 9001:2015. *Calidad & Gestion - Consultoría para Empresas*. https://calidadgestion.wordpress.com/2016/08/25/gap-analisis-para-implementacion-de-iso-90012015/

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación*. McGraw Hill España. https://dialnet.unirioja.es/servlet/libro?codigo=775008

IBM. (2024a). *Cost of a data breach 2024 | IBM*. https://www.ibm.com/reports/data-breach

IBM. (2024b). *What is ISO/IEC 27001? | IBM*. https://www.ibm.com/cloud/compliance/iso-27001

IBM. (2024c, junio 10). *Tipos de ciberamenazas | IBM*. https://www.ibm.com/mx-es/think/topics/cyberthreats-types

INCIBE. (2022). *Desarrollar cultura en seguridad | Empresas | INCIBE*. https://www.incibe.es/empresas/que-te-interesa/desarrollar-cultura-en-seguridad

INCL. (2024). *Informe Final sobre Derechos Digitales en Centroamérica: Enfoque en Honduras, Guatemala, El Salvador y Nicaragua* (p. 21). https://www.icnl.org/wp-

content/uploads/Informe-Final-sobre-Derechos-Digitales-en-Honduras-Guatemala-El-Salvador-y-Nicaragua.pdf

ISACA. (2024). *State of Cybersecurity 2024*. ISACA. https://www.isaca.org/resources/reports/state-of-cybersecurity-2024

ISC2. (2024). *2024 ISC2 Cybersecurity Workforce Study*. https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

*ISO - Organización Internacional de Normalización*. (2025, enero 31). ISO. https://www.iso.org/es/home

*ISO/IEC 27001:2013*. (2013). ISO. https://www.iso.org/contents/data/standard/05/45/54534.html

*ISO/IEC 27001:2022*. (2022a). ISO. https://www.iso.org/es/norma/27001

*ISO/IEC 27001:2022*. (2022b). ISO. https://www.iso.org/es/norma/27001

Kaspersky Lab. (2016, diciembre 23). *Falta de talento en seguridad: Una amenaza inesperada para la ciberseguridad corporativa*. https://latam.kaspersky.com/blog/security_risks_report_lack_of_security_talent/8731/

La Prensa. (2023). *Diseñan ley para proteger datos ante ciberdelincuentes*. www.laprensa.hn. https://www.laprensa.hn/honduras/disenan-ley-proteger-datos-ante-ciberdelincuentes-honduras-AA13131010

*Ley sobre Comercio Electrónico*. (2014). https://www.tsc.gob.hn/biblioteca/index.php/leyes/613-ley-sobre-comercio-electronico

López, T. (2023, enero 20). *SGSI: Qué es y Cómo Implementarlo*. https://innevo.com/blog/que-es-sgsi

Manage Engine. (2024). *Infografía: Evolución de la Ciberseguridad | Historia de la Ciberseguridad—ManageEngine Log360*. https://www.manageengine.com/latam/log-

management/infografia-evolucion-ciberseguridad.html

Martins, J. (2024). *Ciclo PDCA: Qué es y cómo aplicarlo paso a paso [2024] • Asana*. Asana. https://asana.com/es/resources/pdca-cycle

Melo, S. (2021, septiembre 30). Qué es y para qué sirve una lista de verificación. *DataScope*. https://datascope.io/es/blog/que-es-y-para-que-sirve-una-lista-de-verificacion/

*NCSI :: Compare*. (s. f.). Recuperado 23 de febrero de 2025, de https://ncsi.ega.ee/compare/

*NCSI :: Ranking*. (2023). https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1

Nelson. (2024, junio 11). *Metodologías ágiles: Qué son y cuáles son las más utilizadas*. ADEN International Business School. https://www.aden.org/business-magazine/metodologias-agiles/

Peralta Abarca, J. del C., Martínez Bahena, B., & Enríquez Urbano, J. (2020). Industria 4.0. *Inventio*, *16*(39), Article 39. https://doi.org/10.30973/inventio/2020.16.39/4

Perez, P. (2024, enero 18). Pilares de la Seguridad de la Información. Qué son y cómo cumplir con ellos. *PMG SSI - ISO 27001*. https://www.pmg-ssi.com/2024/01/pilares-de-la-seguridad-de-la-informacion-que-son-y-como-cumplir-con-ellos/

*¿Qué es Access Control? | Seguridad de Microsoft*. (2024). https://www.microsoft.com/es-es/security/business/security-101/what-is-access-control

Revista EyN. (2024). *Mercado de ciberseguridad en Centroamérica suma US$130,5 millones en inversiones en 2024*. www.revistaeyn.com. https://www.revistaeyn.com/tecnologia-cultura-digital/mercado-de-ciberseguridad-en-centroamerica-suma-us-1305-millones-en-inversiones-en-2024-OL20096585

Rodríguez, I. (2023). *Los procedimientos de control en auditoría*. https://www.auditool.org/blog/auditoria-externa/los-procedimientos-de-control-en-

auditoria

SYDLE. (2023). *Ciclo PDCA: ¿cuáles son los pasos y cómo funciona? Conoce algunos ejemplos*. Blog SYDLE. https://www.sydle.com/es/blog/ciclo-pdca-61ba2a15876cf6271d556be9

Toro, R. (2015, marzo 30). ISO 27001: Los activos de información. *PMG SSI - ISO 27001*. https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/

Varea, R. (2025, marzo 28). *Una eficaz herramienta contra los ciberataques que acechan a las*

Verizon. (2024). *2024 Data Breach Investigations Report*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Zambrano, A., & Hernández, L. (2020). *CENTROAMÉRICA CIBERSEGURA*. https://www.ipandetec.org/wp-content/uploads/2023/06/Centroamerica-Cibersegura.pdf

Zambrano, H. M. R. (2023). *(PDF) Seguridad de la información y ciberseguridad: Su importancia para los Estados, empresas y las personas, una revisión sistemática*. ResearchGate. https://www.researchgate.net/publication/376045322_Seguridad_de_la_informacion_y_ciberseguridad_su_importancia_para_los_Estados_empresas_y_las_personas_una_revision_sistematica

Zapata, D. (2024). *Instituciones del Estado, las más vulnerables a los ciberataques*. www.elheraldo.hn. https://www.elheraldo.hn/honduras/instituciones-estado-vulnerables-ciberataques-honduras-HL20818492

# ANEXOS

## ANEXO 1: MATRIZ DE ANÁLISIS DOCUMENTAL

**MAESTRÍA EN GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN**
**PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LEYDE BASADO EN ISO/IEC 27001:2022**

**Instrucciones:**

1. Identificar y recopilar documentos relevantes relacionados con la norma ISO/IEC 27001:2022, políticas internas, informes de auditoría, estudios académicos y publicaciones de consultoría en seguridad.
2. Completar cada campo de la siguiente matriz con la información extraída de cada documento.
3. Revisar y actualizar la matriz de forma periódica durante la fase de recolección documental.

| Nombre del Documento | Fuente | Fecha | Aspectos Relevantes | Relevancia para el SGSI | Observaciones |
|---|---|---|---|---|---|
| | | | | | |

**Nombre del Documento:** Título o nombre completo del documento a analizar.
**Fuente:** Origen del documento (ej. norma oficial, documentación interna de LEYDE, revista científica, consultoría especializada).
**Fecha de Publicación/Actualización:** Indicar la fecha en que fue publicado o la última actualización del documento.
**Aspectos Relevantes**: Resumen de los contenidos clave que abordan requisitos, controles, políticas, procedimientos, brechas y recomendaciones relevantes.
**Relevancia para el SGSI**: Explicación de cómo la información del documento contribuye a la comprensión y desarrollo del SGSI en leche y derivados S.A (LEYDE)
**Observaciones**: Comentarios adicionales sobre la calidad, limitaciones, observaciones específicas o recomendaciones del documento.

## ANEXO 3: PRINCIPALES MARCOS UTILIZADOS ISO27001, PMBOK Y LA METODOLOGIA OCTAVE.

| Área/Proceso | ISO/IEC 27001:2022 | PMBOK | OCTAVE |
|---|---|---|---|
| Contexto y alcance del SGSI | | | |
| Liderazgo y gobernanza | | | |
| Evaluación de riesgos | | | |
| Planificación de objetivos de seguridad | | | |
| Implementación de controles | | | |
| Monitoreo y seguimiento | | | |
| Auditorías internas y revisión directiva | | | |
| Mejora continua (PDCA) | | | |
| Gestión de incidentes | | | |

## ANEXO 2: GUION DE ENTREVISTA SEMIESTRUCTURADA

**MAESTRÍA EN GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN**

**PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LEYDE BASADO EN ISO/IEC 27001:2022**

| | |
|---|---|
| **Fecha de entrevista:** | |
| **Área:** | |
| **Entrevistado:** | |
| **Cargo:** | |

**Introducción:**

Esta entrevista tiene como objetivo recopilar información sobre el estado actual de la seguridad de la información en LEYDE y evaluar las necesidades para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001:2022. Sus respuestas serán confidenciales y utilizadas exclusivamente para fines de esta investigación.

**Preguntas:**

1. ¿Cuál es su percepción sobre la seguridad de la información en LEYDE actualmente?
2. ¿Qué medidas de seguridad se aplican actualmente en la empresa para proteger la información?
3. ¿Cuáles considera que son las principales amenazas o riesgos en cuanto a seguridad de la información?
4. ¿Cree que la empresa cuenta con una cultura de seguridad de la información? ¿Por qué?
5. ¿Existen políticas y procedimientos documentados en la empresa para la gestión de la seguridad de la información?
6. ¿Cómo se manejan los incidentes de seguridad dentro de la organización?
7. ¿Qué aspectos considera que deberían mejorarse para fortalecer la seguridad de la información?
8. ¿Qué tan familiarizado está con la norma ISO/IEC 27001:2022?
9. ¿Cree que la implementación de un SGSI basado en esta norma beneficiaría a la empresa? ¿De qué manera?
10. ¿Qué recursos considera que serían necesarios para implementar con éxito un SGSI en LEYDE

**ANEXO 3: CUESTIONARIO**

**Enlace a Google Forms: https://docs.google.com/forms/d/e/1FAIpQLSdgZIiT4bQ-xKluhShpnIcPSfJccVoPpFFHFRxKLkGxcB9mUg/viewform?usp=header**

unitec®
Universidad Tecnológica Centroamericana

Cuestionario sobre la Implementación de un SGSI basado en ISO/IEC 27001:2022 en LEYDE

josimarherrera7@gmail.com Cambiar de cuenta

No compartido

* Indica que la pregunta es obligatoria

Datos generales

1. Género *

- Maculino
- Femenino
- Prefiero no decirlo

2. Área de de Trabajo *

- IT
- Finanzas
- Recursos Humanos
- Producción
- Ventas
- Otro:

3. Años de experiencia en la empresa *

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

## Estado actual de la Seguridad de la Información

4. ¿Conoce sobre la norma ISO/IEC 27001:2022? *

- ◯ Sí
- ◯ No

5. ¿La empresa cuenta con políticas de seguridad de la información claramente definidas? *

- ◯ Sí
- ◯ No
- ◯ No estoy seguro

6. ¿Ha recibido capacitación en seguridad de la información en los últimos 12 meses? *

- ◯ Sí
- ◯ No

7. ¿Considera que la información sensible de la empresa está protegida adecuadamente? *

- ◯ Sí
- ◯ No
- ◯ No estoy seguro

## Brechas y Necesidades en Seguridad de la Información

8. ¿Cuáles considera que son las principales amenazas a la seguridad de la información en la empresa? (Puede marcar más de una opción) *

- [ ] Accesos no autorizados
- [ ] Robo de información
- [ ] Malware / Ransomware
- [ ] Falta de conciencia del personal
- [ ] Otro: _____

9. ¿Cuáles de las siguientes áreas requieren mejoras en seguridad de la información? (Puede marcar más de una opción) *

- [ ] Protección de datos personales
- [ ] Control de accesos
- [ ] Seguridad en redes y sistemas
- [ ] Concienciación del personal
- [ ] Otro: _____

10. ¿Cree que la implementación de un SGSI mejoraría la protección de la información en la empresa? *

- ◯ Si
- ◯ No
- ◯ No estoy seguro

## Factibilidad y Recursos para la Implementación del SGSI

11. ¿Considera que la empresa cuenta con los recursos necesarios para implementar un SGSI? *

- ◯ Sí
- ◯ No
- ◯ No estoy seguro

12. ¿Qué tipo de apoyo considera más importante para la implementación de un SGSI? (Puede marcar más de una opción) *

- [ ] Capacitación del personal
- [ ] Tecnología y herramientas adecuadas
- [ ] Asesoría especializada
- [ ] Otro: _____

13. En una escala del 1 al 5, ¿Qué tan preparado cree que está el personal para adoptar un SGSI? *

- ◯ 1. Nada preparado
- ◯ 2. Poco preparado
- ◯ 3. Medianamente preparado
- ◯ 4. Bien preparado
- ◯ 5. Muy preparado

## Comentarios y recomendaciones

14. ¿Qué acciones considera prioritarias para fortalecer la seguridad de la información en la empresa? *

Tu respuesta

15. ¿Desea agregar algún comentario o sugerencia sobre la implementación del SGSI? *

Tu respuesta

16. ¿Desea agregar algún comentario o sugerencia sobre la implementación del SGSI? *

Tu respuesta

**ANEXO 4: LISTA DE VERIFICACIÓN DE CUMPLIMIENTO**

**MAESTRÍA EN GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN**
**PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LEYDE BASADO EN ISO/IEC 27001:2022**

**Objetivo:**
Evaluar el grado de cumplimiento de LEYDE en relación con los controles y requisitos de la norma ISO/IEC 27001:2022, identificando las brechas existentes.:

| 4 | La Organización y su Contexto | Cumple (Sí/No/Parcial) | Riesgo Asociado (Alto/Medio/Bajo) |
|---|---|---|---|
| **4.1** | **Entendiendo la Organización y su contexto** | | |
| 1.- | ¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información? | | |
| 2.- | ¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información? | | |
| 3.- | ¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información? | | |
| **4.2** | **Expectativas de las partes interesadas** | | |
| 1.- | ¿Se han identificado las partes interesadas? | | |
| 2.- | ¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas? | | |
| 3.- | ¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales? | | |
| **4.3** | **Alcance del SGSI** | | |
| 1.- | ¿Se ha determinado el alcance del SGS y se conserva información documentada? | | |
| **4.4** | **SGS Sistema de Gestión de la Seguridad de la información** | | |
| 1.- | ¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora? | | |

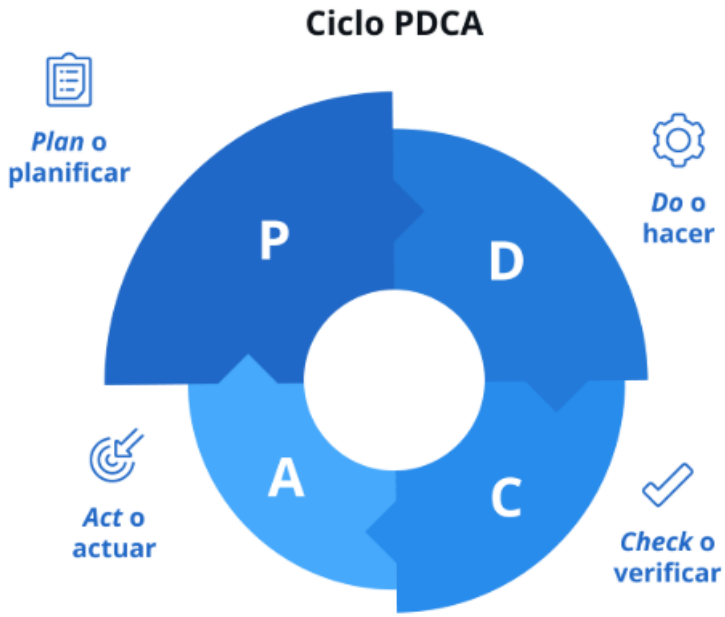
| | | | |
|---|---|---|---|
| **5** | **Liderazgo** | | |
| **5.1** | **Liderazgo y compromiso** | | |
| 1.- | ¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio? | | |
| 2.- | ¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI? | | |
| 3.- | ¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI? | | |
| **5.2** | **Política de la Seguridad de la Información** | | |
| 1.- | ¿Se ha definido una Política de la Seguridad de la Información? | | |
| 2.- | ¿Se ha establecido un marco que permita el establecimiento de objetivos? | | |
| 3.- | ¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa? | | |
| 4.- | ¿Se mantiene información documentada de la política del SGSI y de sus objetivos? | | |
| **5.3** | **Roles y Responsabilidades** | | |
| 1.- | ¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información? | | |
| 2.- | ¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información? | | |
| **6** | **Planificación** | | |
| **6.1** | **Tratamiento de Riesgos y Oportunidades** | | |
| 1.- | ¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación con la Seguridad de la Información? | | |
| 2.- | ¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos? | | |
| 3.- | ¿Se ha definido un proceso de tratamiento de riesgos? | | |
| 4.- | ¿Se han establecido criterios para elaborar una declaración de aplicabilidad? | | |
| 5.- | ¿Se mantiene información documentada de los puntos anteriores? | | |
| **6.2** | **Planificación para consecución de objetivos** | | |
| 1.- | ¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivos del negocio? | | |

| | | | |
|---|---|---|---|
| 2.- | ¿Los objetivos de la Seguridad de la Información están planificados mediante?<br>-Asignación de responsabilidades<br>-Cronograma de ejecución temporal<br>-Método de evaluación | | |
| 3.- | ¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización teniendo en cuenta las funciones principales dentro de la Organización? | | |
| **7** | **Soporte** | | |
| **7.1** | **Recursos** | | |
| 1.- | ¿Se identifican y asignan los recursos necesarios para el SGSI? | | |
| **7.2** | **Competencia** | | |
| 1.- | ¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad? | | |
| 2.- | ¿Se mantiene información actualizada sobre la competencia del personal? | | |
| **7.3** | **Concienciación** | | |
| 1.- | ¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información? | | |
| 2.- | ¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información? | | |
| **7.4** | **Comunicación** | | |
| 1.- | ¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno? | | |
| 2.- | ¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información? | | |
| **7.5** | **Información Documentada** | | |
| 1.- | ¿Se dispone de la documentación requerida por la norma más la requerida por la organización incluyendo?<br>-La política de la Seguridad de la Información y el alcance del Sistema de Gestión<br>-Los procesos principales de la seguridad de la Información<br>-Los Documentos exigidos por la Norma ISO 27001 incluyendo registros<br>-Los Documentos propios de Seguridad de la Información identificados por la empresa (instrucciones técnicas etc.) | | |
| 2.- | ¿Existe un control documental donde se verifica?<br>-Quien publica el documento<br>-Quien lo autoriza y como se revisan<br>-Formatos y Soportes de publicación<br>-Su almacenamiento y protección | | |

| | | | |
|---|---|---|---|
| 3.- | ¿Se controlan los documentos de origen externo? | | |
| **8** | **Operación** | | |
| **8.1** | **Control Operacional** | | |
| 1.- | ¿Los procesos de seguridad de la Información están documentados para controlar que se realizan según lo planificado? | | |
| 2.- | ¿Existe un proceso para evaluar los riesgos en la Seguridad de la Información antes de realizar cambios en el Sistema de Gestión o procesos de Seguridad? | | |
| 3.- | ¿Se establecen medidas y planes para mitigar los riesgos en la Seguridad de la Información ante cambios realizados? | | |
| 4.- | ¿Se identifican y controlan los procesos externalizados en cuanto a los riesgos para la Seguridad de la Información? | | |
| **8.2** | **Análisis de riesgos de la Seguridad de la Información** | | |
| 1.- | ¿Se ha establecido un proceso documentado de análisis y evaluación de riesgos para la Seguridad de la Información donde se identifique?<br>-El propietario del riesgo<br>-La importancia del riesgo o nivel de impacto<br>-La probabilidad de ocurrencia | | |
| **8.3** | **Tratamiento de riesgos de la Seguridad de la Información** | | |
| 1.- | ¿Se ha implementado un plan de tratamiento de riesgos dónde?<br>-Los propietarios del riesgo están informados y han aprobado el plan<br>-Se documentan los resultados | | |
| 2.- | ¿Se identifican todos los controles necesarios para mitigar el riesgo justificando su aplicación? | | |
| 3.- | ¿Se documenta el nivel de aplicación de todos los controles a aplicar? | | |
| **9** | **Evaluación del desempeño** | | |
| **9.1** | **Seguimiento y medición** | | |
| 1.- | ¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información teniendo en cuenta los controles para la seguridad de la información? | | |
| 2.- | ¿Se ha establecido un proceso documentado para evaluar los resultados de las mediciones y de que estos resultados son tomados en cuenta por los responsables tanto de los procesos como de la Seguridad de la Información? | | |
| **9.2** | **Auditorías Internas** | | |

| | | | |
|---|---|---|---|
| 1.- | ¿Se ha establecido una programación de Auditorías Internas y asignado responsables? | | |
| 2.- | ¿Se ha definido el alcance y los requisitos para el informe de auditoría? | | |
| 3.- | ¿Se consideran acciones correctivas y propuestas de cambio en los informes de auditoría? | | |
| **9.3** | **Informe de Revisión por la Dirección** | | |
| 1.- | ¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica? | | |
| 2.- | ¿Se documentan los resultados de los informes y la dirección se implica tanto en su conocimiento como en la toma de decisiones sobre los aspectos cruciales para el SGSI? | | |
| **10** | **Mejora** | | |
| **10.1** | **No Conformidades y acciones correctivas** | | |
| 1.- | ¿Existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento? | | |
| 2.- | ¿Dentro de las acciones correctivas existe una diferenciación entre acciones correctivas sobre la no conformidad y sobre las causas de esta? | | |
| **10.2** | **Mejora continua** | | |
| 1.- | ¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora? | | |

## ANEXO 5: CICLO PDCA




## ANEXO 6: METODOLOGÍA OCTAVE