UNIVERSIDAD NACIONAL DE CHIMBORAZO

VICERRECTORADO DE INVESTIGACIÓN,
VINCULACIÓN Y POSGRADO
DIRECCIÓN DE POSGRADO

TESIS PREVIA LA OBTENCIÓN DEL GRADO DE:
MAGISTER EN CONTABILIDAD Y AUDITORÍA

TEMA:

Propuesta de diseño de un Sistema de Gestión para la Seguridad de la Información bajo ISO 27001:2022. Caso: Legio Seguridad Legsegu Cia. Ltda.

AUTOR:

Mariana Isabel Gualli Pincay

TUTOR:

Zaldumbide Coveña José María

Riobamba, Ecuador.

2026

CERTIFICADO DE TUTOR

Certifico que el presente trabajo de titulación previo a la obtención del Grado de Magíster en Contabilidad y Auditoría con el tema: Propuesta de diseño de un Sistema de Gestión para la Seguridad de la Información bajo ISO 27001:2022. Caso: Legio Seguridad Legsegu Cia. Ltda. ha sido elaborado por **Mariana Isabel Gualli Pincay**, con el asesoramiento permanente de mi persona en calidad de Tutor, por lo que certifico que se encuentra apto para su presentación y defensa respectiva.

Es todo cuanto puedo informar al honor a la verdad.

Riobamba, 6 de agosto de 2026

_____

Zaldumbide Coveña José María

TUTOR

Declaración de autoría Cesión de derechos

Yo **Mariana Isabel Gualli Pincay** con cédula de identidad **Nº 0602948986** declaro y acepto ser responsable de las ideas, doctrinas, resultados y lineamientos alternativos realizados en el presente trabajo de titulación denominado: Propuesta de diseño de un Sistema de Gestión para la Seguridad de la Información bajo ISO 27001:2022. Caso: Legio Seguridad Legsegu Cia. Ltda.

Declaro que mi trabajo investigativo pertenece al patrimonio de la Universidad Nacional de Chimborazo de conformidad con lo establecido en el artículo 20 literal j) de la Ley Orgánica de Educación Superior LOES.

Autorizo a la Universidad Nacional de Chimborazo que pueda hacer uso del referido trabajo de titulación y a difundirlo como estime conveniente por cualquier medio conocido, y para que sea integrado en formato digital al Sistema de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor, dando cumplimiento de esta manera a lo estipulado en el artículo 144 de la Ley Orgánica de Educación Superior LOES.

Riobamba, 6 de agosto de 2026

Mariana Isabel Gualli Pincay

CI: 0602948986

Agradecimiento

Quiero agradecer profundamente a Dios por ser mi guía y fortaleza en este camino académico, iluminando mi mente y mi corazón en cada paso del proceso.

A mi madre, quien con su amor, sacrificio y apoyo incondicional me ha dado la oportunidad de alcanzar mis metas; su ejemplo y sus valores han sido mi mayor inspiración, también expreso mi gratitud a mis hermanos y seres queridos, cuyo aliento constante ha sido fundamental para superar los desafíos que se presentan.

Extiendo un sincero reconocimiento a mi tutor de tesis, José María Zaldumbide Coveña, por su valiosa orientación, paciencia y aportes que enriquecieron este trabajo.

A mis docentes y compañeros de la maestría, quienes con sus conocimientos y experiencias contribuyeron a mi formación académica y personal; finalmente, agradezco a todas las personas que, de manera directa o indirecta, posible hicieron la culminación de esta etapa tan significativa

Dedicatoria

Quiero dedicar el presente trabajo de titulación con profundo amor y gratitud a mi madre, cuya guía, sacrificio y apoyo incondicional me han inspirado a alcanzar mis metas académicas. A mi familia, por ser mi fortaleza en los momentos difíciles y mi mayor motivo de perseverancia.

También lo dedico a mi querida hija Fátima Padilla y mi hermano Sergio Gualli, por creer en mí y brindarme su constante apoyo.

Índice General

Índice de Tablas

Índice de Figuras

Resumen

La seguridad de la información constituye un factor estratégico para las organizaciones debido al incremento de las amenazas cibernéticas y las crecientes exigencias regulatorias. En este contexto, la presente investigación tuvo como objetivo diseñar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2022 para la empresa Legio Seguridad Cía. Ltda., con el propósito de fortalecer la gestión de riesgos y la protección de sus activos de información.

La investigación se desarrolló mediante un enfoque mixto, orientado a diagnosticar el nivel de cumplimiento de los requisitos establecidos en la norma ISO 27001:2022. La población estuvo conformada por los colaboradores de la organización, por lo que se trabajó mediante un censo institucional para la recolección de información, empleando técnicas de observación y entrevista, complementadas con un cuestionario y una ficha de diagnóstico estructurada, a partir de los requisitos de la norma internacional, lo que permitió evaluar el estado de los controles implementados y determinar las principales brechas existentes.

Los resultados evidenciaron un bajo nivel de madurez en el sistema de gestión de seguridad de la información, reflejado en la inexistencia de un sistema de gestión formalmente implementado deficiencias de la gestión documental ausencia de políticas y procedimientos estandarizados, limitada a administración de riesgos debilidades en el control de accesos, gestión de incidentes continuidad del negocio monitoreo de control y procesos de mejora continua así también como las observaciones sobre la asignación de responsabilidades y programas de concienciación sobre seguridad de la información.

Con base en los hallazgos obtenidos, se diseñó una propuesta de sistema de gestión de seguridad de la información alineada con los requisitos de la Norma ISO 27001:2022, integrada por políticas, procedimientos y metodologías para la gestión de riesgos, además de mecanismos de control, documentación técnica y alineamientos para la mejora continua.

Se concluye que la implementación progresiva de esta propuesta permitirá fortalecer la confidencialidad integridad y disponibilidad de la información institucional incrementar el cumplimiento de los requisitos normativos y mejorar la capacidad organizacional gestionar los riesgos sobre la seguridad de la información contribuyendo al fortalecimiento la gobernanza y la sostenibilidad operativa de la empresa

Palabras clave: Gestión de la seguridad de la información, metodología, ISO 27001, sistema de gestión de seguridad de la información.

Abstract

Information security has become a strategic factor for organizations due to the increasing sophistication of cyber threats, growing regulatory requirements, and the need to ensure business continuity. Within this context, this research aimed to design an Information Security Management System based on the ISO 27001:2022 standard for Legio Seguridad Cía. Ltda., with the purpose of strengthening risk management practices and enhancing the protection of the organization's information assets.

The study adopted a mixed-methods approach to assess the organization's compliance with the requirements of the ISO/IEC 27001:2022 standard. A census-based strategy was applied, involving all organizational personnel. Data were collected through observation, interviews, a structured questionnaire, and a diagnostic checklist based on the standard. This approach enabled the assessment of existing security controls and the identification of the organization's principal compliance gap.

The findings revealed a low level of maturity of the Information Security Management System, evidenced by the absence of a formally implemented, deficiencies in document management, the lack of standardized policies and procedures, limited risk management practices, weaknesses in access control, incident management, business continuity, control monitoring, and continuous improvement processes, as well as shortcomings in the assignment of information security responsibilities and awareness programs.

Based on the findings, an Information Security Management System proposal aligned with the requirements was developed. The proposal incorporates information security policies, operational procedures, risk management methodologies, control mechanisms, technical documentation, and guidelines to support the continual improvement of the management system.

It is concluded that the progressive implementation of the proposed will strengthen the confidentiality, integrity, and availability of organizational information, enhance compliance with regulatory and international standard requirements, and improve the organization's capability to manage information security risks, thereby contributing to stronger information security governance and the long-term operational sustainability of the company.

Keywords: Information security management, methodology, ISO 27001, information security management system.

Introducción

En un mundo altamente interconectado, la gestión adecuada de la seguridad de la información se ha convertido en un factor crítico para las organizaciones que buscan proteger sus activos y garantizar la continuidad de sus operaciones.

La norma internacional ISO 27001:2022 establece un marco integral para implementar, mantener y mejorar continuamente un Sistema de Gestión para la Seguridad de la Información (SGSI), asegurando el manejo efectivo de riesgos asociados a la confidencialidad, integridad y disponibilidad de los datos.

Esta investigación, pretende generar una propuesta de diseño de un SGSI basado en ISO 27001:2022, para Legio Seguridad Legsegu Cia. Ltda., una empresa que enfrenta retos crecientes relacionados con la protección de la información en un entorno regulatorio y comercial cada vez más exigente.

Al enfocar como propósito la identificación de vulnerabilidades, el establecimiento de controles adecuados y la alineación a los procesos organizacionales con las mejores prácticas internacionales, se contribuye a mantener la confianza de los clientes y la resiliencia de la empresa frente a posibles amenazas permitiendo de este modo no solo proporcionar un marco estratégico para la seguridad de la información, sino también sentar las bases para su implementación y certificación futura, lo que será necesario tras la vigencia de la Ley Orgánica de Protección de Datos Personales (LOPDP) vigente desde su publicación en el Registro Oficial el 26 de mayo de 2021. Sin embargo, para su aplicación práctica, el régimen sancionatorio entró en vigor dos años después, el 26 de mayo de 2023.

En el contexto ecuatoriano, la entrada en vigor de la Ley Orgánica de Protección de Datos Personales marca un hito significativo en la regulación del manejo de información sensible pues esta legislación exige a las organizaciones adoptar prácticas robustas para garantizar el cumplimiento de derechos fundamentales relacionados con la privacidad y el tratamiento adecuado de los datos personales.

En este sentido, las empresas deben alinear sus políticas y procesos con estándares internacionales como ISO 27001:2022, no solo para cumplir con la normativa nacional, sino también para fortalecer su posición en un entorno comercial cada vez más competitivo.

CAPÍTULO 1

GENERALIDADES

1.1 Planteamiento del problema

La empresa Legsegu Cía Ltda. enfrenta múltiples desafíos en la gestión de la seguridad de la información, lo que compromete la confidencialidad, integridad y disponibilidad de sus datos críticos. Actualmente, la empresa no cuenta con un sistema de gestión de seguridad de la información (SGSI) robusto y estandarizado, lo que ha generado vulnerabilidades y brechas de seguridad. Las causas principales de esta problemática incluyen la falta de un diagnóstico preciso de la situación actual, la ausencia de procedimientos estandarizados basados en normas internacionales como ISO 27001:2022 y la carencia de un manual de buenas prácticas para guiar a los empleados en la protección de la información. Estas deficiencias no solo ponen en riesgo los activos de información de la empresa, sino que también afectan la confianza de los clientes, sus socios comerciales y la reputación de Legsegu en el mercado.

La implementación de un SGSI basado en ISO 27001:2022 en Legsegu Cía Ltda. es esencial para mitigar estos riesgos, pues un sistema bien diseñado proporcionará una estructura clara para identificar y gestionar las amenazas a la seguridad de la información, estableciendo controles adecuados y promoviendo una cultura de seguridad entre los empleados. Entonces, la elaboración de un manual de gestión de seguridad de la información, acompañado de procedimientos y buenas prácticas, no solo ayudará a cumplir con los estándares internacionales, sino que también mejorará la eficiencia operativa y reducirá la probabilidad de incidentes de seguridad.

1.2 Objetivos

1.2.1 Objetivo General

Diseñar un manual de gestión de seguridad de la información bajo ISO 27001 acompañado de procedimientos y buenas prácticas para garantizar la confidencialidad, integridad y disponibilidad de la información en la empresa Legsegu Cia Ltda

1.2.2 Objetivos Específicos

- Realizar el levantamiento y análisis de la información para determinar el diagnóstico de la situación actual de la empresa.
- Generar una plantilla de diagnóstico general basada en ISO 27001

- Generar buenas prácticas y procedimientos para la aplicación de ISO 27001 en la gestión empresarial.

1.2 Justificación de la Investigación

La creciente dependencia de las tecnologías de la información y la proliferación de amenazas cibernéticas hacen que la gestión de la seguridad de la información sea un aspecto crucial para las organizaciones; en este contexto, Legsegu Cía. Ltda. enfrenta desafíos significativos debido a la ausencia de un Sistema de Gestión de Seguridad de la Información (SGSI) robusto y estandarizado, lo que ha resultado en vulnerabilidades y brechas que comprometen la confidencialidad, integridad y disponibilidad de sus datos críticos.

La falta de procedimientos basados en normas internacionales como ISO 27001:2022 y la inexistencia de un manual de gestión de seguridad de la información, acompañada de procedimientos y buenas prácticas reflejan una debilidad estructural que afecta no solo la protección de los activos de información, sino también la confianza de los clientes y la reputación de la empresa en el mercado.

La implementación de un SGSI basado en ISO 27001:2022 es indispensable para abordar esta problemática, ya que proporciona un marco estructurado que permite identificar, evaluar y gestionar los riesgos asociados a la seguridad de la información, así, este enfoque no solo ayudará a cumplir con estándares internacionales y la normativa local, como la Ley Orgánica de Protección de Datos Personales en Ecuador, sino que también fortalecerá la resiliencia de la empresa ante incidentes de seguridad.

Además, la elaboración de un manual de gestión de seguridad de la información, acompañada de procedimientos claros y buenas prácticas, contribuirá a promover una cultura organizacional enfocada en la seguridad, incrementando la eficiencia operativa y reduciendo la probabilidad de consecuencias financieras y legales.

Por tanto, este proyecto no solo es relevante, sino estratégico para garantizar la sostenibilidad y competitividad de Legsegu Cía. Ltda. en un entorno cada vez más exigente y regulado, asegurando su contribución a un entorno empresarial más ético y transparente.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Antecedentes Investigativos

Para la presente investigación se realizó una lectura y conocimiento previos de trabajos de distintos autores, en relación con la gestión de seguridad de la información bajo ISO 27001, en el Ecuador. A continuación, mediante tesis relacionadas podemos citar trabajos realizados en varias universidades así:

Arellano Veloz (2023) desarrolló un modelo de gestión de seguridad de la información enfocado en una institución financiera cooperativa en Ambato, Ecuador. Su estudio, realizado en la Pontificia Universidad Católica del Ecuador (PUCE), se basó en la identificación de riesgos asociados a la información crítica de la organización y en la aplicación de estándares internacionales para mejorar la protección de los datos. La propuesta incluye estrategias para implementar controles, fortalecer la gestión de riesgos y promover una cultura organizacional orientada a la seguridad de la información, contribuyendo al cumplimiento normativo y la continuidad del negocio. (Arellano Veloz, 2023)

Mera Amores, Isaac Fabricio (2022- PUCE) mediante un estudio realizado en ALTAC, una empresa de contabilidad y auditoría en Quito evaluó la seguridad de la información utilizando el estándar ISO/IEC 27001. Como parte del análisis, se clasificaron los activos de la empresa en cuatro categorías: Activos de Información, Talento Humano, Hardware y Sistemas de Información. Posteriormente, se identifican amenazas y vulnerabilidades asociadas a estos activos, lo que permitió calcular los riesgos y priorizar acciones correctivas. El estudio también incluyó una revisión del cumplimiento de los controles definidos en el Anexo A de la norma ISO 27001, proporcionando recomendaciones específicas para fortalecer la seguridad de la información en la empresa. Este trabajo destaca la importancia de gestionar adecuadamente los riesgos y de adoptar medidas proactivas para mejorar la protección de los activos críticos en el ámbito organizacional. (Mera Amores, 2022)

Chávez y Moya (2022) desarrollaron un proyecto enfocado en la creación de un programa de seguridad de la información para una empresa de gestión de cobranzas, con el propósito de salvar la confidencialidad, integridad y disponibilidad de sus activos de información. El estudio comenzó con un diagnóstico de la situación actual de la empresa, basado en los lineamientos de la norma ISO 27001 y utilizando una herramienta de evaluación

de madurez desarrollada por los autores. Los resultados evidenciaron la ausencia de un sistema de gestión de seguridad de la información (SGSI) y un bajo nivel de madurez frente a los requisitos. Posteriormente, se identificaron las partes interesadas, los tipos de información manejada y su nivel de criticidad, en función de los principios de seguridad de la información , en el análisis de riesgos, se identifican amenazas y vulnerabilidades asociadas, como la destrucción de información, errores de mantenimiento y abuso de privilegios. (Chávez Cabrera, 2022)

María Gabriela Pardo Cuenca (2015) Un proyecto desarrollado en la Universidad Nacional de Loja tuvo como objetivo principal proporcionar medidas de control para proteger los activos de información gestionados por la Unidad de Telecomunicaciones e Información (UTI). Este trabajo se fundamentó en los lineamientos de la norma ISO/IEC 27001 para planificar un Sistema de Gestión de Seguridad de la Información (SGSI) y en la metodología MAGERIT v3 para analizar y gestionar los riesgos informáticos donde mediante entrevistas al personal técnico, se identifican necesidades clave en materia de seguridad de la información. Como resultado del análisis, se activan mecanismos de control para mitigar riesgos y se impulsó la creación de una cultura de seguridad a nivel institucional. Al finalizar el proyecto, se socializó con el personal de la UTI la propuesta del Manual de Políticas de Seguridad de la Información, validando su efectividad como herramienta para minimizar los riesgos asociados a los activos informáticos de la universidad. (Pardo Cuenca, 2015)

John Ruder Contador Minaya - Cristhian Andre Tapia Huaman (Perú- 2024) mediante un estudio realizado en la empresa minera Colibrí SAC, Lima 2023, tuvo como objetivo analizar la influencia del diseño e implementación de la norma ISO 27001 en la mejora de la seguridad de la información. La investigación abarcó a los 70 trabajadores de la sede central, utilizando técnicas como observación, análisis documental, encuestas y entrevistas. Los resultados fueron evaluados con un cuestionario validado con un 82% de confiabilidad, donde se identificó carencias en infraestructura y licenciamiento, como la ausencia de equipos certificados y software con licencias originales, lo que representa riesgos altos, incluyendo exposición a virus, programa maligno y vulneración de datos confidenciales. A pesar de estas deficiencias, se concluyó con un 95% de confianza que la implementación de la norma ISO 27001 mejora significativamente la seguridad de la información, demostrando una relación positiva entre ambas variables en el contexto de la empresa minera. (Contador Minaya, 2023)

2.2 Antecedentes Legales

En Ecuador, la Protección de Datos Personales se sustenta en varias disposiciones constitucionales y legales que establecen principios, derechos, obligaciones y garantía A continuación, se detallan los aspectos clave del marco legal:

2.2.1 Legislación Ecuador

Constitución de la Republica del Ecuador, aprobada en 2008, establece el derecho a la protección de datos personales como un derecho fundamental. Algunos artículos relevantes son:

Artículo 66, numeral 19: Reconoce el derecho a la protección de datos personales, incluyendo el acceso, rectificación, actualización y eliminación de información.

Artículo 92: Regula el acceso a la información pública y privada, garantizando la protección de los datos personales. (Asamblea Constituyente del Ecuador., 2008)

Ley Orgánica de Protección de Datos Personales (LOPDP)

La LOPDP fue publicada en el Registro Oficial en mayo de 2021 y establece las bases para la protección de datos personales en Ecuador. Sus principales aspectos son:

Derechos de los titulares de los datos: Incluyen el acceso, rectificación, supresión, oposición, portabilidad y otros derechos relacionados con el tratamiento de sus datos.

Obligaciones de los responsables del tratamiento: Los responsables del tratamiento deben garantizar la seguridad de los datos, obtener consentimiento explícito para su uso y cumplir con los principios establecidos en la ley.

Creación de la Autoridad de Protección de Datos: La ley prevé la creación de una entidad encargada de supervisar y garantizar el cumplimiento de las normativas, aunque su implementación todavía está en proceso.

Base jurídica para el tratamiento de datos: Incluye consentimiento informado, cumplimiento de obligaciones legales, interés legítimo, ejecución de contratos, entre otros. (Asamblea Nacional del Ecuador., 2021)

Normas relacionadas

Existen otras normativas que interactúan con la LOPDP en el marco del tratamiento de datos:

Código Orgánico Integral Penal (COIP): Tipifica delitos relacionados con la violación de datos personales y actos sancionados como el acceso no autorizado, la venta de información privada**,** Art. 229 (Revelación ilegal de base de datos), Art. 232 (Ataque a la integridad de

sistemas informáticos), Art. 233 (Delitos contra la información pública reservada) y Art. 234 (Acceso no consentido a un sistema informático): entre otros.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos: Regula aspectos del uso de información personal en entornos digitales. Art. 1 (Objeto de la Ley), Art. 48 al 50 (De la Protección al Consumidor), Art. 39 y 40 (De la Confidencialidad).

Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP): Garantiza el acceso a la información pública respetando la protección de datos personales. Artículos (1, 6, y 9).

2.2.2 Legislación Internacional

La LOPDP incorpora principios y estándares establecidos en regulaciones internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea; estas conexiones fortalecen su alineación con marcos globales. A continuación, se describen algunos puntos clave. (Parlamento Europeo & Consejo de la Unión Europea., 2016)

a) Principios compartidos

Tanto la LOPDP como el GDPR comparten principios esenciales, como:

Licitud, lealtad y transparencia: Ambos exigen que los datos personales se traten de manera transparente y justa.

Limitación de la finalidad: Los datos solo pueden usarse para las multas específicas declaradas.

Minimización de datos: Solo se recopilan los datos estrictamente necesarios.

b) Transferencias internacionales

La LOPDP establece restricciones para la transferencia de datos personales fuera de Ecuador, similares a los requisitos del GDPR.

Exige garantías adecuadas de protección, como cláusulas contractuales o certificaciones internacionales.

c) Derechos de los titulares

La LOPDP y el GDPR garantizan derechos como el acceso, rectificación, oposición y supresión de datos.

2.3 Base teórica

La ISO 27001 es una norma internacional creada por la Organización Internacional de Normalización (ISO) junto con la Comisión Electrotécnica Internacional (IEC). Su estructura se basa en el ciclo de mejora continua, conocido como PDCA (Planificar, Hacer, Verificar,

Actuar), teniendo como propósito principal el establecer un enfoque sistemático para identificar, analizar y gestionar los riesgos asociados con la seguridad de la información

ISO 27001 es una norma reconocida internacionalmente que define los requisitos para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI); este estándar ayuda a las organizaciones a proteger su información crítica, cumplir con las regulaciones legales y normativas, y aumentar la confianza de sus partes interesadas al garantizar la seguridad de la información. (International Organization for Standardization (ISO), & International Electrotechnical Commission (IEC)., 2022)

2.3.1 Origen de la ISO 27001

La primera versión fue publicada en 2005, y la más reciente se actualizó en 2022 para reflejar las modernas necesidades de seguridad de la información toda vez que esta norma se aplica a organizaciones de cualquier tamaño, sector o ubicación geográfica y es útil tanto para empresas privadas como para organismos públicos y aquellos sin finalidad de lucro.

La ISO 27001 ha experimentado una evolución desde su primera publicación adaptándose a las crecientes amenazas y desafíos relacionados con la seguridad de la información, así, la actualización más reciente, realizada en el año2022, incorpora nuevos requisitos y controles diseñados para enfrentar las necesidades contemporáneas, como la seguridad en entornos digitales, el uso de tecnologías emergentes y la gestión de datos en un mundo altamente interconectado.

2.3.2 Ámbito de aplicación

La ISO 27001 es un estándar versátil y global que puede ser implementado por organizaciones de cualquier tamaño, sector o región geográfica. Entre sus principales características, destaca:

Flexibilidad: Se adapta tanto a pequeñas y medianas empresas (pymes) como a grandes corporaciones multinacionales.

Aplicabilidad en distintos sectores: Desde tecnología, banca y salud, hasta fabricación, educación y servicios gubernamentales.

Uso por diversos tipos de entidades: Es útil para empresas privadas, instituciones públicas, organizaciones sin fines de lucro y cualquier entidad que maneje información sensible o desee fortalecer su ciberseguridad.

2.3.3 Relación con otras normas

La ISO 27001 forma parte de la familia de normas ISO 27000, un conjunto de estándares internacionales que abordan diferentes aspectos de la gestión de la seguridad de la información. Entre los más destacados se encuentran:

ISO 27002: Controles de seguridad de la información. - Que proporciona recomendaciones para seleccionar, implementar y gestionar controles de seguridad.

Complemento de ISO 27001: Mientras que la ISO 27001 define los requisitos, la ISO 27002 actúa como una guía práctica para aplicar los controles necesarios para cumplir con esos requisitos.

Cobertura: Incluye áreas como la gestión de activos, la seguridad en recursos humanos, la protección de la red y la gestión de incidentes.

ISO 27701: Gestión de la privacidad. - Que extiende el alcance de la ISO 27001 para incluir la protección de datos personales y ayuda a las organizaciones a cumplir con regulaciones de privacidad como el Reglamento General de Protección de Datos (GDPR) en Europa o la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador.

Componentes principales: Incluye directrices para implementar un Sistema de Gestión de Información de Privacidad (SGIP), cubriendo el tratamiento de datos personales, consentimiento, derechos de los titulares de datos y transferencias internacionales.

La combinación de estas normas permite a las organizaciones establecer un marco sólido para proteger tanto la información corporativa como los datos personales, cumpliendo con estándares internacionales y fortaleciendo su posición frente a riesgos y regulaciones

2.3.4 Requisitos principales de la norma

La ISO 27001 establece una serie de requisitos que deben cumplirse para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) de manera efectiva. Estos requisitos se organizan en cláusulas principales y anexos, con un enfoque basado en riesgos y mejora continua de la siguiente manera.

Clausula 1.1 Contexto de la organización

Entender el contexto interno y externo: Identificar factores que puedan influir en los objetivos y la seguridad de la información.

Partes interesadas: Determinar quiénes son los interesados relevantes (clientes, proveedores, reguladores) y sus expectativas en cuanto a la seguridad de la información.

Alcance del SGSI: Definir claramente los límites y el alcance del sistema, especificando las áreas y activos cubiertos.

Clausula 1.2. Liderazgo

Compromiso de la alta dirección: La dirección debe apoyar y promover activamente el SGSI.

Política de seguridad de la información: Establecer y mantener una política que defina objetivos y compromisos relacionados con la seguridad de la información.

Roles y responsabilidades: Designar responsabilidades específicas para la implementación y supervisión del SGSI.

Clausula 1.3. Planificación

Gestión de riesgos: Identificar, analizar y evaluar los riesgos de seguridad de la información.

Tratamiento de riesgos: Gestionar y mitigar los riesgos identificados.

Clausula 1.4. Soporte

Esta cláusula abarca los recursos y elementos necesarios para la implementación eficaz del SGSI:

Recursos: Asegurar que se disponga de recursos humanos, técnicos y financieros adecuados para mantener el SGSI.

Competencias: Capacitar al personal para que tenga las habilidades y conocimientos necesarios en materia de seguridad de la información.

Conciencia: Garantizar que los empleados comprendan sus roles y responsabilidades en la protección de la información.

Comunicación: Definir cómo se comunicarán las políticas, procedimientos y actividades relacionadas con el SGSI dentro y fuera de la organización.

Documentación y control de información: Crear, actualizar y proteger la documentación necesaria para el SGSI, incluidos los procedimientos, registros y políticas.

Clausula 1.5. Operación

Se enfoca en la implementación práctica del SGSI:

Planificación y control operativo: Asegurar que las actividades operativas relacionadas con la seguridad de la información se ejecutarán de acuerdo con los planos establecidos.

Evaluación de riesgos: Implementar las medidas definidas en el tratamiento de riesgos, asegurando que los controles sean eficaces y adecuados.

Gestión de cambios: Controlar los cambios operativos que puedan afectar la seguridad de la información, evitando impactos negativos.

Clausula 1.6. Evaluación del desempeño

La ISO 27001 exige un seguimiento y evaluación continua del SGSI:

Seguimiento, medición y análisis: Supervisar los indicadores claves relacionados con la seguridad de la información.

Auditorías internas: Realizar auditorías periódicas para verificar el cumplimiento de la norma y la eficacia del SGSI.

Revisión por la dirección: Evaluar periódicamente el SGSI para asegurar que se alinea con los objetivos estratégicos y sigue siendo adecuado frente a cambios en el entorno.

Clausula 1.7. Mejora

Este apartado promueve la mejora continua del SGSI:

No conformidades y acciones correctivas: Identificar y abordar las desviaciones o problemas en la gestión de la seguridad de la información, asegurando que no se repitan.

Mejora continua: Revisar y perfeccionar el SGSI para adaptarlo a nuevos riesgos, tecnologías y cambios organizativos.

2.3.5 Controles de Seguridad

El Anexo A de la ISO 27001 incluye un catálogo de 93 controles de seguridad organizados en 4 categorías principales, que deben ser seleccionados e implementados según el tratamiento de riesgos, estos controles están alineados con la ISO 27002, que proporciona directrices detalladas para su aplicación siendo estos:

Controles organizativos

Incluyen políticas y procedimientos generales para la gestión de la seguridad, como:

Establecimiento de roles y responsabilidades, Gestión de relaciones con terceros y protección contra amenazas internas.

Controles de personas

Están relacionados con la formación y gestión del personal:

Capacitación en seguridad de la información, verificación de antecedentes para empleados con acceso a datos sensibles, gestión de la terminación laboral para asegurar la protección de la información.

Controles tecnológicos

Se enfocan en la implementación de medidas técnicas, como:

Cifrado de datos, Gestión de accesos y autenticación, Monitoreo de sistemas y redes.

Gestión de incidentes de seguridad.

Controles físicos

Abarcan la protección de los entornos donde se almacena o procesa información:

Seguridad en los accesos físicos, Protección contra desastres naturales o incendios; y, monitoreo de instalaciones.

2.3.6 Documentación requerida

La norma exige que se mantenga una documentación clara y organizada para demostrar el cumplimiento. Entre los documentos obligatorios destacan:

- Política de seguridad de la información.
- Declaración de aplicabilidad (SoA, por sus siglas en inglés).
- Informe de evaluación de riesgos.
- Plan de tratamiento de riesgos.
- Procedimientos de gestión de incidentes.

2.3. Beneficios de su implementación

La ISO 27001 no solo protege la información y reduce los riesgos, sino que también mejora la competitividad y la confianza en el mercado. Además, ofrece varios beneficios a las organizaciones así, por ejemplo:

Mejora de la seguridad de la información: La ISO 27001 proporciona un marco estructurado para identificar, gestionar y proteger la información sensible, lo que reduce el riesgo de brechas de seguridad.

Cumplimiento de regulaciones y leyes: Implementar ISO 27001 ayuda a cumplir con diversas normativas relacionadas con la protección de datos y la privacidad, como es el caso del RGPD (Reglamento General de Protección de Datos).

Confianza y reputación: Al obtener la certificación ISO 27001, las empresas demuestran su compromiso con la seguridad de la información, lo que aumenta la confianza de clientes, proveedores y socios comerciales.

Reducción de riesgos: La norma ayuda a identificar y mitigar riesgos relacionados con la seguridad de la información, como ataques cibernéticos, pérdida de datos, accesos no autorizados, entre otros.

Mejora de procesos internos: La implementación de la norma permite a las organizaciones mejorar sus procesos de gestión de la seguridad de la información, promoviendo la eficiencia y la efectividad a largo plazo.

Ventaja competitiva: Contar con una certificación ISO 27001 puede ser un diferenciador importante en un mercado competitivo, ya que los clientes a menudo prefieren trabajar con empresas que demuestren un enfoque serio hacia la seguridad de la información.

Protección contra pérdidas económicas: Al reducir el riesgo de incidentes de seguridad, las empresas disminuyen la probabilidad de pérdidas económicas asociadas con el robo de datos, interrupciones del negocio o sanciones regulatorias.

Mejor gestión de incidentes de seguridad: Con la implementación de ISO 27001, las empresas desarrollan planes de respuesta a incidentes, lo que permite una acción rápida y eficaz en caso de dichos incidentes, además de que se fomenta una cultura organizacional centrada en la seguridad, sensibilizando a todos los empleados sobre la importancia de proteger la información.

Mejora continua: La norma promueve la mejora continua de la seguridad de la información, lo que permite a la organización adaptarse a los cambios tecnológicos y las amenazas emergentes.

2.4. Marco Conceptual

Para implementar la norma ISO/IEC 27001 (un estándar internacional para sistemas de gestión de seguridad de la información, SGSI), es crucial entender ciertos conceptos clave. Estos te permitirán desarrollar un sistema robusto que cumpla con los requisitos de la norma. A continuación, se presentan los conceptos principales:

2.4.1 Seguridad de la Información

La seguridad de la información es el conjunto de medidas, políticas y tecnologías diseñadas para proteger los datos contra el acceso, uso, alteración o destrucción no autorizados, que se basa en tres pilares fundamentales:

Confidencialidad: Garantiza que la información solo esté disponible para personas autorizadas así, por ejemplo: implementar contraseñas o cifrado en documentos sensibles.

Integridad: Asegura que los datos no sean alterados o modificados sin autorización, por ejemplo: usar controles de versión en sistemas de gestión documental.

Disponibilidad: Garantiza que la información esté accesible cuando se necesita. Así por ejemplo: sistemas de respaldo y recuperación ante desastres. (International Organization for Standardization (ISO), & International Electrotechnical Commission (IEC)., 2022)

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

Un SGSI es un marco sistemático y organizado que basa su accionar en procesos procedimientos y actividades que permitan cumplir con la normativa legal vigente, el cual debe:

Definir políticas: Reglas generales para gestionar la seguridad de la información.

Implementa controles: Procedimientos y herramientas para proteger la información.

Monitorea y mejora: Audita y actualiza constantemente el sistema.

Este marco permite gestionar de manera estructurada los riesgos y asegura el cumplimiento con los requisitos legales y contractuales. (International Organization for Standardization (ISO), & International Electrotechnical Commission (IEC)., 2022)

2.4.3. Contexto de la Organización

Entender el contexto de la organización implica:

Factores internos: Estructura organizacional, objetivos, procesos, y recursos.

Factores externos: Entorno competitivo, regulaciones legales, y amenazas externas.

Partes interesadas: Identificar a todas las personas u organizaciones (clientes, empleados, proveedores, autoridades) que influyen o se ven afectadas por la seguridad de la información.

Ejemplo práctico: Identificar que una organización financiera está expuesta a regulaciones de protección de datos (como GDPR) y amenazas de ciberataques. (International Organization for Standardization (ISO), & International Electrotechnical Commission (IEC)., 2022)

2.4.4. Análisis de Riesgos

El análisis de riesgos es un componente central del SGSI. Pasos clave:

Identificar riesgos: Determinar amenazas (p. ej., malware) y vulnerabilidades (p. ej., sistemas sin parches).

Evaluar riesgos: Analizar la probabilidad e impacto de cada riesgo.

Priorizar riesgos: Clasificar los riesgos según su gravedad.

Mitigar riesgos: Implementar controles específicos para reducirlos a un nivel aceptable.

Herramientas comunes: Análisis FODA, matrices de riesgos,

2.4.5. Controles de Seguridad

ISO 27001 define una lista de controles en el Anexo A. Estos controles son medidas técnicas, físicas y administrativas para gestionar los riesgos. Ejemplos:

Controles organizacionales: Política de seguridad, gestión de riesgos, acuerdos de confidencialidad.

Controles de personas: Formación y concienciación en seguridad.

Controles físicos: Acceso restringido a edificios, cerraduras, cámaras de vigilancia.

Controles tecnológicos: Firewalls, cifrado, gestión de contraseñas, antivirus.

2.4.6. Declaración de Aplicabilidad (SoA)

Este documento es esencial en ISO 27001. Incluye:

Los controles que la organización ha decidido implementar.

Los controles que se han excluido, junto con la justificación. Ejemplo: Si una organización no almacena datos en la nube, puede justificar que no aplica controles relacionados con la seguridad en servicios de nube.

2.4.7. Gestión Documental

ISO 27001 requiere que ciertos documentos sean creados y mantenidos, como:

Política de seguridad de la información.

Evaluaciones de riesgos.

Procedimientos de gestión de incidentes.

Registros de auditorías y acciones correctivas.

La documentación no solo demuestra conformidad con la norma, sino que también establece una guía clara para los empleados.

2.4.8. Auditoría Interna

Las auditorías internas son esenciales para evaluar si el SGSI cumple con los requisitos de ISO 27001 y funciona eficazmente. Pasos principales:

Planificación: Determinar el alcance y frecuencia de las auditorías.

Ejecución: Revisar la documentación, entrevistar al personal, y evaluar los controles implementados.

Informes: Documentar hallazgos y áreas de mejora.

Seguimiento: Corregir no conformidades identificadas.

2.4.9. Mejora Continua (Ciclo PDCA)

ISO 27001 se basa en el ciclo de mejora continua:

Planificar: Identificar riesgos, establecer objetivos de seguridad, y planificar controles.

Hacer: Implementar políticas, procedimientos, y controles.

Verificar: Realizar auditorías internas y monitorear el desempeño.

Actuar: Corregir errores, actualizar controles y mejorar continuamente.

Este ciclo asegura que el SGSI se mantenga efectivo frente a cambios internos y externos.

2.4.10. Requisitos Legales y Reglamentarios

Es obligatorio identificar y cumplir con las leyes y regulaciones relacionadas con la seguridad de la información. Ejemplos:

Reglamento General de Protección de Datos (GDPR): Para organizaciones que manejan datos personales en Europa.

Ley de Protección de Datos Personales: En países como México, España o Argentina.

Normas sectoriales: Como PCI DSS para organizaciones que manejan pagos con tarjeta.

2.4.11. Liderazgo y Compromiso

El éxito de la implementación depende del compromiso de la alta dirección. Sus responsabilidades incluyen:

Establecer una política de seguridad clara.

Proveer recursos necesarios (personal, tecnología, presupuesto).

Participar en revisiones del SGSI y tomar decisiones estratégicas.

2.4.12. Formación y Concienciación

Los empleados son la primera línea de defensa. Por lo tanto, es importante:

Capacitar al personal sobre prácticas seguras (gestión de contraseñas, evitar phishing, etc.).

Realizar campañas de concienciación para mantener una cultura de seguridad. Ejemplo: Simulaciones de ataques de phishing para educar al personal.

2.4.13. Gestión de Incidentes

La norma requiere que la organización tenga un proceso claro para manejar incidentes de seguridad:

Detección: Identificar el incidente (p. ej., intento de hackeo, fuga de datos).

Notificación: Reportar el incidente a las partes responsables.

Respuesta: Tomar medidas para minimizar el impacto (p. ej., desconectar un sistema comprometido).

Lecciones aprendidas: Documentar el incidente, analizar las causas y prevenir futuros eventos

CAPÍTULO 3

DISEÑO METODOLÓGICO

3.1 Enfoque de la Investigación

Para alcanzar una comprensión integral y detallada del tema, se eligió un enfoque de investigación mixto que integró las fortalezas de los métodos cualitativos, caracterizados por su flexibilidad y capacidad para profundizar en los detalles, con las ventajas de los métodos cuantitativos, reconocidos por su rigor y posibilidad de generalización. Este diseño permitió analizar la gestión del sistema de seguridad en la empresa Legio Seguridad Legsegu Cía. Ltda., tomando como referencia los requisitos establecidos en la norma ISO 2700

3.2 Diseño de la Investigación

La presente investigación se desarrolló bajo un diseño no experimental, debido a que la variable no fue manipulada y los fenómenos se observaron en su contexto natural. El estudio se centró en evaluar el estado actual del Sistema de Gestión de Seguridad de la Información (SGSI) de Legio Seguridad Legsegu Cía. Ltda., identificando el nivel de cumplimiento de los requisitos establecidos en la norma ISO/IEC 27001:2022, sin intervenir ni modificar las condiciones existentes.

Asimismo, el diseño fue de tipo transversal, puesto que la información se recopiló en un único momento del tiempo, permitiendo realizar un diagnóstico de la situación organizacional y establecer una propuesta de mejora basada en los resultados obtenidos

3.3 Tipo de investigación

Por el nivel o alcance: El alcance de esta investigación se clasifica como descriptivo, dado que se enfoca en realizar un diagnóstico del cumplimiento de la norma ISO 27001. Este diagnóstico tiene como objetivo evaluar el estado actual del sistema de gestión de seguridad de la información dentro de una organización. A través de esta evaluación, se identifican fortalezas, debilidades, oportunidades y amenazas (FODA), lo que permite distinguir los aspectos que ya cumplen con los requisitos de la norma y aquellos que necesitan ser mejorados para alcanzar los estándares establecidos.

Por el lugar: En cuanto a la ubicación del análisis, la base teórica del diagnóstico se sustenta en los lineamientos y requisitos proporcionados por la norma ISO 27001, junto con guías y mejores prácticas reconocidas internacionalmente en el ámbito de la seguridad de la información. Además, se incorporaron referencias a estudios de caso y experiencias de otras organizaciones, lo que enriqueció el análisis al permitir comparaciones y la identificación de patrones comunes en la gestión de la seguridad.

Investigación de Campo: El diseño de la investigación también se clasifica como de campo, ya que los datos fueron recolectados directamente de la realidad, estudiando los fenómenos tal como ocurren en su contexto natural, sin manipular las variables. Para ello, se utilizó una metodología que incluyó la recopilación de información mediante herramientas como encuestas y entrevistas, asegurando que los datos obtenidos fueran representativos de la situación real de la organización. Este enfoque permitió obtener una visión precisa y detallada de las áreas que requieren atención y mejora en el sistema de gestión de seguridad de la información.

3.4 Nivel de Investigación

Inductivo: Porque permitió deducir información por medio de la aplicación de instrumentos, en este caso se consideraron los requisitos de la norma ISO 27001 como modelo generalizado a la empresa Legio Seguridad Legsegu Cía. Ltda.

3.5 Métodos de Investigación

Método Inductivo: En este estudio se utilizó el método inductivo, ya que facilitó la obtención de conclusiones a partir del análisis de datos recogidos mediante la aplicación de diversos instrumentos. Este enfoque permitió interpretar la información obtenida al considerar a la empresa Legio Seguridad Legsegu Cía. Ltda. como un caso representativo para la implementación de los requisitos de la norma ISO 27001. De esta forma, el análisis particular de esta empresa sirvió como base para comprender la aplicabilidad de la norma.

Método Descriptivo: Se aplicó el método inductivo porque permitió deducir información por medio de la aplicación de instrumentos, en este caso se consideró a la empresa Legio Seguridad Legsegu Cía. Ltda. como modelo de aplicación de ISO 27001.

El método descriptivo fue empleado para examinar y detallar características específicas de la situación estudiada, permitiendo evaluar los procesos de gestión de la seguridad de la información dentro de un marco temporal. Este enfoque se utilizó para analizar los datos recopilados, identificando la trazabilidad de los requisitos de la norma ISO 27001.

3.6 Técnicas e Instrumentos de Recolección de Datos

Entrevista y Observación. - Estas técnicas permitieron recopilar información relevante y específica sobre la realidad empresarial de Legio Seguridad en términos de la gestión de seguridad de la información. A través de entrevistas con los responsables y observaciones directas, se obtuvieron datos cualitativos clave para comprender el estado actual de la implementación de la norma ISO 27001.

3.7 Técnicas para el procesamiento e Interpretación de Datos

Ficha de Diagnóstico ISO 27001: Este instrumento fue diseñado como un documento estructurado para registrar de forma sistemática y detallada todas las observaciones obtenidas durante el proceso de investigación. La ficha permitió organizar y analizar los datos relacionados con los requisitos de la norma y su cumplimiento dentro de la empresa estudiada.

Cuestionario: Se utilizó como herramienta para obtener información adicional de los colaboradores de la empresa, con el objetivo de evaluar su conocimiento, percepción y

experiencia en la gestión de la seguridad de la información. Los datos recopilados a través del cuestionario complementaron las observaciones y entrevistas, proporcionando un enfoque integral al análisis de la implementación de la norma.

Este conjunto de métodos, técnicas e instrumentos permitió abordar el estudio desde diferentes perspectivas, garantizando un análisis detallado y completo de la implementación de la norma ISO 27001 en la empresa Legio Seguridad Legsegu Cía. Ltda.

3.8 Población y Muestra

La población objeto de estudio estuvo conformada por la totalidad de los colaboradores de Legio Seguridad Legsegu Cía. Ltda., integrada por 20 trabajadores pertenecientes a las diferentes áreas de la organización.

Debido al reducido tamaño de la población, se trabajó con la totalidad de sus integrantes; por consiguiente, se realizó un censo poblacional y no fue necesario aplicar una fórmula para determinar una muestra, ya que todos los colaboradores participaron en la recolección de la información.

Por tratarse de un censo, no se aplicó ningún procedimiento de muestreo probabilístico o no probabilístico, garantizando así la representación completa de la población de estudio.

Tabla 1 Población

POBLACION	CANTIDAD
Gerente	1
Supervisor	1
Talento humano	1
Coordinador	1
Logística	16
TOTAL	20

Nota: Autor

3.9 Validación del instrumento

El instrumento de recolección de datos fue elaborado con base en los requisitos, controles y lineamientos establecidos en la norma internacional ISO/IEC 27001:2022, considerando las cláusulas de gestión y los controles de seguridad de la información aplicables a la organización.

Posteriormente, el instrumento fue sometido a validación de contenido mediante juicio de expertos. En este proceso participaron tres especialistas con experiencia en Sistemas de

Gestión de Seguridad de la Información, auditoría basada en normas ISO, gestión de riesgos y metodología de la investigación.

Los expertos evaluaron los siguientes criterios:

- Pertinencia de los ítems.
- Claridad de la redacción.
- Coherencia con los objetivos de investigación.
- Correspondencia con las dimensiones evaluadas.
- Relevancia técnica respecto de la norma ISO/IEC 27001:2022.

Con base en las observaciones formuladas, se realizaron ajustes relacionados con la redacción, organización y precisión técnica de algunos ítems, obteniéndose la versión definitiva del instrumento para su aplicación.

3.10 Variables

Considerando que la investigación posee un enfoque descriptivo y propositivo, se trabajó con una única variable de estudio:

Variable: Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2022

Definición conceptual: El Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de políticas, procesos, procedimientos, recursos y controles que permiten proteger la confidencialidad, integridad y disponibilidad de la información mediante un proceso sistemático de gestión de riesgos, conforme a los requisitos establecidos en la norma internacional ISO/IEC 27001:2022.

- Dimensiones

Contexto de la organización

Liderazgo

Planificación

Apoyo

Operación

Evaluación del desempeño

Mejora continua

Controles del Anexo A

- Indicadores

Nivel de cumplimiento de los requisitos

Existencia de políticas

Gestión de riesgos

Gestión documental

Gestión de activos

Control de accesos

Gestión de incidentes

Capacitación

Auditorías internas

Mejora continua

- Escala de valoración

0 No cumple

1 Cumplimiento parcial

2 Cumple

Esta escala permitió determinar el grado de cumplimiento de cada requisito evaluado y establecer el nivel de madurez del SGSI de la organización.

3.11 Modalidad de la investigación

La investigación se desarrolló bajo un enfoque mixto, integrando métodos cuantitativos y cualitativos. El componente cuantitativo permitió medir el nivel de cumplimiento de los requisitos de la norma ISO/IEC 27001:2022 mediante listas de verificación y cuestionarios estructurados, mientras que el componente cualitativo facilitó la interpretación de la información obtenida a través de entrevistas y observación directa de los procesos organizacionales.

En ningún momento se manipularon variables ni se realizaron experimentos, por lo que la investigación mantiene un diseño no experimental.

CAPÍTULO 4

4.1 ANTECEDENTES DE LA ORGANIZACIÓN

4.1.1 Descripción General de la Empresa

LEGIO Seguridad es una empresa ecuatoriana especializada en el desarrollo e implementación de soluciones tecnológicas para seguridad física, seguridad electrónica, automatización, control de accesos y transformación digital empresarial. Su propuesta de valor integra tecnologías avanzadas con servicios especializados que permiten fortalecer la protección de personas, activos e información mediante soluciones inteligentes adaptadas a las necesidades de cada organización.

La empresa opera principalmente en Ecuador y extiende sus servicios a Colombia y Chile, atendiendo diversos sectores productivos como industrias, concesionarios automotrices, edificios corporativos, condominios y organizaciones públicas y privadas.

Su portafolio comprende soluciones de:

Control inteligente de accesos.

Videovigilancia.

Automatización.

Desarrollo de software.

Fleet Management.

Sistemas biométricos.

Garitas virtuales.

Gestión tecnológica.

Renting tecnológico.

Leasing tecnológico.

LEGIO combina infraestructura tecnológica, innovación permanente y servicios administrados para ofrecer soluciones orientadas a incrementar la seguridad operacional y optimizar los procesos de negocio de sus clientes. (Legio Seguridad, 2026)

4.1.2 Misión

Proporcionar soluciones tecnológicas avanzadas que fortalezcan la seguridad y eficiencia de nuestros clientes mediante sistemas confiables, innovadores y adaptables, ofreciendo productos y servicios de alta calidad que protejan personas y activos, contribuyendo al crecimiento sostenible de las organizaciones. (Legio Seguridad, 2026)

4.1.3 Visión

Ser líderes en el sector de seguridad tecnológica en América Latina, reconocidos por la innovación y la oferta de soluciones integrales que mejoren la seguridad y la eficiencia operativa de las organizaciones, promoviendo un entorno seguro, confiable y tecnológicamente integrado. (Legio Seguridad, 2026)

4.1.4 Objetivos Organizacionales

Aunque la organización no publica expresamente sus objetivos estratégicos, a partir de su misión, visión y portafolio de servicios pueden identificarse los siguientes objetivos institucionales:

Objetivo General

Proporcionar soluciones integrales de seguridad tecnológica que incrementen la protección física, lógica y operacional de las organizaciones mediante innovación continua y transformación digital.

Objetivos Específicos

Implementar soluciones tecnológicas adaptadas a cada cliente.

Garantizar la continuidad operativa mediante servicios especializados.

Optimizar procesos empresariales utilizando automatización.

Desarrollar software orientado al control y gestión de seguridad.

Fortalecer la seguridad física mediante sistemas inteligentes.

Incrementar la eficiencia operativa de los clientes.

Mantener altos estándares de calidad e innovación tecnológica.

Expandir la presencia regional en Latinoamérica.

4.1.5 Funciones Organizacionales

Las principales funciones de LEGIO comprenden:

Gestión Comercial

Prospectar clientes.

Elaborar propuestas técnicas.

Gestión contractual.

Atención comercial.

Ingeniería

Diseño de soluciones.

Levantamiento de requerimientos.

Arquitectura tecnológica.

Integración de plataformas.

Implementación

Instalación de infraestructura.

Configuración de sistemas.

Puesta en marcha.

Capacitación al cliente.

Operaciones

Monitoreo.
Soporte técnico.
Mantenimiento preventivo.
Gestión de incidencias.
Desarrollo Tecnológico
Desarrollo de software.
Innovación tecnológica.
Integraciones.
Automatización.
Gestión Administrativa
Finanzas.
Talento Humano.
Compras.
Gestión documental.
Cumplimiento legal.

4.1.6 Estructura Organizacional

A partir de la información institucional y del tipo de organización tecnológica, se propone la siguiente estructura funcional.

Gráfico 1. Organigrama Institucional

Nota: Elaboración -Autor.

Fuente: Legio Seguridad

Esta estructura responde al modelo funcional típico de empresas dedicadas al desarrollo e integración de soluciones tecnológicas.

4.1.7 Procesos Institucionales

Siguiendo la clasificación de la ISO 9001:2015 y modelos de gestión empresarial, los procesos de LEGIO pueden organizarse de la siguiente manera.

Gráfico 2. Mapa de procesos

Nota: Elaboración -Autor.

Fuente: Legio Seguridad

4.1.8 Cadena de Valor de LEGIO

Basada en el modelo de Porter adaptado al sector tecnológico, la cadena de valor se detalla en el siguiente diagrama:

Gráfico 3. Cadena de Valor

Nota: Elaboración -Autor.

Fuente: Legio Seguridad

4.1.9 Relación con la Investigación

El presente trabajo de investigación se desarrolla sobre LEGIO debido a que la organización presta servicios especializados en seguridad tecnológica, videovigilancia, control de accesos, biometría, automatización y desarrollo de software, actividades que implican el tratamiento permanente de información personal, datos biométricos y registros de acceso. En este contexto, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la ISO/IEC 27001:2022 constituye un elemento estratégico para fortalecer la confidencialidad, integridad y disponibilidad de la información, mejorar la gestión de riesgos, asegurar el cumplimiento normativo y consolidar la confianza de clientes y partes interesadas.

La evaluación realizada permitirá identificar brechas frente a los requisitos de la norma internacional y proponer un modelo de mejora continua, alineado con los objetivos estratégicos de la organización

Análisis y Discusión de los Resultados

4.2 Análisis Descriptivo de los Resultados

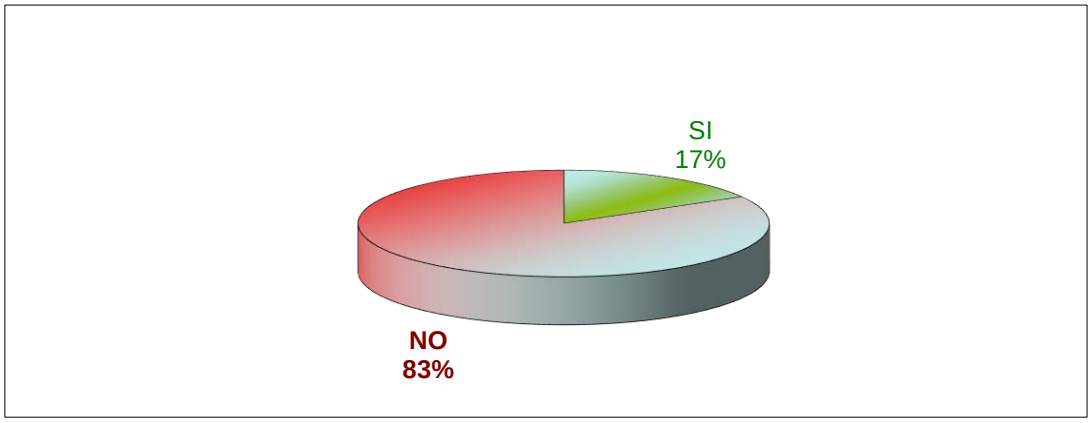
4.2.1 Análisis por Áreas sobre la norma ISO 27001

Tabla 2. Análisis sobre Políticas de Seguridad de la Información

POLÍTICAS DE SEGURIDAD SOBRE ISO 27001		
DETALLE SOBRE PUNTOS DE LA NORMA	**RESPUESTA**	**VALOR**
Existen documento(s) de políticas de seguridad de SI	FALSO	0
Existe normativa relativa a la seguridad de los SI	VERDADERO	1
Existen procedimientos relativos a la seguridad de SI	FALSO	0
Existe un responsable de las políticas, normas y procedimientos	FALSO	0
Existen mecanismos para la comunicación a los usuarios de las normas	FALSO	0
Existen controles regulares para verificar la efectividad de las políticas	FALSO	0
TOTAL		1

Nota: Elaboración -Autor

Gráfica 1. Políticas de Seguridad - Porcentaje por área analizada



Nota: Elaboración -Autor

Hallazgos

A partir de la evaluación realizada, se evidencia una significativa ausencia de alineación de la organización con los requisitos de la norma ISO 27001 en cuanto a políticas de seguridad de la información. Los resultados indican:

Ausencia de documentación: No existen documentos formales que establezcan las políticas de seguridad de la información.

Falta de responsables: No se ha designado un responsable específico para gestionar las políticas, normas y procedimientos de seguridad.

Débiles mecanismos de comunicación: La organización no cuenta con canales efectivos para comunicar las normas de seguridad a los usuarios.

Ausencia de controles: No se realizan verificaciones periódicas para evaluar la efectividad de las políticas implementadas.

Análisis Detallado

Cumplimiento mínimo: El puntaje total obtenido es de 1 punto sobre un posible total de 6, lo que representa un cumplimiento inferior al 17%.

Áreas críticas: Todas las áreas evaluadas, excepto la existencia de normativa relativa a la seguridad de los SI, presentan deficiencias significativas.

Riesgos asociados: La falta de políticas de seguridad sólidas expone a la organización a una amplia gama de riesgos, incluyendo:

Pérdida de datos: Mayor probabilidad de incidentes de seguridad que resulten en la pérdida de información confidencial.

Incumplimiento normativo: Riesgo de sanciones legales y reputacionales por no cumplir con los requisitos de seguridad establecidos.

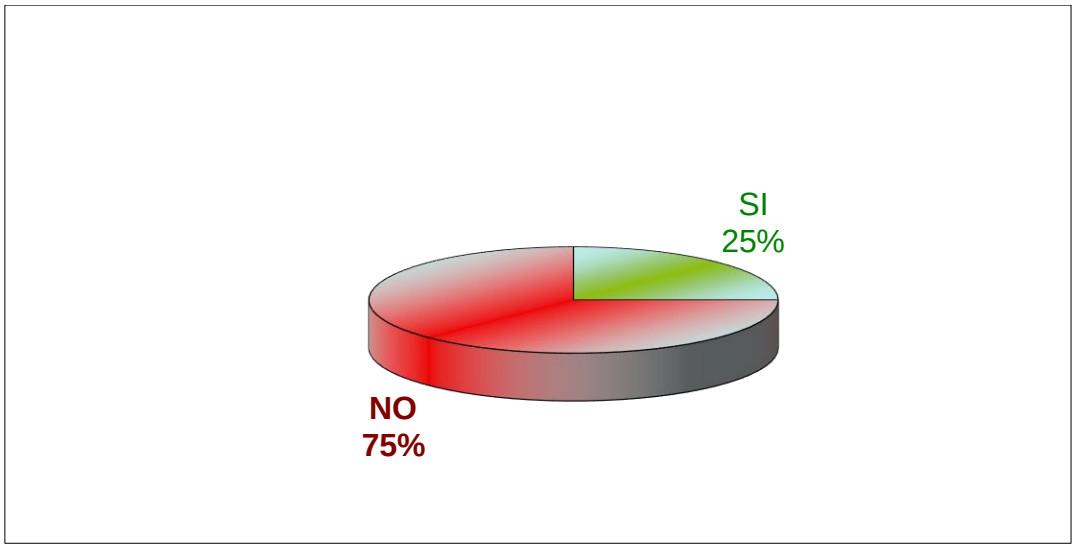
Disminución de la confianza: Pérdida de confianza por parte de clientes y socios comerciales debido a una gestión de seguridad inadecuada.

Tabla 3. Análisis sobre la organización de la seguridad de la información

ORGANIZACIÓN DE LA SEGURIDAD SOBRE ISO 27001		
DETALLE SOBRE PUNTOS DE LA NORMA	**RESPUESTA**	**VALOR**
Existen roles y responsabilidades definidos para las personas implicadas en la seguridad	FALSO	0
Existe un responsable encargado de evaluar la adquisición y cambios de SI	FALSO	0
La Dirección y las áreas de la Organización participa en temas de seguridad	FALSO	0
Existen condiciones contractuales de seguridad con terceros y outsourcing	FALSO	0
Existen criterios de seguridad en el manejo de terceras partes	FALSO	0
La empresa cuenta con programas de formación y capacitación en seguridad dirigidos a empleados, clientes y terceros.	VERDADERO	1
Existe un acuerdo de confidencialidad de la información que se accede	VERDADERO	1
Se revisa la organización de la seguridad periódicamente por una empresa externa	FALSO	0
TOTAL		**2**

Nota: Elaboración -Autor

Gráfica 2. Organización de la Seguridad - Porcentaje por área analizada



Nota: Elaboración -Autor

La evaluación realizada sobre la organización de la seguridad de la información revela una situación preocupante. Aunque se observan algunos aspectos positivos, como la implementación de programas de formación y acuerdos de confidencialidad, la mayoría de los puntos evaluados muestran un incumplimiento significativo con los requisitos de la norma ISO 27001.

Hallazgos

Falta de roles y responsabilidades definidas: No existe una clara asignación de funciones en materia de seguridad de la información, lo que dificulta la gestión y el cumplimiento de las políticas.

Ausencia de evaluación de adquisiciones y cambios: No se realizan evaluaciones de seguridad en el proceso de adquisición o modificación de sistemas de información.

Baja participación de la dirección y áreas: La dirección y las demás áreas de la organización no están suficientemente involucradas en los temas de seguridad.

Débiles controles sobre terceros: No existen mecanismos para garantizar la seguridad de la información cuando se trabaja con terceros o se externalizan servicios.

Ausencia de revisiones externas: La organización no cuenta con evaluaciones periódicas de su sistema de gestión de seguridad por parte de terceros.

Análisis Detallado

Cumplimiento limitado: El puntaje total obtenido es de 2 puntos sobre un posible total de 8, lo que representa un cumplimiento inferior, equivalente al 25%.

Áreas críticas: Todas las áreas evaluadas, excepto los programas de formación y los acuerdos de confidencialidad, presentan deficiencias significativas.

Riesgos asociados: La falta de una organización de seguridad sólida expone a la organización a una amplia gama de riesgos, incluyendo:

Pérdida de control sobre la información: Mayor probabilidad de incidentes de seguridad debido a la falta de roles y responsabilidades claras.

Introducción de vulnerabilidades: Riesgo de introducir vulnerabilidades en los sistemas de información a través de adquisiciones o cambios no evaluados.

Incumplimiento normativo: Riesgo de sanciones legales y reputacionales por no cumplir con los requisitos de seguridad establecidos.

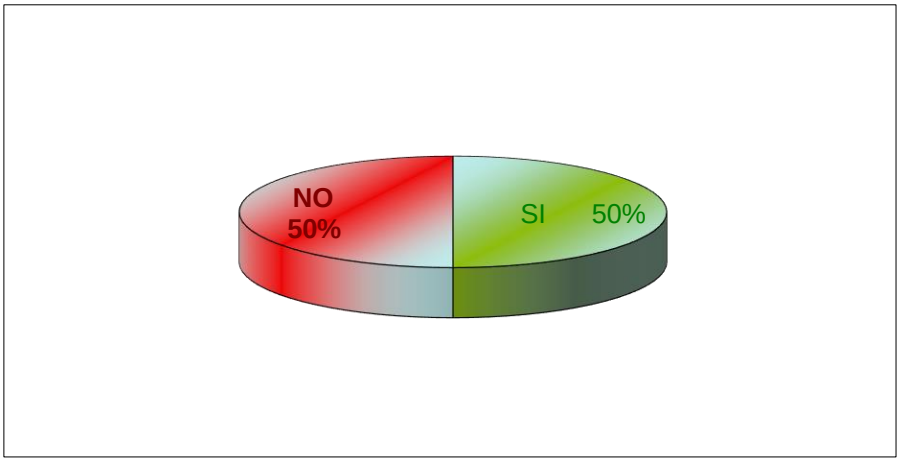
Debilidades en la cadena de suministro: Mayor exposición a riesgos debido a la falta de control sobre terceros.

Tabla 4. Administración de activos- clasificación y control de activos

ADMINISTRACIÓN DE ACTIVOS- CLASIFICACIÓN Y CONTROL DE ACTIVOS SOBRE ISO 27001		
DETALLE SOBRE PUNTOS DE LA NORMA	**RESPUESTA**	**VALOR**
Existen un inventario de activos actualizado	VERDADERO	1
El Inventario contiene activos de datos, software, equipos y servicios	VERDADERO	1
Se dispone de una clasificación de la información según la criticidad de esta	FALSO	0
Existe un responsable de los activos	FALSO	0
Existen procedimientos para clasificar la información	FALSO	0
Existen procedimientos de etiquetado de la información	VERDADERO	1
TOTAL		3

Nota: Elaboración -Autor

Gráfica 3. Administración de activos- clasificación y control de activos Porcentaje por área analizada



Nota: Elaboración -Autor

La evaluación realizada sobre la administración de activos de la información revela una situación mixta. Por un lado, se evidencia un inventario de activos actualizado y la existencia de procedimientos de etiquetado. Sin embargo, se detectaron deficiencias significativas en otros aspectos fundamentales como la clasificación de la información, la asignación de responsabilidades y la definición de procedimientos para la clasificación.

Hallazgos:

Inventario incompleto: Aunque existe un inventario de activos, este no incluye una clasificación detallada de la información según su criticidad.

Falta de responsables: No se ha designado un responsable específico para la gestión de los activos de información.

Ausencia de procedimientos: No existen procedimientos formales para clasificar y etiquetar la información de manera consistente.

Análisis Detallado

Cumplimiento parcial: El puntaje total obtenido es de 3 puntos sobre un posible total de 6, lo que representa un cumplimiento del 50%.

Áreas críticas: La clasificación de la información y la asignación de responsabilidades son las áreas que presentan mayores deficiencias.

Riesgos asociados: La falta de una adecuada administración de activos expone a la organización a los siguientes riesgos:

Pérdida de control sobre la información: Dificultad para identificar y proteger los activos más críticos.

Decisiones de seguridad inadecuadas: Implementación de medidas de seguridad desproporcionadas o insuficientes debido a la falta de clasificación de la información.

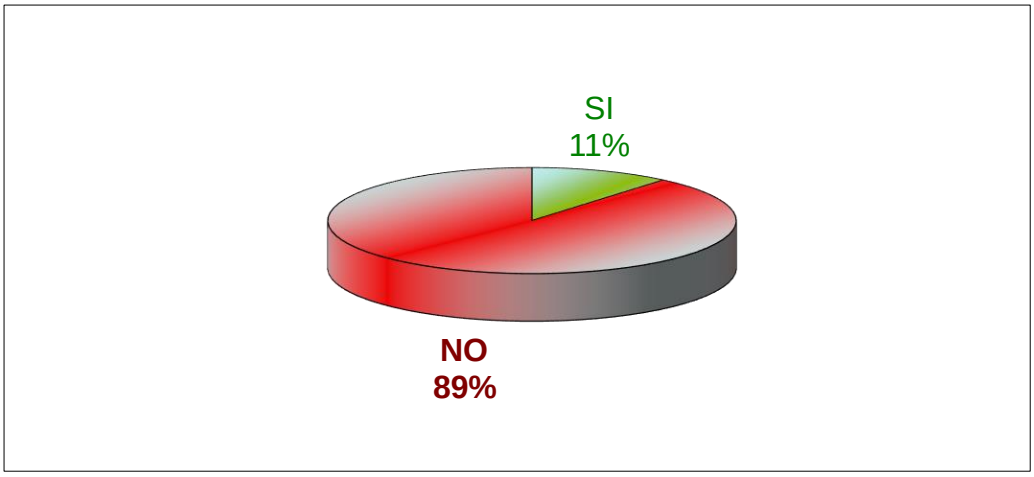
Incumplimiento normativo: Riesgo de sanciones legales y reputacionales por no cumplir con los requisitos de seguridad establecidos.

Tabla 5. Seguridad de los Recursos Humanos sobre ISO 27001

SEGURIDAD DE LOS RECURSOS HUMANOS SOBRE ISO 27001		
DETALLE SOBRE PUNTOS DE LA NORMA	**RESPUESTA**	**VALOR**
Se tienen definidas responsabilidades y roles de seguridad	FALSO	0
Se tiene en cuenta la seguridad en la selección y baja del personal	FALSO	0
Se plasman las condiciones de confidencialidad y responsabilidades en los contratos	VERDADERO	1
El personal recibe la formación necesaria en seguridad y gestión de activos.	FALSO	0
Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad	FALSO	0
Se recogen los datos de los incidentes de forma detallada	FALSO	0
Informan los usuarios de las vulnerabilidades observadas o sospechadas	FALSO	0
Se informa a los usuarios de que no deben, en ninguna circunstancia, probar las vulnerabilidades	FALSO	0
Existe un proceso disciplinario de la seguridad de la información	FALSO	0
TOTAL		1

Nota: Elaboración -Autor

Gráfica 4. Seguridad de la información del personal - Porcentaje por área analizada



Nota: Elaboración -Autor

La evaluación realizada sobre la seguridad de los recursos humanos revela un panorama preocupante. A pesar de que existe un reconocimiento de la importancia de la confidencialidad en los contratos, la mayoría de los puntos evaluados muestran un incumplimiento significativo con los requisitos de la norma ISO 27001.

Hallazgos:

Falta de roles y responsabilidades definidas: No existe una clara asignación de funciones en materia de seguridad de la información para el personal.

Débiles procesos de selección y baja: No se consideran los aspectos de seguridad en los procesos de contratación y despido.

Ausencia de canales de comunicación: No existen mecanismos claros para reportar incidentes de seguridad y vulnerabilidades.

Falta de acciones disciplinarias: No se han establecido procedimientos disciplinarios para abordar las infracciones a las políticas de seguridad.

Análisis Detallado

Cumplimiento mínimo: El puntaje total obtenido es de 1 punto sobre un posible total de 9, lo que representa un cumplimiento inferior al 12%.

Áreas críticas: Todas las áreas evaluadas, excepto el reconocimiento de la confidencialidad en los contratos, presentan deficiencias significativas.

Riesgos asociados: La falta de una gestión adecuada de la seguridad de los recursos humanos expone a la organización a los siguientes riesgos:

Fugas de información: Mayor probabilidad de que los empleados compartan información confidencial de forma accidental o intencional.

Sabotaje: Riesgo de que los empleados descontentos o malintencionados causen daños a los sistemas de información.

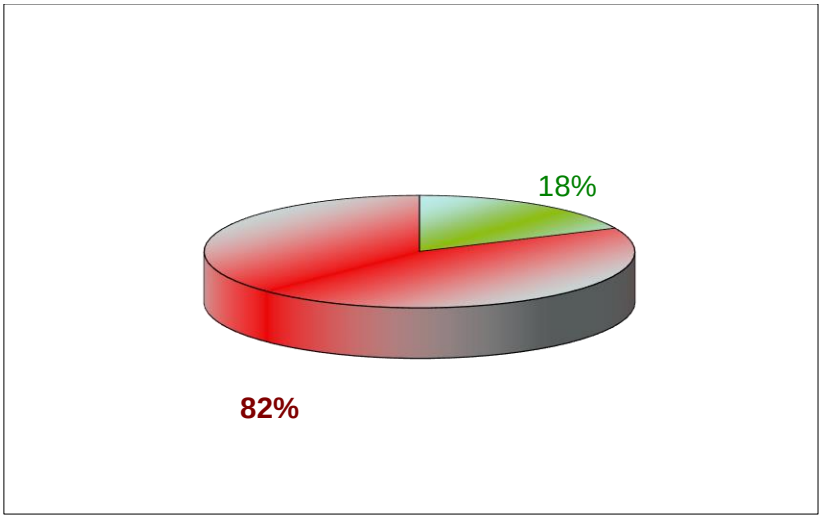
Errores humanos: Mayor probabilidad de errores humanos que puedan comprometer la seguridad de la información.

Tabla 6. Seguridad física y del ambiente sobre la información

SEGURIDAD FÍSICA Y DEL AMBIENTE SOBRE ISO 27001		
DETALLE SOBRE PUNTOS DE LA NORMA	**RESPUESTA**	**VALOR**
Existe perímetro de seguridad física (una pared, puerta con llave).	VERDADERO	1
Existen controles de entrada para protegerse frente al acceso de personal no autorizado	VERDADERO	1
El área segura está cerrada, aislada y protegida de eventos naturales	FALSO	0
En las áreas seguras existen controles adicionales al personal propio y ajeno	FALSO	0
Las áreas de carga y expedición están aisladas de las áreas de SI	FALSO	0
La ubicación de los equipos está de tal manera para minimizar accesos innecesarios.	FALSO	0
Existen protecciones frente a fallos en la alimentación eléctrica	FALSO	0
Existe seguridad en el cableado frente a daños e intercepciones	FALSO	0
Se asegura la disponibilidad e integridad de todos los equipos	FALSO	0
Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente	FALSO	0
Se incluye la seguridad en equipos móviles	FALSO	0
TOTAL		**2**

Nota: Elaboración -Autor

Gráfica 5. - Porcentaje por área analizada Porcentaje por área analizada



Nota: Elaboración -Autor

La evaluación realizada sobre la seguridad física y del ambiente revela un cumplimiento menor con los requisitos de la norma ISO 27001. Si bien existen algunas medidas básicas de seguridad, como un perímetro físico y controles de acceso, se identificaron múltiples deficiencias en áreas clave como la protección de áreas seguras, la gestión de riesgos ambientales y la seguridad de los equipos.

Hallazgos:

Falta de protección en áreas seguras: Las áreas donde se almacena información sensible no cuentan con las medidas de seguridad adecuadas.

Débiles controles en áreas de carga y expedición: No existe una separación clara entre las áreas de carga y expedición y las áreas donde se maneja información sensible.

Ubicación inadecuada de equipos: La ubicación de los equipos no minimiza el acceso no autorizado.

Vulnerabilidades en la infraestructura: No existen protecciones suficientes contra fallos en la alimentación eléctrica, daños en el cableado y otros riesgos físicos.

Falta de seguridad para equipos móviles: Los dispositivos móviles no están protegidos de forma adecuada.

Análisis Detallado

Cumplimiento limitado: El puntaje total obtenido es de 2 puntos sobre un posible total de 11, lo que representa un cumplimiento inferior al 19%.

Áreas críticas: La mayoría de las áreas evaluadas presentan deficiencias significativas, lo que indica una necesidad urgente de mejorar las medidas de seguridad física y ambiental.

Riesgos asociados: La falta de una seguridad física adecuada expone a la organización a los siguientes riesgos:

Acceso no autorizado: Mayor probabilidad de que personas no autorizadas accedan a la información sensible.

Pérdida o daño de equipos: Riesgo de pérdida o daño de equipos debido a desastres naturales, incendios, inundaciones o sabotaje.

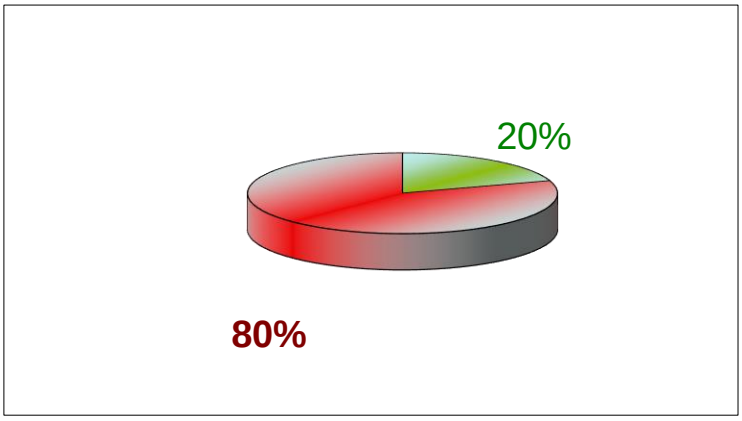
Interrupción de los servicios: Mayor probabilidad de interrupciones en los servicios debido a fallos en la infraestructura.

Tabla 7. Gestión de comunicaciones y operaciones

GESTIÓN DE COMUNICACIONES Y OPERACIONES SOBRE ISO 27001		
DETALLE SOBRE PUNTOS DE LA NORMA	**RESPUESTA**	**VALOR**
Todos los procedimientos operativos identificados en la política de seguridad están documentados	FALSO	0
Están establecidas responsabilidades para controlar los cambios en equipos	FALSO	0
Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad	FALSO	0
Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas	VERDADERO	1
Existe una separación de los entornos de desarrollo y producción	FALSO	0
Existen contratistas externos para la gestión de los Sistemas de Información	FALSO	0
Existe un Plan de Capacidad para garantizar los recursos necesarios de procesamiento y almacenamiento.	FALSO	0
Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones	FALSO	0
Existen controles contra software maligno	VERDADERO	1
Se realizan copias o respaldos de backup de la información esencial para el negocio	VERDADERO	1
Existen registros para las actividades realizadas por los operadores y administradores	FALSO	0
Existen registros de los fallos detectados	FALSO	0
Existen rastro de auditoría	FALSO	0
Existe algún control en las redes	FALSO	0
Están establecidos controles para realizar la gestión de los medios informáticos. (cintas, discos, removibles, informes impresos)	FALSO	0
Los medios informáticos deben eliminarse de forma segura, dado que pueden contener información sensible.	FALSO	0
Existe seguridad de la documentación de los Sistemas	FALSO	0
Existen acuerdos para intercambio de información y software	FALSO	0
Existen medidas de seguridad de los medios en el tránsito	FALSO	0
Existen medidas de seguridad en el comercio electrónico.	FALSO	0
Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada	FALSO	0
Existen medidas de seguridad en las transacciones en linea	VERDADERO	1
Se monitorean las actividades relacionadas a la seguridad	FALSO	0
TOTAL		4

Nota: Elaboración -Autor

Gráfica 6. Gestión de comunicaciones y operaciones sobre ISO 27001



Nota: Elaboración -Autor

La evaluación realizada sobre la gestión de comunicaciones y operaciones revela un cumplimiento muy bajo con los requisitos de la norma ISO 27001. A pesar de que se han implementado algunas medidas básicas de seguridad, como controles contra software maligno, copias de seguridad y seguridad en transacciones en línea, la mayoría de los puntos evaluados muestran deficiencias significativas.

Hallazgos:

Falta de documentación: No existe una documentación completa de los procedimientos operativos y de los cambios en los sistemas.

Ausencia de gestión de incidentes: No se han establecido procedimientos claros para responder a incidentes de seguridad.

Débiles controles de acceso: No existe una separación clara entre los entornos de desarrollo y producción, ni controles adecuados para limitar el acceso a los sistemas.

Falta de gestión de cambios: No se siguen procesos formales para la gestión de cambios en los sistemas.

Vulnerabilidades en la infraestructura: No existen controles adecuados para proteger la red, los equipos y los datos.

Débil gestión de medios: No se han establecido procedimientos para la gestión segura de los medios informáticos.

Análisis Detallado

Cumplimiento muy bajo: El puntaje total obtenido es de 4 puntos sobre un posible total de 21, lo que representa un cumplimiento inferior al 20%.

Áreas críticas: La mayoría de las áreas evaluadas presentan deficiencias significativas, lo que indica una necesidad urgente de mejorar la gestión de comunicaciones y operaciones.

Riesgos asociados: La falta de una gestión adecuada de las comunicaciones y operaciones expone a la organización a los siguientes riesgos:

Pérdida de datos: Mayor probabilidad de pérdida de datos debido a fallos en los sistemas, ataques cibernéticos o errores humanos.

Interrupción de los servicios: Mayor probabilidad de interrupciones en los servicios debido a fallos en la infraestructura o ataques cibernéticos.

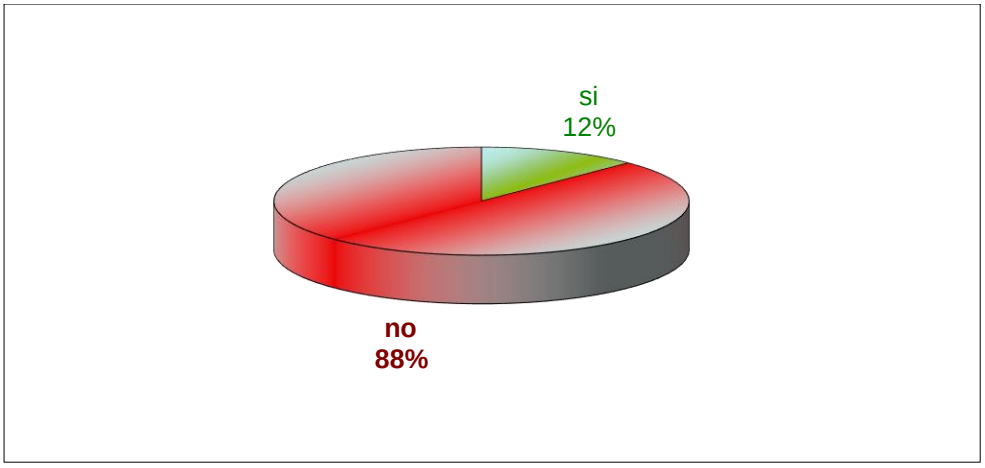
Incumplimiento normativo: Riesgo de sanciones legales y reputacionales por no cumplir con los requisitos de seguridad establecidos

Tabla 8. Control de accesos de información

CONTROL DE ACCESOS (ISO 27001)		
DETALLE SOBRE PUNTOS DE LA NORMA	**RESPUESTA**	**VALOR**
Existe una política de control de accesos	FALSO	0
Existe un procedimiento formal de registro y baja de accesos	FALSO	0
Se controla y restringe la asignación y uso de privilegios en entornos multiusuario	FALSO	0
Existe una gestión de los password de usuarios	FALSO	0
Existe una revisión de los derechos de acceso de los usuarios	FALSO	0
Existe el uso del password	FALSO	0
Se protege el acceso de los equipos desatendidos	FALSO	0
Existen políticas de limpieza en el puesto de trabajo	VERDADERO	1
Existe una política de uso de los servicios de red	FALSO	0
Se asegura la ruta (path) desde el terminal al servicio	FALSO	0
Existe una autenticación de usuarios en conexiones externas	FALSO	0
Existe una autenticación de los nodos	FALSO	0
Existe un control de la conexión de redes	FALSO	0
Existe un control del routing de las redes	FALSO	0
Existe una identificación única de usuario y una automática de terminales	FALSO	0
Existen procedimientos de log-on al terminal	FALSO	0
Se ha incorporado medidas de seguridad a la Tecnología móvil	FALSO	0
Está controlado el teletrabajo por la organización	VERDADERO	1
TOTAL		2

Nota: Elaboración -Autor

Gráfica 7. Control de acceso a la información



Nota: Elaboración -Autor

La evaluación realizada sobre el control de accesos revela un cumplimiento muy bajo con los requisitos de la norma ISO 27001. A pesar de que existen algunas políticas básicas de limpieza en el puesto de trabajo y control del teletrabajo, la mayoría de los puntos evaluados muestran deficiencias significativas.

Hallazgos:

Falta de políticas y procedimientos: No existen políticas formales para el control de accesos, la gestión de contraseñas, la revisión de privilegios y otros aspectos críticos.

Débiles controles de acceso: No se han implementado medidas adecuadas para controlar el acceso a los sistemas y datos, como la autenticación de usuarios, la protección de equipos desatendidos y la gestión de redes.

Ausencia de gestión de identidades: No existe una gestión adecuada de las identidades de los usuarios, incluyendo la creación, modificación y eliminación de cuentas.

Análisis Detallado

Cumplimiento muy bajo: El puntaje total obtenido es de 2 puntos sobre un posible total de 18, lo que representa un cumplimiento inferior al 11%.

Áreas críticas: La mayoría de las áreas evaluadas presentan deficiencias significativas, lo que indica una necesidad urgente de mejorar los controles de acceso.

Riesgos asociados: La falta de un control de acceso adecuado expone a la organización a los siguientes riesgos:

Acceso no autorizado: Mayor probabilidad de que personas no autorizadas accedan a los sistemas y datos.

Pérdida o modificación de datos: Riesgo de pérdida o modificación de datos debido a acciones de usuarios no autorizados.

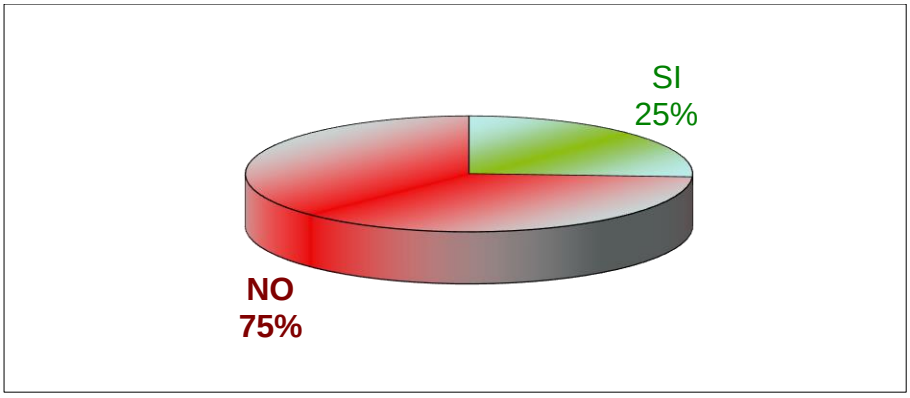
Incumplimiento normativo: Riesgo de sanciones legales y reputacionales por no cumplir con los requisitos de seguridad establecidos.

Tabla 9. Desarrollo y Mantenimiento de los Sistemas

DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS		
DETALLE SOBRE PUNTOS DE LA NORMA	**RESPUESTA**	**VALOR**
Se asegura que la seguridad está implantada en los Sistemas de Información	FALSO	0
Existe seguridad en las aplicaciones	VERDADERO	1
Existen controles criptográficos.	FALSO	0
Existe seguridad en los ficheros de los sistemas	FALSO	0
Existe seguridad en los procesos de desarrollo, testing y soporte	VERDADERO	1
Existen controles de seguridad para los resultados de los sistemas	FALSO	0
Existe la gestión de los cambios en los SO.	FALSO	0
Se controlan las vulnerabilidades de los equipos	FALSO	0
TOTAL		2

Nota: Elaboración -Autor

Gráfica 8. Porcentaje Desarrollo y Mantenimiento de los Sistemas



Nota: Elaboración -Autor

A partir de la evaluación realizada y los datos proporcionados, se observa que el estado actual del desarrollo y mantenimiento de los sistemas presenta algunas deficiencias significativas en cuanto a la seguridad de la información.

Hallazgos

Seguridad en las aplicaciones: Se ha identificado la existencia de controles de seguridad en las aplicaciones, lo cual es un aspecto positivo.

Seguridad en los procesos de desarrollo, testing y soporte: La presencia de controles de seguridad en estas etapas del ciclo de vida del software indica un cierto nivel de conciencia sobre la importancia de la seguridad desde el inicio del desarrollo.

Falta de implantación generalizada de la seguridad: El resultado global de la evaluación indica que la seguridad no está completamente integrada en los sistemas de información.

Ausencia de controles criptográficos: La falta de controles criptográficos es una debilidad importante, ya que estos son fundamentales para proteger la confidencialidad e integridad de la información.

Vulnerabilidades en ficheros, sistemas operativos y resultados de los sistemas: La evaluación revela la existencia de varias vulnerabilidades en componentes clave de los sistemas, lo que los hace susceptibles a ataques.

Falta de gestión de cambios y control de vulnerabilidades: La ausencia de procesos para gestionar los cambios en los sistemas operativos y controlar las vulnerabilidades de los equipos aumenta el riesgo de incidentes de seguridad.

Análisis detallado

El puntaje total obtenido en esta área es de 2 verdaderas sobre un posible total (el total máximo posible no se especifica en la consulta). Este bajo puntaje confirma la necesidad de implementar medidas correctivas para mejorar la seguridad de los sistemas.

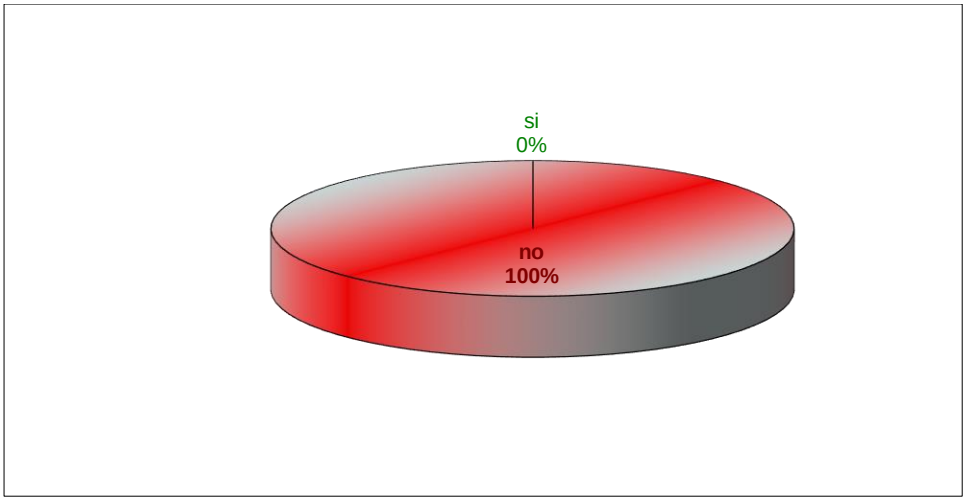
Los resultados de la evaluación indican que la organización debe realizar una revisión exhaustiva de sus prácticas de desarrollo y mantenimiento de sistemas para garantizar el cumplimiento de los requisitos de la norma ISO 2700.

Tabla 10. Administración de incidentes seguridad de la información ISO 27001

ADMINISTRACIÓN DE INCIDENTES SEGURIDAD DE LA INFORMACIO ISO 27001		
DETALLE SOBRE PUNTOS DE LA NORMA	RESPUESTA	VALOR
Se comunican los eventos de seguridad	FALSO	0
Se comunican las debilidades de seguridad	FALSO	0
Existe definidas las responsabilidades antes un incidente.	FALSO	0
Existe un procedimiento formal de respuesta	FALSO	0
Existe la gestión de incidentes	FALSO	0
TOTAL		0

Nota: Elaboración -Autor

Gráfica 9. Administración de incidentes seguridad de la información ISO 27001



Nota: Elaboración -Autor

Seguridad implantada: La ausencia de seguridad generalizada indica una falta de enfoque integral en la protección de los sistemas.

Controles criptográficos: La falta de estos controles expone los datos a riesgos como la interceptación y la alteración.

Seguridad en ficheros y sistemas: La ausencia de medidas de seguridad en estos elementos fundamentales aumenta la vulnerabilidad ante ataques.

Resultados de los sistemas: La falta de controles específicos para los resultados de los sistemas puede llevar a la exposición de información confidencial.

Gestión de cambios y vulnerabilidades: La ausencia de estos procesos incrementa el riesgo de introducir vulnerabilidades y dificulta la detección de las existentes.

Análisis detallado

Riesgo elevado de incidentes: La combinación de estos factores aumenta significativamente el riesgo de sufrir incidentes de seguridad, como brechas de datos, ataques cibernéticos y pérdida de información confidencial.

Incumplimiento normativo: La falta de cumplimiento de la norma ISO 27001 puede exponer a la organización a sanciones legales y reputacionales.

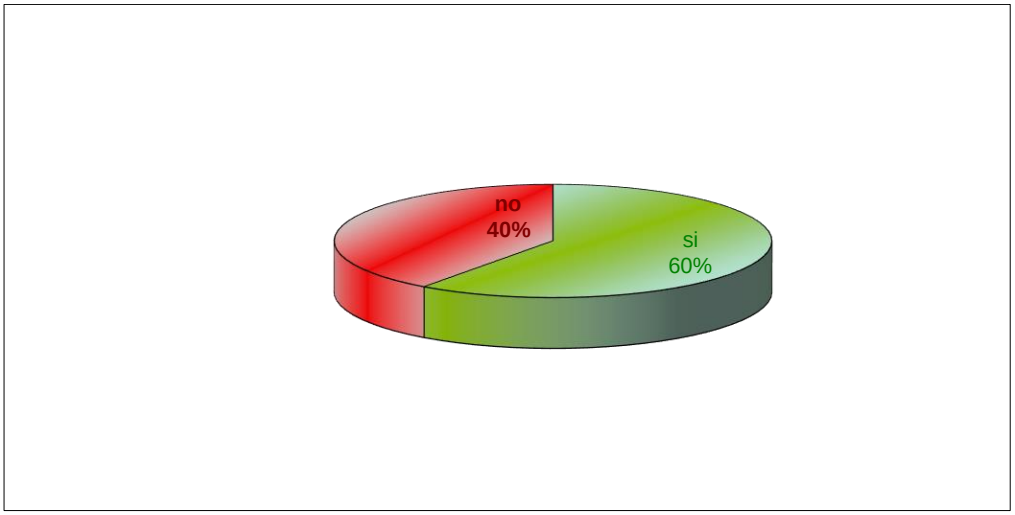
Pérdida de confianza: Los clientes y socios comerciales pueden perder confianza en la organización si se producen incidentes de seguridad.

Tabla 11. Gestión de la continuidad del negocio ISO 27001

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
DETALLE SOBRE PUNTOS DE LA NORMA	**RESPUESTA**	**VALOR**
Existen procesos para la gestión de la continuidad.	VERDADERO	1
Existe un plan de continuidad del negocio y análisis de impacto	FALSO	0
Existe un diseño, redacción e implantación de planes de continuidad	FALSO	0
Existe un marco de planificación para la continuidad del negocio	VERDADERO	1
Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio.	VERDADERO	1
TOTAL		3

Nota: Elaboración -Autor

Gráfica 10. Gestión de la continuidad del negocio



Nota: Elaboración -Autor

A partir de la evaluación realizada, se observa que la organización ha implementado algunos aspectos relacionados con la gestión de la continuidad del negocio, pero aún existen áreas de mejora significativas.

Hallazgos

Existencia de procesos: Se han establecido procesos para la gestión de la continuidad, lo que indica un primer paso hacia la implementación de un plan de continuidad.

Marco de planificación: a organización cuenta con un marco formal de planificación para la continuidad del negocio que establece los lineamientos, responsabilidades y procesos necesarios para garantizar su gestión adecuada. lo cual es fundamental para establecer las bases de un plan efectivo.

Pruebas y mantenimiento: Se realizan pruebas y mantenimiento de los planes de continuidad, lo que garantiza que estos estén actualizados y sean efectivos.

Falta de plan y análisis de impacto La ausencia de un plan de continuidad del negocio puede afectar la capacidad de la organización para responder y recuperarse ante interrupciones operativas.

Falta de diseño, redacción e implementación: La falta de estos elementos indica que los planes de continuidad no están completamente desarrollados ni puestos en práctica.

Análisis detallado.

El puntaje total obtenido en esta área es de 3 verdaderas sobre un posible total (el total máximo posible no se especifica en la consulta). Si bien este puntaje indica que se han tomado algunas medidas, la ausencia de un plan formal y un análisis de impacto detallado son deficiencias importantes que deben ser abordadas.

Implicaciones de los resultados:

Vulnerabilidad ante interrupciones: La falta de un plan de continuidad del negocio bien definido expone a la organización a un mayor riesgo de sufrir interrupciones en sus operaciones y de experimentar pérdidas financieras y de reputación.

Dificultad para responder a incidentes: En caso de producirse un incidente, la organización no estará preparada para responder de manera rápida y efectiva, lo que puede prolongar la duración de la interrupción y aumentar los daños.

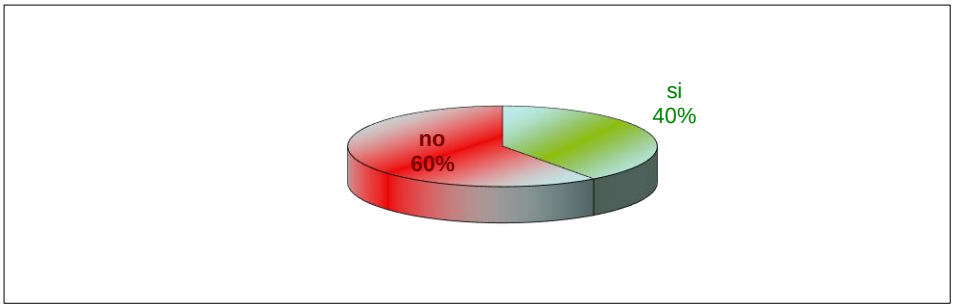
Tabla 12. Cumplimiento sobre la norma ISO 27001

CUMPLIMIENTO SOBRE LA NORMA ISO 27001

DETALLE SOBRE PUNTOS DE LA NORMA	RESPUESTA	VALOR
Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas	VERDADERO	1
Existe el resguardo de la propiedad intelectual	FALSO	0
Existe el resguardo de los registros de la organización	VERDADERO	1
Existe una revisión de la política de seguridad y de la conformidad técnica	FALSO	0
Existen consideraciones sobre las auditorías de los sistemas	FALSO	0
TOTAL		2

Nota: Elaboración -Autor

Gráfica 11. Cumplimiento sobre la norma ISO 27001



Nota: Elaboración -Autor

El análisis de los datos proporcionados revela que la organización ha cumplido con algunos aspectos relacionados con el cumplimiento normativo, pero aún existen áreas significativas de mejora.

Hallazgos

Cumplimiento con la legislación: La organización ha demostrado un compromiso con el cumplimiento de las leyes y regulaciones aplicables a sus sistemas.

Resguardo de los registros: Se evidencia un esfuerzo por proteger la integridad y confidencialidad de los registros de la organización.

Propiedad intelectual: La falta de medidas para proteger la propiedad intelectual expone a la organización a riesgos de piratería y competencia desleal.

Revisión de políticas y conformidad técnica: La ausencia de revisiones periódicas de las políticas de seguridad y de la conformidad técnica indica una falta de proactividad en la gestión de riesgos.

Auditorías de sistemas: La falta de consideraciones sobre las auditorías de sistemas limita la capacidad de la organización para identificar y corregir vulnerabilidades.

Implicaciones de los resultados

Riesgos legales: La falta de cumplimiento normativo en todas las áreas puede exponer a la organización a sanciones legales y multas.

Pérdida de reputación: La violación de derechos de propiedad intelectual o la filtración de información confidencial puede dañar la reputación de la organización.

Vulnerabilidades: La falta de revisiones periódicas y auditorías puede llevar a la identificación tardía de vulnerabilidades en los sistemas.

4.3 Conclusión del Análisis de los Resultados de la Gestión en Calidad (ISO 27001)

El cuadro presentado muestra un diagnóstico inicial de la implementación de un sistema de gestión del sistema de seguridad basado en la norma ISO 27001. Los resultados obtenidos indican un nivel de cumplimiento general bajo, con áreas que requieren una mejora significativa.

La organización ha iniciado un camino importante hacia la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001. Sin embargo, aún queda mucho por hacer para alcanzar un nivel de madurez adecuado.

Capítulo 5

Marco Propositivo

Antecedentes

Vulnerabilidades identificadas y justificación del marco propositivo

Como resultado del diagnóstico institucional desarrollado en el Capítulo IV, se identificaron diversas vulnerabilidades relacionadas con la gestión de la seguridad de la información. Si bien la organización cuenta con una sólida infraestructura tecnológica, soluciones avanzadas de seguridad electrónica y procesos operativos orientados a la prestación de servicios, el análisis evidenció oportunidades de mejora respecto al cumplimiento de los requisitos establecidos en la ISO/IEC 27001:2022.

Las principales brechas se relacionan con aspectos de gobernanza, gestión documental, administración de riesgos, formalización de políticas y procedimientos, asignación de responsabilidades, monitoreo de controles y fortalecimiento de la cultura organizacional en materia de seguridad de la información. Estas vulnerabilidades incrementan la probabilidad de que se materialicen riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional.

En este contexto, la creación del marco propositivo constituye la respuesta técnica a las vulnerabilidades identificadas durante la investigación, ya que plantea un conjunto de políticas, procedimientos, controles, metodologías y mecanismos de mejora continua orientados a cerrar las brechas detectadas y facilitar la implementación progresiva de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con los requisitos de la ISO/IEC 27001:2022. De esta manera, la propuesta no solo busca corregir las debilidades actuales, sino también fortalecer la capacidad institucional para gestionar los riesgos de forma sistemática, asegurar

el cumplimiento normativo y consolidar una cultura organizacional basada en la seguridad de la información.

Vulnerabilidades generales identificadas durante el diagnóstico

Tabla 13 Vulnerabilidades detectadas

Área evaluada	Vulnerabilidad identificada	Riesgo asociado	Nivel de impacto
Gobernanza	Ausencia de un SGSI formalmente implementado	Falta de dirección estratégica en seguridad de la información	Alto
Gestión documental	Políticas y procedimientos de seguridad incompletos o no estandarizados	Aplicación inconsistente de controles	Alto
Gestión de riesgos	Metodología de evaluación y tratamiento de riesgos no formalizada	Materialización de amenazas sin tratamiento adecuado	Alto
Gestión de activos	Inventario de activos de información susceptible de fortalecimiento	Pérdida de trazabilidad y control de activos críticos	Medio
Control de accesos	Roles y privilegios con oportunidades de mejora en su revisión periódica	Accesos no autorizados a información sensible	Alto
Continuidad del negocio	Procedimientos de continuidad y recuperación con margen de fortalecimiento	Interrupción prolongada de los servicios	Alto
Gestión de incidentes	Proceso de notificación, análisis y respuesta a incidentes parcialmente documentado	Respuesta tardía ante incidentes de seguridad	Alto
Gestión de proveedores	Controles de seguridad para terceros no completamente formalizados	Riesgos derivados de proveedores y contratistas	Medio
Concienciación del personal	Capacitación periódica en seguridad de la información limitada	Error humano y aumento de incidentes	Medio
Cumplimiento normativo	Evidencia documental de cumplimiento con ISO/IEC 27001:2022 en proceso de consolidación	Observaciones en auditorías y riesgos regulatorios	Alto
Monitoreo y mejora	Indicadores y métricas de desempeño del SGSI no definidos	Dificultad para evaluar la eficacia de los controles	Medio
Protección de la información	Clasificación y tratamiento de la información con oportunidades de estandarización	Divulgación o uso inadecuado de información crítica	Alto

Nota: Elaboración -Autor a partir del diagnóstico institucional realizado en el Capítulo 4

Las vulnerabilidades descritas constituyen un diagnóstico general que fundamenta el diseño del marco propositivo presentado en el siguiente capítulo. Cada una de ellas será abordada mediante controles, políticas, procedimientos y mecanismos de mejora alineados con los dominios y controles de la ISO/IEC 27001:2022, con el propósito de fortalecer la madurez del Sistema de Gestión de Seguridad de la Información de LEGIO Seguridad.

Manual de implementación de ISO 27001

El presente manual tiene como objetivo proporcionar una guía práctica para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a los requisitos de la norma ISO/IEC 27001.

Este manual está dirigido a la empresa Legio Seguridad Legsegu Cia. Ltda, misma que busca proteger sus activos de información, minimizar los riesgos de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información, bajo el triángulo de la seguridad de la información, pilar fundamental de la parte técnica, que apoya a la parte administrativa y de gestión para el respectivo cumplimiento legal.

Principios Fundamentales

Confidencialidad: Asegurar que la información solo está disponible para personas autorizadas.

Integridad: Salvaguardar la exactitud y completitud de la información y sus métodos de procesamiento.

Disponibilidad: Garantizar que la información esté accesible cuando sea necesaria.

Buenas Prácticas

1. Establecimiento del Alcance del SGSI

Identificar los límites y el alcance del sistema considerando los activos, procesos, ubicaciones y partes interesadas.

Documentar el alcance en función de los objetivos de negocio y los requisitos legales.

2. Liderazgo y Compromiso

Asegurar el apoyo de la alta dirección.

Designar un responsable del SGSI (e.g., un Oficial de Seguridad de la Información).

Establecer una política de seguridad de la información alineada con los objetivos estratégicos.

3. Análisis de Riesgos

Identificación de Activos: Crear un inventario de activos y clasificar la información.

Evaluación de Amenazas y Vulnerabilidades: Identificar posibles amenazas y vulnerabilidades asociadas.

Evaluación de Impacto: Determinar el impacto potencial de la materialización de los riesgos.

Tratamiento de Riesgos: Definir controles adecuados para mitigar, transferir, aceptar o evitar los riesgos.

4. Controles de Seguridad

Los controles deben implementarse según el Anexo A de la norma ISO 27001:

Políticas de Seguridad: Establecer y comunicar políticas claras.

Organización de la Seguridad de la Información: Definir roles y responsabilidades.

Seguridad de los Recursos Humanos: Realizar verificaciones previas a la contratación y formación continua.

Gestión de Activos: Etiquetar y proteger los activos según su importancia.

Control de Acceso: Aplicar principios como el de menor privilegio.

Cifrado: Proteger la información sensible mediante técnicas de cifrado.

Gestión de Incidentes: Establecer un proceso para la detección, respuesta y aprendizaje de incidentes.

5. Formación y Concienciación

Implementar programas de capacitación periódicos para todos los empleados.

Fomentar una cultura de seguridad en todos los niveles de la organización.

6. Monitoreo y Auditoría

Realizar auditorías internas periódicas para evaluar la efectividad del SGSI.

Supervisar los indicadores clave de rendimiento (KPIs) relacionados con la seguridad de la información.

7. Mejora Continua

Aplicar el ciclo PDCA (Planificar, Hacer, Verificar, Actuar) para garantizar la mejora continua del SGSI, el ciclo PHVA (también conocido como PDCA, por sus siglas en inglés: Plan-Do-Check-Act) es una herramienta fundamental en los sistemas de gestión de la calidad. Este ciclo ayuda a las organizaciones a mejorar continuamente sus procesos, productos o servicios.

1. Planificar (P - Plan)

Definimos los objetivos que queremos alcanzar.

Identificamos los problemas o áreas de mejora.

Analizamos los recursos necesarios y establecemos un plan para resolverlos.

Ejemplo: La empresa Legio Seguridad Legsegu Cia. Ltda detecta que hay muchas quejas por problemas de seguridad de la información; en esta fase, se analiza el problema, se identifica la causa (equipos sin licencias de seguridad) y se diseña un plan para configurarlos

2. Hacer (H - Do)

Puesta en marcha lo que se planificó.

Se implementan los cambios o mejoras de manera controlada (por ejemplo, en una pequeña parte del proceso como puede ser las licencias de antivirus en computadoras, para probar).

Ejemplo: La empresa Legio Seguridad Legsegu Cia. Ltda configura los equipos con su respectiva licencia de antivirus y analiza las computadoras que dispone de antivirus frente a las que no lo tienen para verificar si el problema se reduce.

Lo propio se puede hacer con los diferentes elementos que componen una red segura como son:

Tabla 14. Elementos de una Red Segura

Categoría	Elemento de Ciberseguridad	Descripción
Protección de la red	Firewall	Filtra y monitorea el tráfico de red entrante y saliente para bloquear actividades no autorizadas.
	Segmentación de red	Divide la red en secciones para minimizar el impacto de ataques en áreas críticas.
	Sistemas de detección y prevención de intrusos (IDS/IPS)	Detectan y previenen accesos no autorizados y actividades maliciosas.
Protección de endpoints	Antivirus y antimalware	Detectan y eliminan software malicioso en dispositivos como computadoras y servidores.
	Gestión de dispositivos móviles (MDM)	Controla y asegura dispositivos móviles utilizados en la red corporativa.
Seguridad de datos	Cifrado de datos	Protege la información tanto en tránsito como en reposo, haciéndola ilegible para usuarios no autorizados.
	Respaldo y recuperación	Realiza copias de seguridad periódicas y garantiza planes de recuperación ante desastres para evitar pérdida de datos.

	Prevención de pérdida de datos (DLP)	Monitorea y controla la transferencia de datos sensibles para evitar fugas o accesos no autorizados.
Gestión de accesos	Autenticación multifactor (MFA)	Añade capas de seguridad a los procesos de inicio de sesión para evitar accesos no autorizados.
	Control de acceso basado en roles (RBAC)	Permite acceso a datos y sistemas solo a los usuarios con permisos específicos.
	Gestión de identidades (IAM)	Administra y protege la identidad digital de usuarios, asegurando accesos autorizados.
Gestión de riesgos	Evaluación de vulnerabilidades	Identifica y mitiga puntos débiles en los sistemas antes de que sean explotados.
	Pruebas de penetración (pentesting)	Simulan ataques reales para evaluar la efectividad de las medidas de seguridad.
	Plan de respuesta a incidentes	Define procedimientos claros para mitigar daños y restaurar operaciones tras un ataque.
Monitoreo y auditoría	Sistemas de monitoreo continuo	Detectan anomalías en tiempo real en el tráfico de red, sistemas y aplicaciones.
	Auditorías de seguridad	Revisiones regulares de políticas y controles para garantizar el cumplimiento de normas y la efectividad de medidas.
Capacitación y cultura	Concienciación en ciberseguridad	Entrena a los empleados sobre buenas prácticas y prevención de amenazas como phishing y ataques de ingeniería social.
	Simulaciones de ataques	Realiza pruebas como correos de phishing simulados para medir la preparación de los empleados.
Cumplimiento normativo	Adherencia a estándares	Cumple con normativas y estándares relevantes como ISO 27001, GDPR, CCPA, entre otros.

	Políticas de seguridad de la información	Define reglas internas para gestionar y proteger los datos sensibles y las operaciones críticas.
Infraestructura segura	Gestión de parches y actualizaciones	Garantiza que sistemas, aplicaciones y hardware estén actualizados para corregir vulnerabilidades conocidas.
	Endurecimiento de sistemas	Configura sistemas y servidores eliminando configuraciones por defecto que puedan ser explotadas.
Seguridad en la nube	Configuración segura de la nube	Asegura que los servicios en la nube tengan configuraciones adecuadas para proteger datos y operaciones.
	Seguridad de aplicaciones SaaS	Implementa medidas para proteger aplicaciones en la nube utilizadas por la empresa, como autenticación robusta y monitoreo.

Nota. Elaboración autor.

3. Verificar (V - Check)

Revisión de los resultados obtenidos y los comparamos con los objetivos que habíamos establecido.

Análisis sobre las acciones implementadas y su funcionamiento

Ejemplo: Legio Seguridad Legsegu Cia. Ltda. revisa los equipos de prueba que contienen antivirus y se observa que la reducción de riesgo sobre la seguridad de la información en un margen superior al 70% que resulta un indicador aceptable y susceptible de mejora constituyéndose en una solución efectiva.

4. Actuar (A - Act)

Si los resultados fueron buenos, estandarizamos las mejoras para aplicarlas en toda la organización.

Si no se alcanzaron los objetivos, volvemos al paso de Planificar y ajustamos el enfoque.

Ejemplo: En Legio Seguridad Legsegu Cia. Ltda. Después de confirmar que recalibrar las máquinas resuelve el problema, se aplican los cambios a todas las máquinas de la fábrica.

Revisar y actualizar el SGSI periódicamente para adaptarse a nuevos riesgos y cambios organizacionales.

Documentación Requerida

Política de Seguridad de la Información

Tabla 15. Propuesta para desarrollo de Política de Seguridad de la Información

POLITICA DE SEGURIDAD DE LA INFORMACION	
Sección	Contenido
Nombre de la Organización	[Legio Seguridad Legsegu Cia. Ltda]
Propósito	Definir el compromiso de la organización con la protección de la información y el cumplimiento de la norma ISO 27001.
Alcance	Aplicable a todos los sistemas, procesos y personas que interactúan con la información de [Nombre de la Organización].
Declaración de la Política	1. Proteger la confidencialidad, integridad y disponibilidad de la información.2. Cumplir con todas las leyes, regulaciones y requisitos contractuales aplicables.3. Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la mejora continua.4. Realizar evaluaciones regulares de riesgos y tratarlos adecuadamente. 5. Capacitar al personal en prácticas seguras.
Aprobado por:	[Nombre y firma del Director General]
Fecha de Aprobación:	[Fecha]

Nota. Elaboración autor

Análisis de Riesgos y Plan de Tratamiento de Riesgos

Tabla 16. Propuesta de matriz de análisis y tratamiento de riesgos

ID del Riesgo	Descripción	Activo Impactado	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Nivel de Riesgo	Categoría del Riesgo
R01	Acceso no autorizado a la red interna	Servidores	Hackeo	Configuración débil	Alto	Media	Alto	Confidencialidad, Integridad
R02	Pérdida de datos por falla del sistema	Base de datos de clientes	Falla del sistema	Falta de respaldo	Alto	Baja	Medio	Confidencialidad, Disponibilidad

R03	Daño físico a equipos	Servidores, equipos de red	Desastre natural, sabotaje	Falta de protección física	Medio	Baja	Bajo	Disponibilidad

Nota. Elaboración autor

Inventario de Activos

Tabla 17. Propuesta de matriz de inventario de activos

ID del Activo	Nombre del Activo	Tipo	Propietario	Ubicación	Valoración de Importancia	Medidas de Protección	Información Sensible Almacenada	Clasificación de la Información
A001	Servidor Principal	Hardware	Equipo de TI	Centro de Datos	Alta	Firewall, Copias de Seguridad	Datos de clientes, información financiera	Confidencial
A002	Laptop del Director	Hardware	Director General	Oficina	Alta	Encriptación, contraseña fuerte	Información estratégica, datos de proyectos	Confidencial
A003	Base de Datos de Clientes	Software	Departamento de Marketing	Servidor Principal	Alta	Copias de Seguridad, acceso restringido	Datos personales de clientes	Confidencial
A004	Código Fuente del Software Principal	Software	Equipo de Desarrollo	Repositorio Git	Alta	Control de versiones, acceso restringido	Propiedad intelectual	Confidencial

Nota. Elaboración autor - Planes de Continuidad de Negocio

Tabla 18. Propuesta de matriz de seguimiento de continuidad de negocio ante incidentes de SI

Proceso Crítico	Impacto en caso de interrupción	Tiempo de Recuperación Objetivo (RTO)	Tiempo Máximo Permitido (RPO)	Responsable	Procedimientos de Recuperación	Pruebas de Recuperación
Procesamiento de datos	Pérdida de ingresos, insatisfacción del cliente	4 horas	24 horas	Equipo de TI	Notificar a [Equipo de Respuesta], activar respaldo en [Ubicación Alterna], validar la restauración de los servicios	Semestral
Atención al cliente	Pérdida de clientes, reputación dañada	2 horas	12 horas	Equipo de Atención al Cliente	Redirigir llamadas a un centro de llamadas externo, habilitar un sistema de tickets en línea	Trimestral

Nota: Elaboración Autor

Registros de Incidentes de Seguridad

Tabla 19. Propuesta de Registro de incidentes

ID del Incidente	Fecha	Descripción	Impacto (Confidencialidad, Integridad, Disponibilidad)	Sistema Afectado	Causa Raíz	Acciones Tomadas	Responsable	Estado	Fecha de Cierre	Lecciones Aprendidas
INC001	[Fecha]	Acceso no autorizado detectado	Confidencialidad	Servidor de correo	Contraseña débil	Bloqueo de IP, refuerzo de contraseñas, cambio de contraseña forzado	Equipo de TI	Resuelto	[Fecha]	Implementar política de contraseñas más robusta
INC002	[Fecha]	Pérdida de un dispositivo móvil	Confidencialidad, Disponibilidad	Dispositivo del empleado X	Extravío	Bloqueo remoto del dispositivo,	Equipo de TI	Resuelto	[Fecha]	Implementar un sistema de localización

					notificación a los empleados				para dispositivos móviles

Nota: Elaboración Autor

Resultados de Auditorías

Tabla 20. Propuesta de resultados de auditorías sobre seguridad de la información

ID del Hallazgo	Descripción	Nivel de Riesgo (Alto/Medio/Bajo)	Causa Raíz	Recomendaciones	Responsable	Fecha Límite	Estado	Fecha de Cierre	Evidencia de Cierre
H01	Contraseñas débiles detectadas	Alto	Falta de políticas claras	Implementar contraseñas fuertes, capacitación a usuarios	Equipo de TI	[Fecha]	En Progreso		Política de contraseñas actualizada
H02	Falta de documentación de procesos críticos	Medio	Falta de estandarización	Documentar todos los procesos críticos	Departamento de Calidad	[Fecha]	Planificado		Documentación de procesos actualizada

Nota: Elaboración Autor

Conclusión

El cumplimiento de ISO 27001 en Legio Seguridad Legsegu Cia. Ltda requiere un compromiso constante por parte de toda la organización. Esta propuesta de manual es una herramienta esencial para establecer una base sólida de seguridad de la información, garantizando la protección de los activos críticos y la confianza de las partes interesadas.

Capítulo 6

Conclusiones

Situación actual de los sistemas de gestión

Como resultado del diagnóstico institucional realizado, se determinó que **LEGIO Seguridad LEGSEGU Cía. Ltda. no cuenta actualmente con un Sistema de Gestión de Seguridad de la Información (SGSI) implementado y certificado conforme a la norma ISO/IEC 27001:2022**, ni con un marco documental que integre de manera formal las políticas, procedimientos, controles y mecanismos de seguimiento requeridos por este estándar internacional. Si bien la organización dispone de procesos operativos y soluciones tecnológicas orientadas a la seguridad de sus clientes, estos no se encuentran estructurados bajo un sistema de gestión alineado con los requisitos de la norma. En consecuencia, la **propuesta desarrollada en esta investigación surge como respuesta a esta necesidad**, planteando el diseño de un SGSI que permita fortalecer la gestión de riesgos, proteger los activos de información, mejorar el cumplimiento normativo y establecer un modelo de mejora continua acorde con las mejores prácticas internacionales.

La creación de un manual de gestión de seguridad de la información bajo la norma ISO 27001 permite estructurar un enfoque integral para garantizar la confidencialidad, integridad y disponibilidad de la información en la empresa Legsegu Cia Ltda. Este esfuerzo no solo fortalece la protección de los datos, sino que también asegura el cumplimiento de estándares internacionales, aumentando la confianza de clientes y partes interesadas.

Levantamiento y análisis de información: Este paso inicial permitió identificar el estado actual de la empresa en términos de seguridad de la información. El diagnóstico evidenció las brechas existentes, sirviendo como base para diseñar estrategias efectivas de mejora.

Plantilla de diagnóstico general: La plantilla basada en ISO 27001 facilitó una evaluación uniforme y detallada, proporcionando una herramienta práctica y replicable para identificar vulnerabilidades y oportunidades de mejora.

Elaboración del manual: La creación del manual de buenas prácticas y procedimientos aseguró la implementación de controles específicos adaptados a las necesidades de Legsegu Cia Ltda, alineados con los requisitos de la norma ISO 27001, promoviendo una cultura organizacional orientada a la seguridad de la información

Recomendaciones

Implementación y Mantenimiento del SGSI (Sistema de Gestión de Seguridad de la Información): Asegurar que el manual propuesto sea implementado y mantenido de manera continua, actualizándolo ante cambios en el entorno organizacional o tecnológico.

Capacitación del Personal: Realizar sesiones de capacitación y sensibilización para todos los niveles de la organización. Es fundamental que los empleados de Legio Seguridad Legsegu Cia. Ltda comprendan su rol en la protección de la información y el cumplimiento de las políticas establecidas.

Monitoreo y Mejora Continua: Establecer métricas de desempeño y auditorías periódicas para evaluar la eficacia de las políticas y procedimientos definidos. Aplicar mejoras en función de los resultados obtenidos y las lecciones aprendidas.

Gestión de Riesgos: Implementar un proceso sistemático de identificación, análisis, evaluación y tratamiento de riesgos relacionados con la seguridad de la información. Priorizar los controles para abordar las amenazas críticas detectadas.

Integración con Otros Sistemas de Gestión: Si la empresa tiene implementados otros estándares, como ISO 9001 (gestión de calidad) o ISO 22301 (gestión de continuidad de negocio), buscar sinergias entre los sistemas para optimizar recursos y fortalecer la gestión organizacional.

Compromiso de la Alta Dirección: Asegurar el apoyo continuo de la alta dirección para garantizar los recursos necesarios y promover una cultura organizacional que valore la seguridad de la información como un pilar estratégico.

Estas acciones permitirán a Legsegu Cia Ltda no solo cumplir con los requisitos de ISO 27001, sino también posicionarse como una organización confiable en el manejo de información.

Bibliografía

Alulema Lara, D. O. (06 de 06 de 2021). Norma ISO 37001 en el Sistema de Gestión Innovador de Antisoborno en el Registro Civil, identificación, cedulación y servicios electrónicos de la provincia de Tungurahua. *Tesis*. Ambato, Tungurahua , Ecuador : Repositorio unidad de Posgrados UTA. Obtenido de https://repositorio.uta.edu.ec/items/648bdb4c-eb47-4263-8b50-ac54d658d8d7

ANI Agencia Nacional de Infraestructura . (2022). *Maual Antisobornos ANI* . Bogota , Bogota , Colombia . Obtenido de https://www.ani.gov.co/sites/default/files/sig/tpsc-m-003_manual_antisoborno_ani_v2.pdf

Arellano Veloz, C. E. (2023). Modelo de gestión de la seguridad de la información en una institución financiera cooperativa. *Modelo de gestión de la seguridad de la información en una institución financiera cooperativa*. Pontificia Universidad Católica del Ecuador. Repositorio Institucional PUCE. Obtenido de https://repositorio.puce.edu.ec/items/33ccc110-78e3-4b72-a3ac-924d5bfcb414?utm_

Asamblea Constituyente del Ecuador. (2008). Constitución de la República del Ecuador. Registro Oficial N.º 449, 20 de octubre de 2008. *Constitución de la República del Ecuador. Registro Oficial N.º 449, 20 de octubre de 2008.* Obtenido de https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial, Quinto Suplemento N.º 459, 26 de mayo de 2021. *Ley Orgánica de Protección de Datos Personales. Registro Oficial, Quinto Suplemento N.º 459, 26 de mayo de 2021.* Obtenido de https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/14649-suplemento-al-registro-oficial-no-459

Ashqui, C. R. (20 de 04 de 2023). IDENTIFICACIÓN DE GRABADOS Y MARCAS SERIALES EN EL. *Tesis*. Riobamba, Chimborazo, Ecuador: Repositorio UNACH. Obtenido de http://dspace.unach.edu.ec/bitstream/51000/11299/1/Colcha%20Ashqui%2c%20C%20%282023%29Identificaci%c3%b3n%20de%20grabados%20y%20marcas%20seriales%20en%20el%20robo%20de%20veh%c3%adculos%20en%20la%20ciudad%20de%20Riobamba.%20.%28Tesis%20de%20Pregrado%29Univ

Chávez Cabrera, R. L. (2022). Desarrollo del programa del sistema de gestión de seguridad de la información para una empresa de cobranzas. *Desarrollo del programa del sistema de gestión de seguridad de la información para una empresa de cobranzas*. Repositorio Institucional UDLA. Obtenido de https://dspace.udla.edu.ec/handle/33000/14467?

Compliance 360. (12 de 09 de 2024). Implementación y Certificación ISO 37001. Lima, LIma , Perú. Obtenido de https://compliance360.pe/2023/08/28/implementacion-y-certificacion-iso-37001/

Contador Minaya, J. R. (2023). Diseño e implementación de la ISO 27001 para mejorar la seguridad de información de la Empresa Minera Colibrí S.A.C., Lima – 2023. *Diseño e implementación de la ISO 27001 para mejorar la seguridad de información de la Empresa Minera Colibrí S.A.C., Lima – 2023*. Repositorio Institucional UNJFSC. Obtenido de https://repositorio.unjfsc.edu.pe/handle/20.500.14067/8975?utm_source

International Organization for Standardization (ISO), & International Electrotechnical Commission (IEC). (2022). ISO/IEC 27000:2022 Information security, cybersecurity and privacy protection — Information security management systems — Overview and vocabulary. ISO. *ISO/IEC 27000:2022 Information security, cybersecurity and privacy protection — Information security management systems — Overview and vocabulary. ISO.* Obtenido de https://www.iso.org/standard/73906.html

International Organization for Standardization (ISO), & International Electrotechnical Commission (IEC). (2022). SO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO. *SO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.* Obtenido de https://www.iso.org/standard/27001

ISO37001. (01 de 01 de 2016). ISO 37001 Sistema de Gestión Antisoborno. *standard ISO*. Berna, Berna, Suiza: Standard ISO. Obtenido de https://www.iso.org/obp/ui#iso:std:iso:37001:ed-1:v1:es

Kohl. (2024). *Compliance, Anti-bribery, and Corporate Social Responsibility. In: Managing SMEs in Times of Rapid Change.* (Springer, Ed.) New York, New York , Estados Unidos : Future of Business and Finance. Obtenido de https://doi.org/10.1007/978-3-031-71272-2_7

Legio Seguridad. (07 de 07 de 2026). *legio.ec*. Obtenido de legio.ec: https://legio.ec/quienes-somos/

Lizarzaburu, E. R. (2019). *Gestión empresarial: una revisión ala norma IOS 37001 antisoborno.* Caracas , Caracas , Venezuela : Cetro de investigación CLAD. Obtenido de https://clad.org/wp-content/uploads/2021/04/073-04-LBBNC.pdf

Mera Amores, I. F. (2022). Propuesta de gestión de la seguridad de la información basado en la norma ISO 27001. Caso de estudio: empresa ALTAC. *Propuesta de gestión de la seguridad de la información basado en la norma ISO 27001. Caso de estudio: empresa ALTAC*. Repositorio Institucional PUCE. Obtenido de https://repositorio.puce.edu.ec/items/3ac14304-ef60-4eeb-a4e1-0b4a0dd1aa8c?utm

MInisterio de Economía y Finanzas . (2022). *Pymes e ISO 37001* . Quito , Pichincha , Ecuador : Ministerio de Economía Finanzas Ecuador . Obtenido de https://www.finanzas.gob.ec/wp-content/uploads/downloads/2019/08/ISO_37001_2016.pdf

Nieto Guano, J. F. (25 de 10 de 2021). Propuesta de diseño de un sistema de gestión antisoborno bajo la Norma Internacional ISO 37001:2016 Sistemas de Gestión Antisoborno Caso: Cuerpo de Bomberos del Distrito Metropolitano de Quito. *Tesis*. Quito, Pichincha, Ecuador: UASB Digital. Obtenido de https://repositorio.uasb.edu.ec/bitstream/10644/8352/1/T3647-MGCI-Nieto-Propuesta.pdf

Pardo Cuenca, M. G. (2015). Modelo de gestión de seguridad de la información para la Universidad Nacional de Loja basado en la norma ISO/IEC 27001. *Modelo de gestión de seguridad de la información para la Universidad Nacional de Loja basado en la norma ISO/IEC 27001*. Repositorio Institucional de la Universidad Nacional de Loja. Obtenido de https://dspace.unl.edu.ec/items/bd5468ba-655c-4b0c-ae9e-e6278c98b0d5?utm_

Parlamento Europeo & Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Prot. *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Prot*. Diario Oficial de la Unión Europea, L119, 1–88. Obtenido de https://eur-lex.europa.eu/eli/reg/2016/679/oj

Perez, M. $. (2019). *Reputation enhancement throutg ISO 37001certification.* New York .

Pineda Vergara, R. E. (10 de 02 de 2022). Análisis del Sistema de Gestión Antisoborno ISO 37001, como. *Tesis*. Lima, Lima, Perú: Repositorio Universidad cesar Vallejo. Obtenido de https://repositorio.ucv.edu.pe/handle/20.500.12692/82185

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. The TQM Journal, 33(7), 76–105.

Hernandez Collante, L., Pranolo, A., & Prasetya Wibawa, A. (2024). Implementation plan of the information security management system based on the NTC-ISO-IEC 27001:2013 standard and security risk analysis: Case study: Higher education institution. Transactions on Energy Systems and Engineering Applications, 5(2), 1–20. https://doi.org/10.32397/tesea.vol5.n2.635

(2022). The performance implications of ISO/IEC 27001. Journal name unknown, Source: ScienceDirect.

ResearchGate. (2019). Information Safety Process Development According to ISO 27001 for…. Procedia title unspecified.

ResearchGate. (2023). Enhancing Information Security Management in Small and Medium Enterprises (SMEs) Through ISO 27001 Compliance.

(n.d.). Diffusion and Adoption of Information Security Management Standards Across Countries and Industries. In Academia.edu – includes ISO 27001 diffusion data.

ResearchGate. (2021). Impact of ISO 27001 and Concealment on Performance.

Susanto, H., Almunawar, M. N., & Chee Tuan, Y. (2012). A novel method on ISO 27001 reviews: ISMS compliance readiness level measurement.

Mataracıoğlu, T., & Özkan, S. (2011, August 10). Governing information security in conjunction with COBIT and ISO 27001.

Ristov, S., Gusev, M., & Kostoska, M. (2012, April 5). Cloud computing security in business information systems.

ANEXO 1

Checklist de Verificación de Ciberseguridad

Este checklist está diseñado para ayudarte a evaluar y fortalecer la postura de ciberseguridad de una organización.

1. Políticas y Procedimientos

- ¿Existen políticas de seguridad de la información actualizadas?
- ¿Están definidas políticas de contraseñas seguras y su renovación periódica?
- ¿Se implementan principios de acceso basado en el menor privilegio?
- ¿Se cuenta con un plan de respuesta a incidentes documentado?
- ¿Existen acuerdos de confidencialidad y políticas de uso aceptable para empleados?

2. Protección de Datos

- ¿Se realiza cifrado de datos sensibles en tránsito y en reposo?
- ¿Se llevan a cabo respaldos regulares de datos críticos?
- ¿Están los respaldos protegidos y accesibles solo a personal autorizado?
- ¿Se implementan controles de prevención de pérdida de datos (DLP)?
- ¿Los datos sensibles están clasificados según su criticidad?

3. Control de Accesos

- ¿Está habilitada la autenticación multifactor (MFA) para sistemas críticos?
- ¿Se revisan y actualizan periódicamente los permisos de acceso?
- ¿Se revocan accesos de manera inmediata tras la salida de un empleado?
- ¿Se utiliza una solución de gestión de identidades y accesos (IAM)?
- ¿Las cuentas administrativas están protegidas y restringidas?

4. Protección de Infraestructura y Red

- ¿Se utilizan firewalls configurados correctamente para proteger la red?
- ¿Se cuenta con sistemas IDS/IPS para detectar y prevenir intrusiones?
- ¿Está segmentada la red para separar sistemas críticos?
- ¿Se implementa filtrado web y bloqueo de sitios maliciosos?
- ¿Los puntos de acceso Wi-Fi están protegidos con WPA3 o equivalente?

5. Protección de Endpoints

- ¿Todos los dispositivos tienen software antivirus y antimalware actualizado?
- ¿Se utilizan herramientas de gestión de dispositivos móviles (MDM)?
- ¿Se aplica el endurecimiento de sistemas en servidores y estaciones de trabajo?

- ¿Los parches y actualizaciones de software se aplican regularmente?
- ¿Los dispositivos USB y periféricos externos están controlados?

6. Monitoreo y Respuesta

- ¿Se implementa monitoreo continuo del tráfico de red y sistemas?
- ¿Se generan alertas ante actividades sospechosas o anómalas?
- ¿Se realizan pruebas regulares de penetración y evaluaciones de vulnerabilidades?
- ¿Se realiza análisis de registros y auditorías de seguridad periódicas?
- ¿Existen sistemas SIEM (Gestión de Información y Eventos de Seguridad)?

7. Capacitación y Concienciación

- ¿Se capacita regularmente a los empleados en ciberseguridad?
- ¿Se realizan simulacros de phishing para evaluar la preparación del personal?
- ¿Los empleados saben cómo identificar y reportar actividades sospechosas?
- ¿Se fomenta una cultura organizacional de seguridad de la información?

8. Cumplimiento Normativo

- ¿La organización cumple con normativas y estándares relevantes (ISO 27001, GDPR, PCI DSS, etc.)?
- ¿Se mantienen registros de auditorías y evidencias de cumplimiento?
- ¿Se evalúan y actualizan las políticas según cambios regulatorios?

9. Seguridad en la Nube

- ¿Las configuraciones de servicios en la nube siguen las mejores prácticas de seguridad?
- ¿Se monitorean las actividades en la nube para detectar accesos no autorizados?
- ¿Se realiza cifrado de datos en servicios de almacenamiento en la nube?
- ¿Se utilizan herramientas CASB (Cloud Access Security Broker)?

10. Gestión de Terceros

- ¿Se evalúan los riesgos de seguridad en proveedores y terceros?
- ¿Existen contratos que incluyan cláusulas de seguridad y cumplimiento?
- ¿Se monitorean los accesos otorgados a terceros a los sistemas de la empresa?
- ¿Se realizan auditorías de seguridad a proveedores críticos?

ANEXO 2

Checklist de Verificación de Seguridad de la Información

Este check list abarca los elementos clave que una organización debe revisar para garantizar la protección de su información y la continuidad de sus operaciones.

1. Políticas y Gobernanza

- ¿Existe una política de seguridad de la información aprobada y actualizada?
- ¿Se han definido roles y responsabilidades en materia de seguridad de la información?
- ¿La alta dirección apoya y supervisa las iniciativas de seguridad?
- ¿Se realizan revisiones periódicas de las políticas de seguridad?
- ¿Existen sanciones documentadas para violaciones a las políticas?

2. Gestión de Activos

- ¿Se cuenta con un inventario actualizado de activos de información (hardware, software, datos)?
- ¿Están clasificados los activos según su importancia y sensibilidad?
- ¿Existen controles para proteger los activos más críticos?
- ¿Se realiza un seguimiento de la propiedad y el uso de los activos?
- 3. Control de Acceso
- ¿Se utilizan contraseñas seguras y políticas de autenticación robustas?
- ¿Está implementada la autenticación multifactor (MFA) para accesos críticos?
- ¿Se aplica el principio de privilegio mínimo para los accesos?
- ¿Se revocan inmediatamente los accesos de empleados y contratistas al finalizar su relación laboral?
- ¿Se auditan regularmente los permisos y roles asignados?

4. Seguridad Física y Ambiental

- ¿Están las áreas donde se almacenan datos críticos protegidas físicamente?
- ¿Se controlan los accesos físicos mediante tarjetas, cerraduras o biometría?
- ¿Existen medidas de protección contra incendios, inundaciones y otros desastres?
- ¿Se supervisan las áreas sensibles mediante cámaras y registros de acceso?
- ¿Se han establecido controles para dispositivos personales (BYOD)?

5. Gestión de Riesgos

- ¿Se realiza un análisis de riesgos periódicamente para identificar amenazas y vulnerabilidades?
- ¿Se documentan y gestionan los riesgos identificados?
- ¿Existen planes de mitigación para riesgos críticos?
- ¿Se han definido indicadores clave de riesgo (KRI)?
- 6. Seguridad Operativa
- ¿Se aplican parches y actualizaciones regularmente a sistemas y software?
- ¿Existen controles para evitar la instalación de software no autorizado?
- ¿Se monitorean las actividades en los sistemas para detectar accesos no autorizados o comportamientos anómalos?
- ¿Se implementan políticas de gestión segura de medios de almacenamiento (USB, discos externos)?

7. Protección de Datos

- ¿Se cifran los datos sensibles en tránsito y en reposo?
- ¿Se realizan copias de seguridad periódicas y se prueban los procedimientos de recuperación?
- ¿Existen controles para la eliminación segura de datos obsoletos?
- ¿Se aplican controles para prevenir la pérdida de datos (DLP)?
- 8. Gestión de Incidentes
- ¿Se cuenta con un plan de respuesta a incidentes formal y probado?
- ¿Están definidos los procedimientos para detectar, reportar y contener incidentes?
- ¿Se realizan simulacros de incidentes para evaluar la preparación?
- ¿Se documentan y analizan los incidentes para evitar recurrencias?

9. Cumplimiento Normativo

- ¿Se cumplen las normativas aplicables (GDPR, ISO 27001- LOPDP)?
- ¿Existen registros documentados de cumplimiento normativo?
- ¿Se realizan auditorías regulares para verificar el cumplimiento?

10. Capacitación y Concienciación

- ¿Se capacita regularmente al personal en temas de seguridad de la información?
- ¿Existen programas de concienciación sobre amenazas como phishing, ransomware y ingeniería social?
- ¿Se evalúa la efectividad de las capacitaciones mediante pruebas o simulaciones?

11. Seguridad de Proveedores y Terceros

- ¿Se evalúan los riesgos asociados a proveedores y terceros?
- ¿Se incluyen cláusulas de seguridad en los contratos con terceros?
- ¿Se auditan regularmente los servicios de proveedores críticos?
- ¿Se limita el acceso de terceros a los sistemas y datos de la organización?

12. Mejora Continua

- ¿Se revisan y actualizan regularmente los controles de seguridad?
- ¿Se realiza una evaluación posterior a incidentes para identificar lecciones aprendidas?
- ¿Se incorporan nuevas tecnologías y mejores prácticas a medida que evolucionan las amenazas?
- Este check list puede usarse como guía para auditorías internas o externas y para desarrollar un plan de acción en materia de seguridad de la información.