UNIVERSIDAD HISPANOAMERICANA

ESCUELA DE INFORMÁTICA

GRADO DE LICENCIATURA

TITULO:

Desarrollar una propuesta de Implementación de Mejoras en Seguridad de la Información Alineado a ISO 27001:27002 para la Mitigación de Riesgos en la Empresa SISLOCAR Caldera, para julio 2025.

SUSTENTANTE:

IGNACIO JOSUÉ CRUZ CHAVES

Tutor:

Marco Vinicio Soto Monge

Julio, 2025.

Contenido

Índice de Figuras

Índice de Gráficos

Índice de Tablas

DECLARACIÓN JURADA

DECLARACIÓN JURADA

Yo Ignacio Josué Cruz Chaves, mayor de edad, portador de la cédula de identidad número 6-0467-0316 egresado de la carrera de Ingeniería Informática de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Licenciatura en Ingeniería Informática juro solemnemente que mi trabajo de investigación titulado: Desarrollar una propuesta de Implementación de Mejoras en Seguridad de la Información Alineado a ISO 27001 27002, para la Mitigación de Riesgos en la empresa SISOCAR Caldera, Julio 2025 es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público.

En fe de lo anterior, firmo en la ciudad de San José, a los catorce días del mes de agosto del año dos mil veinticinco.

Ignacio Cruz Ch.
Firma del estudiante
Cédula: 604670316

CARTAS DE APROBACIÓN DEL TUTOR

CARTA DEL TUTOR

San José, 14 de Agosto de 2025

Esteban Gonzalez Vargas
Director
Ingeniería Informática
Universidad Hispanoamericana
Sede Llorente

Estimada señora:

El estudiante **IGNACIO JOSUÉ CRUZ CHAVES**, cédula de identidad número **604670316**, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado **"Desarrollar una propuesta de Implementación de Mejoras en Seguridad de la Información Alineado a ISO 27001:27002 para la Mitigación de Riesgos en la Empresa SISLOCAR Caldera, para julio 2025.",** el cual ha elaborado para optar por el grado académico de **Licenciatura** en Ingeniería Informática.

En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

a) Original del tema	10%	10%
b) Cumplimiento de entrega de avances	20%	5%
c) Coherencia entre los objetivos, los instrumentos aplicados y los resultados de la investigación	30%	25%
d) Relevancia de las conclusiones y recomendaciones	20%	20%
e) Calidad, detalle del marco teórico	20%	20%
TOTAL		**80%**

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente, MARCO VINICIO SOTO MONGE (FIRMA)
Firmado digitalmente por MARCO VINICIO SOTO MONGE (FIRMA)
Fecha: 2025.08.14 20:23:27 -06'00'

Marco Vinicio Soto Monge

Cédula 110360428

CARTA DE APROBACIÓN DEL LECTOR

CARTA DE LECTOR

San José,

Universidad Hispanoamericana
Sede Llorente
Carrera de Informática

Estimado señor

El estudiante Ignacio Josué Cruz Chaves, cédula de identidad 604670316, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado "Desarrollar una propuesta de Implementación de Mejoras en Seguridad de la Información Alineado a ISO 27001:27002 para la Mitigación de Riesgos en la Empresa SISLOCAR Caldera, para julio 2025".

He revisado y he hecho las observaciones relativas al contenido analizado, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.

Atte.

Randall Vargas Villalobos

Firmado digitalmente por Randall Vargas Villalobos
Fecha: 2025.09.15 11:15:52 -06'00'

Firma
Randall Vargas Villalobos
Cédula: 1-1140-0113

CARTA DE AUTORIZACIÓN DEL CENIT

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

Abangares, Guanacaste, 01 de octubre de 2025

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito Ignacio Josué Cruz Chaves con número de identificación 6-0467-0316 autor del trabajo de graduación titulado "Desarrollar una propuesta de Implementación de Mejoras en Seguridad de la Información Alineado a ISO 27001:27002 para la Mitigación de Riesgos en la Empresa SISLOCAR Caldera, para julio 2025" presentado y aprobado en el año 2025 como requisito para optar por el título de Licenciatura en Ingeniería Informática; Sí autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,

Ignacio Cruz Ch. 604670316

Firma y Documento de Identidad

ANEXO 1 (Versión en línea dentro del Repositorio)
LICENCIA Y AUTORIZACIÓN DE LOS AUTORES PARA PUBLICAR Y PERMITIR LA CONSULTA Y USO

Parte 1. Términos de la licencia general para publicación de obras en el repositorio institucional

Como titular del derecho de autor, confiero al Centro de Información Tecnológico (CENIT) una licencia no exclusiva, limitada y gratuita sobre la obra que se integrará en el Repositorio Institucional, que se ajusta a las siguientes características:

a) Estará vigente a partir de la fecha de inclusión en el repositorio, el autor podrá dar por terminada la licencia solicitándolo a la Universidad por escrito.

b) Autoriza al Centro de Información Tecnológico (CENIT) a publicar la obra en digital, los usuarios puedan consultar el contenido de su Trabajo Final de Graduación en la página Web de la Biblioteca Digital de la Universidad Hispanoamericana

c) Los autores aceptan que la autorización se hace a título gratuito, por lo tanto, renuncian a recibir beneficio alguno por la publicación, distribución, comunicación pública y cualquier otro uso que se haga en los términos de la presente licencia y de la licencia de uso con que se publica.

d) Los autores manifiestan que se trata de una obra original sobre la que tienen los derechos que autorizan y que son ellos quienes asumen total responsabilidad por el contenido de su obra ante el Centro de Información Tecnológico (CENIT) y ante terceros. En todo caso el Centro de Información Tecnológico (CENIT) se compromete a indicar siempre la autoría incluyendo el nombre del autor y la fecha de publicación.

e) Autorizo al Centro de Información Tecnológica (CENIT) para incluir la obra en los índices y buscadores que estimen necesarios para promover su difusión.

f) Acepto que el Centro de Información Tecnológico (CENIT) pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

g) Autorizo que la obra sea puesta a disposición de la comunidad universitaria en los términos autorizados en los literales anteriores bajo los límites definidos por la universidad en las “Condiciones de uso de estricto cumplimiento” de los recursos publicados en Repositorio Institucional.

SI EL DOCUMENTO SE BASA EN UN TRABAJO QUE HA SIDO PATROCINADO O APOYADO POR UNA AGENCIA O UNA ORGANIZACIÓN, CON EXCEPCIÓN DEL CENTRO DE INFORMACIÓN TECNOLÓGICO (CENIT), EL AUTOR GARANTIZA QUE SE HA CUMPLIDO CON LOS DERECHOS Y OBLIGACIONES REQUERIDOS POR EL RESPECTIVO CONTRATO O ACUERDO.

CARTA DE ACEPTACIÓN DE LA EMPRESA

Señoras y señores
Universidad Hispanoamericana

Estimados:

Por medio de la presente hago constar que, en mi condición de Subgerente de Operaciones, yo Jose Luis Chan Galagarza la persona responsable en/de **Sislocar S.A**, brindo autorización para que el estudiante Ignacio Josué Cruz Chaves, cédula de identidad 604670316, desarrolle en esta empresa su trabajo de investigación, en su caso su Tesis.

Además, indico que, en la presentación de los resultados, de manera escrita y oral, puede utilizarse públicamente el nombre de esta empresa.
Asimismo, solicito que toda la información obtenida de esta empresa se utilice de manera confidencial, solamente para fines investigativos y educativos.

Cualquier consulta, sírvanse en contactarme al correo electrónico JchanG@sislocar.co.cr o al teléfono 64853427.

Atentamente.

Atte.

José Luis Chan Galagarza
Cédula: 6-0200-0561
Subgerente de Operaciones.

DEDICATORIA

“La perseverancia es la clave del éxito.” Charles Chaplin

Este trabajo es el resultado de un esfuerzo en grupo y del apoyo incondicional de quienes siempre han estado a mi lado. Dedico este logro a:

- Mis padres, Virginia Chaves y Trinidad Cruz, por ser la base de mi formación, por su amor, sacrificio y las enseñanzas que me han guiado en cada paso y decisión.
- Mi hermana, Meylin Arguedas, por su apoyo incondicional, por estar siempre presente y motivarme a seguir adelante incluso en los momentos más difíciles, por darme la posibilidad y los recursos para estar hoy donde estoy.
- Mi pequeño gran grupo de amigos, quienes con su compañía, confianza y palabras de aliento me dieron fuerzas para superar los retos y disfrutar de este proceso.
- Mi familia en general, por su comprensión y ánimo constante durante esta etapa académica.

Cada uno de ustedes ha sido pieza fundamental en este viaje, Mi más profundo agradecimiento, este logro no es solo mío, sino también de ustedes.

AGRADECIMIENTO

En primer lugar, quiero expresar mi más sincero agradecimiento a Dios, por darme la fortaleza, la sabiduría y la perseverancia necesarias para culminar esta importante etapa de mi vida.

Agradezco profundamente a mis padres, Virginia Chaves y Trinidad Cruz, quienes, con su amor incondicional, esfuerzo y sacrificio han sido mi mayor fuente de inspiración. Ellos me enseñaron el valor de la disciplina, la honestidad y el trabajo duro, principios que me acompañaron en todo el proceso académico y personal.

Un reconocimiento especial merece mi hermana, Meylin Arguedas, por su apoyo incondicional y por estar siempre a mi lado en los momentos más difíciles. Sus palabras de aliento y su fe en mí fueron un pilar fundamental para continuar con determinación este proyecto.

También quiero agradecer a mi grupo de amigos, quienes no solo compartieron alegrías y buenos momentos, sino que también me brindaron ánimo en las etapas más exigentes de esta carrera. Su compañía y respaldo hicieron que este camino fuera más llevadero y enriquecedor.

Extiendo mi gratitud a mis profesores y mentores académicos, quienes con sus enseñanzas, exigencia y guía me ayudaron a desarrollar las habilidades necesarias para crecer tanto profesional como personalmente. Sus consejos y conocimientos han dejado una huella que perdurará a lo largo de mi vida.

Finalmente, agradezco a todos aquellos que, de una u otra manera, contribuyeron a que este logro fuera posible. Cada gesto de apoyo, cada palabra de aliento y cada muestra de confianza se convirtieron en la motivación que me impulsó a llegar hasta aquí.

ABREVIATURAS

SGSI Sistema de Gestión de Seguridad de la Información

ISO International Organization for Standardization

IEC International Electrotechnical Commission

ISO/IEC 27001 Norma internacional para sistemas de gestión de seguridad de la información

ISO/IEC 27002 Código de buenas prácticas para controles de seguridad de la información

TI Tecnología de la Información

CIA Confidencialidad, Integridad y Disponibilidad (principios de seguridad)

PDCA Planificar, Hacer, Verificar, Actuar (ciclo de mejora continua)

ANS Acuerdo de Nivel de Servicio

SOP Procedimiento Operativo Estándar

RTO Tiempo Objetivo de Recuperación

BIA Análisis de Impacto al Negocio

GAP Brecha (diferencia entre estado actual y deseado)

CSIRT Equipo de Respuesta ante Incidentes de Seguridad Informática

GDPR Reglamento General de Protección de Datos (por sus siglas en inglés)

KPI Indicador Clave de Desempeño

RESUMEN

Este proyecto tiene como objetivo principal implementar mejoras en la seguridad de la información, alineadas con los estándares ISO/IEC 27001 y 27002, para mitigar los riesgos cibernéticos en la empresa SISLOCAR Caldera S.A. Se aborda la implementación de dichas mejoras con el fin de proteger la información sensible que, como empresa aduanera, constituye el mayor activo de la organización. El estudio se fundamenta en los estándares internacionales mencionados, utilizándolos como marco para el fortalecimiento de la gestión segura de los datos manejados.

Se realizó un diagnóstico exhaustivo mediante un enfoque de metodología mixta para detectar brechas y vulnerabilidades existentes. Para ello, se evaluaron los procesos operativos, los mecanismos de control de acceso y las prácticas de protección de datos. Se emplearon instrumentos clave, como la Matriz de Riesgos, el análisis de brechas y el análisis documental, para obtener una visión verosímil de la situación actual de la empresa. Con respecto a los hallazgos, se detectaron deficiencias en el sistema de resguardo de la seguridad de la información, lo que brinda una oportunidad para establecer un enfoque estratégico en la gestión del riesgo. Esto permitirá la consolidación de un Sistema de Gestión de Seguridad de la Información (SGSI) robusto.

Como parte de las soluciones propuestas, se diseñó un plan de mejoras continuas que incluye controles específicos para cada área sensible, abordando la protección de datos, el cifrado y la prevención de amenazas cibernéticas. En conclusión, este proyecto establece una relación recíproca entre la teoría de los estándares ISO/IEC 27001 y 27002 y la práctica de la mejora continua. Al poner en marcha los controles establecidos, se busca reducir la exposición a amenazas digitales, creando una cultura institucional preventiva que asegure la calidad operativa de la organización.

CAPÍTULO I: PLANTEAMIENTO DEL TEMA

1.1 ANTECEDENTES Y JUSTIFICACIÓN DEL ANTEPROYECTO

En el desarrollo de un proyecto de investigación sólido y pertinente, es indispensable establecer fundamentos contextuales que permitan comprender la ubicación y relevancia de la problemática abordada. Resulta esencial ofrecer una panorámica realista que sitúe a la empresa y al campo de estudio, con el fin de comprender su entorno, estructura y dinámica operativa. En esta sección, se presentan dichos elementos contextuales, enfocados en la empresa SISLOCAR, ubicada en Caldera, Puntarenas.

Asimismo, se justifica la importancia del proyecto, considerando tanto las razones internas que evidencian su necesidad a nivel organizacional, como los factores externos que refuerzan la urgencia de su ejecución. En este sentido, el presente estudio tiene como objetivo principal abordar la implementación de mejoras en la seguridad de la información, alineadas con las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022**,** como estrategia para mitigar riesgos informáticos en la empresa SISLOCAR Caldera. Con ello, se pretende generar conocimiento que fortalezca la comprensión del fenómeno y promueva soluciones innovadoras en el ámbito de la informática aplicada a la gestión empresarial.

1.1.1 Antecedentes del Contexto de la Empresa

SISLOCAR Caldera S.A. es una empresa costarricense con sede en el distrito de Caldera, cantón de Esparza, provincia de Puntarenas, Costa Rica. Fue fundada en el año 2008, y desde sus inicios se ha enfocado en ofrecer soluciones logísticas integrales que incluyen servicios de

transporte terrestre de carga, almacenamiento, distribución y apoyo en trámites aduanales. La compañía ha logrado consolidarse como un actor relevante en la región del Pacífico costarricense, gracias a su ubicación estratégica cercana al Puerto de Caldera, una de las principales puertas de entrada y salida de mercancías del país. Los datos aquí expuestos se extraen de los archivos empresariales.

Dentro de su gestión operativa, cuenta con una infraestructura robusta, compuesta por una bodega de 3,500 m², con capacidad para 20 contenedores, herramientas de operación como montacargas, rack selectivo y posee la capacidad para el almacenamiento de vehículos en un área de 12,000 m².

En el campo de logística y operación del riesgo, cuenta con herramientas que le acreditan certificaciones y prácticas, que respaldan la gestión del riesgo, en cuanto a la protección de los activos que transportan y almacenan. Entre ellos se puede mencionar, Certificación BASC, relaciona con la logística aplicada para la protección contra el contrabando. También cuentan con Bandera Azul Ecológica, que demuestra la responsabilidad con el ambiente.

Establecen políticas estrictas para la gestión de productos peligrosos, contando con todos los implementos requeridos por el Reglamento Técnico RTCR 478: 2015. Aplican también, el Sistema SITRAT, que establece el monitoreo constante de la temperatura en cámaras frías, para evitar la pérdida de mercadería perecedera. Por último, aplican el sistema SGAE, que establece la trazabilidad de verificación y seguimiento por parte del cliente, de la carga en tránsito.

Misión

La misión de SISLOCAR Caldera S.A. consiste en brindar servicios logísticos eficientes, seguros y confiables, contribuyendo al desarrollo comercial de sus clientes mediante la optimización de la cadena de suministro.

Visión

Su visión proyecta a la empresa como una organización líder en el sector logístico regional, comprometida con la mejora continua, la innovación tecnológica y el respeto por el medio ambiente.

Objetivos

Entre sus objetivos estratégicos se encuentran:

1. Garantizar altos niveles de calidad y seguridad en el transporte y manejo de mercancías.
2. Promover la adopción de tecnologías que mejoren la trazabilidad y eficiencia de sus procesos.
3. Fortalecer la satisfacción del cliente a través de un servicio personalizado y oportuno.
4. Impulsar el desarrollo sostenible mediante prácticas responsables en sus operaciones.

Valores

Ofrecemos servicios logísticos flexibles y excepcionales basados en sólidos valores. Nos enorgullecemos de adaptarnos a las necesidades cambiantes de nuestros clientes y buscar constantemente la mejora.

1. Flexibilidad de nuestros servicios al servicio de nuestros clientes para adaptarnos a las cambiantes situaciones logísticas.
2. Respeto hacia nuestros empleados, clientes, competidores, leyes, proveedores y el medio ambiente.
3. Transparencia: Enfrentar nuestros errores ante nuestros clientes, buscando siempre la mejora continua.
4. Empatía: Nos ponemos en el lugar de nuestros clientes y entendemos el impacto de nuestro trabajo en sus operaciones.

Organización y Áreas de Operación

SISLOCAR Caldera S.A. cuenta con una estructura organizacional funcional, conformada por áreas administrativas, operativas, logísticas y de mantenimiento. La empresa opera con una flota de vehículos propios y personal capacitado para asegurar el cumplimiento de normativas nacionales e internacionales en materia de transporte de carga. Además, mantiene alianzas estratégicas con empresas del sector portuario y aduanal para brindar un servicio integral. En la figura N° 1, se presenta el organigrama estructural de la empresa.

Figura N° 1. Organigrama SISLOCAR Caldera S.A

Fuente: Datos de la empresa (2024).

Historia y Evolución

Desde su fundación, la empresa ha transitado por distintas etapas de desarrollo. En sus primeros años, se concentró en el transporte de carga nacional, pero gradualmente amplió su portafolio de servicios hacia la logística integral, incluyendo almacenaje temporal, distribución regional y gestión documental. La cercanía al Puerto de Caldera ha sido un factor clave para su posicionamiento en el mercado, ya que permite una respuesta rápida y eficiente ante las necesidades del comercio internacional. En la figura N° 1, se ofrece una línea de tiempo, que describe la evolución histórica de la empresa.

Figura N° 2. Evolución histórica de la empresa

Fuente: Elaboración del investigador, con datos de la empresa SISLOCAR (2024).

Como se puede denotar en la figura anterior, la evolución de la empresa se ha desarrollado de forma acelerada y procurando siempre estar acorde con los estándares de calidad y seguridad de un mundo globalizado. En los últimos cinco años, SISLOCAR ha apostado por la digitalización de sus procesos internos, mediante la implementación de software logístico, monitoreo por GPS y automatización de tareas administrativas. No obstante, esta transformación tecnológica ha revelado debilidades en materia de seguridad de la información, razón por la cual se hace necesaria una intervención estratégica en esta área.

Tendencias del Mercado

El sector logístico costarricense se encuentra en una etapa de transformación marcada por la globalización, la innovación tecnológica y la necesidad de adoptar prácticas sostenibles. Las empresas del sector enfrentan crecientes demandas de trazabilidad, seguridad de la información, cumplimiento normativo y eficiencia operativa.

En este contexto, la incorporación de estándares internacionales en seguridad informática, como los propuestos por la norma ISO/IEC 27001 e ISO/IEC 27002 se ha convertido en una prioridad para las organizaciones que desean mantener su competitividad y proteger sus activos digitales. Ante esta tendencia, SISLOCAR Caldera S.A. se ve desafiada a fortalecer sus sistemas de gestión de la información, no solo para garantizar la continuidad del negocio, sino también para responder adecuadamente a los nuevos requerimientos del mercado logístico nacional e internacional.

1.1.2 Justificación del Proyecto

En el contexto de una sociedad globalizada, la evolución tecnológica avanza a un ritmo vertiginoso, obligando a las empresas a adoptar medidas estratégicas para proteger sus operaciones y los servicios que ofrecen. Los ciberataques han transformado significativamente la dinámica empresarial y la vida del colectivo humano, lo que ha generado una creciente preocupación por la seguridad de la información. En este sentido, la digitalización de las organizaciones comerciales debe ir acompañada de estrategias de protección que garanticen la integridad de los datos, la confidencialidad de la información y la seguridad de los procesos operativos.

A nivel mundial, el panorama resulta desafiante y exige la implementación de mecanismos eficaces para la protección de los sistemas de información. Al respecto, David y Monsalve (2023) señalan:

> Según datos publicados, el 57% de las empresas en países como el Reino Unido, Alemania y Estados Unidos sufrieron al menos un ciberataque, y el 42% de ellas enfrentó dos o más ataques en el último año (2019). Este panorama presenta un desafío importante para las empresas, generando incertidumbre y preguntas sobre las medidas necesarias para combatir la creciente amenaza cibernética. (p. 8).

La estadística evidencia el incremento de los ciberataques en empresas de diversos sectores económicos, lo que pone de manifiesto la urgencia de fortalecer los protocolos de seguridad informática. Esto requiere la constante actualización de estrategias que permitan detectar y mitigar amenazas digitales cada vez más sofisticadas.

En este contexto, la empresa SISLOCAR Caldera S.A**.** reconoce la necesidad de adoptar normativas internacionales como ISO/IEC 27001 y 27002, que establecen criterios para la gestión de la seguridad de la información. Para ello, resulta indispensable contar con un estudio previo científicamente fundamentado que permita la toma de decisiones orientadas a la práctica de la ciber resiliencia. Este enfoque no solo busca prevenir ataques, sino también fortalecer la capacidad de respuesta y recuperación ante eventuales incidentes, garantizando la continuidad operativa.

La seguridad de la información constituye un eje fundamental en el sector logístico, donde la confidencialidad y la gestión eficiente de los datos resultan cruciales para la calidad del servicio y la confianza de los clientes. En este marco, SISLOCAR Caldera S.A**.,** ubicada en el distrito de

Caldera, provincia de Puntarenas, se especializa en servicios logísticos integrales, que incluyen transporte de mercancías, almacenamiento temporal y gestión documental para empresas nacionales e internacionales. En los últimos años, la compañía ha experimentado un notable crecimiento en su volumen de operaciones, lo que ha impulsado la incorporación de herramientas tecnológicas y sistemas digitales para optimizar la gestión operativa y administrativa.

No obstante, esta expansión tecnológica no ha estado acompañada por una planificación estructurada en términos de seguridad de la información. Actualmente, la empresa carece de una política formal de seguridad informática, no dispone de un sistema integral de gestión de riesgos y sus controles se implementan de manera reactiva e independiente. Entre los aspectos críticos identificados se encuentran la ausencia de protocolos de clasificación de la información, la gestión deficiente de accesos y la falta de procedimientos sistematizados para la respuesta a incidentes. Asimismo, los respaldos de información no están organizados de manera estructurada, y algunos equipos clave de operación no cuentan con las actualizaciones de seguridad necesarias.

Un diagnóstico interno, realizada en marzo de 2025 reveló que el 65% de los equipos informáticos no tenían software antivirus actualizado**,** y que los accesos a los sistemas administrativos eran compartidos entre múltiples usuarios sin trazabilidad de actividad**.** También se identificó una alta dependencia del correo electrónico como canal de comunicación operativa, sin mecanismos adecuados de cifrado o validación de identidad.

Estos hallazgos evidencian un estado de vulnerabilidad que expone a la empresa a riesgos de seguridad digital, pérdida de datos y accesos no autorizados. Por tanto, la adopción de un enfoque proactivo en seguridad informática es imperativa para garantizar la protección de los sistemas de información y fortalecer la resiliencia organizativa frente a amenazas cibernéticas en

un entorno cada vez más complejo y desafiante que procure el establecimiento de una cultura organizacional orientada a la protección de los activos informáticos.

1.2 Definición del Problema

La definición de problema consiste en una acción lógica que transforma la idea que produjo el génesis a la indagación, en un problema de investigación. Se convierte en el mapa de ruta que oriente los procesos de indagación, correlacionando todos los elementos que intervienen en él. De acuerdo con Tecla (2006) mencionado en, Torres y Monroy (2019), "El planteamiento del problema en una investigación, representa una etapa importantísima, diríase que incluso crucial, al grado que algunos autores señalan que el planteamiento correcto del problema equivale a tener avances en la mitad de la investigación" (p. 1)

De acuerdo con lo citado por los autores anteriores, se puede inferir la relevancia del planteamiento del problema, a través de una conciencia investigativa, que precisa de forma detallada, el rumbo, los procesos y la ruta clara, para la obtención de resultados confiables y significativos que no comprometan el rigor académico del proceso indagativo y poder así optimizar los recursos que garanticen la confiabilidad y pertinencia de los hallazgos.

Entonces, la empresa SISLOCAR Caldera S. A, dedicada a los servicios aduaneros en el puerto de Caldera, enfrenta un entorno cada vez más vulnerable a los riesgos de ciberseguridad debido al manejo intensivo de información sensible en sus procesos. La digitalización y automatización de los procedimientos aduaneros, aunque ha mejorado la eficiencia operativa, ha incrementado la exposición a amenazas cibernéticas que pueden comprometer la integridad, confidencialidad y disponibilidad de la información crítica. Estos riesgos no solo impactan la

continuidad de las operaciones, sino que también pueden generar consecuencias financieras, legales y reputacionales severas para la empresa.

En este contexto, la falta de un sistema robusto de gestión de la seguridad de la información, alineado con estándares internacionales como ISO 27001 e ISO 27002, impide a SISLOCAR garantizar la protección efectiva de su infraestructura tecnológica y los datos que maneja. Actualmente, los controles de seguridad implementados son insuficientes para enfrentar amenazas sofisticadas y emergentes, lo que pone en riesgo la confiabilidad de los procesos aduaneros.

Es por esto por lo que surge la necesidad de desarrollar una propuesta de implementación de mejoras en seguridad de la información, alineada con las normas ISO 27001 y 27002, que permita mitigar los riesgos identificados. La solución debe estar orientada a fortalecer los controles de seguridad, establecer una gestión adecuada de riesgos y promover una cultura organizacional que priorice la ciberseguridad.

1.2.1 Problemática

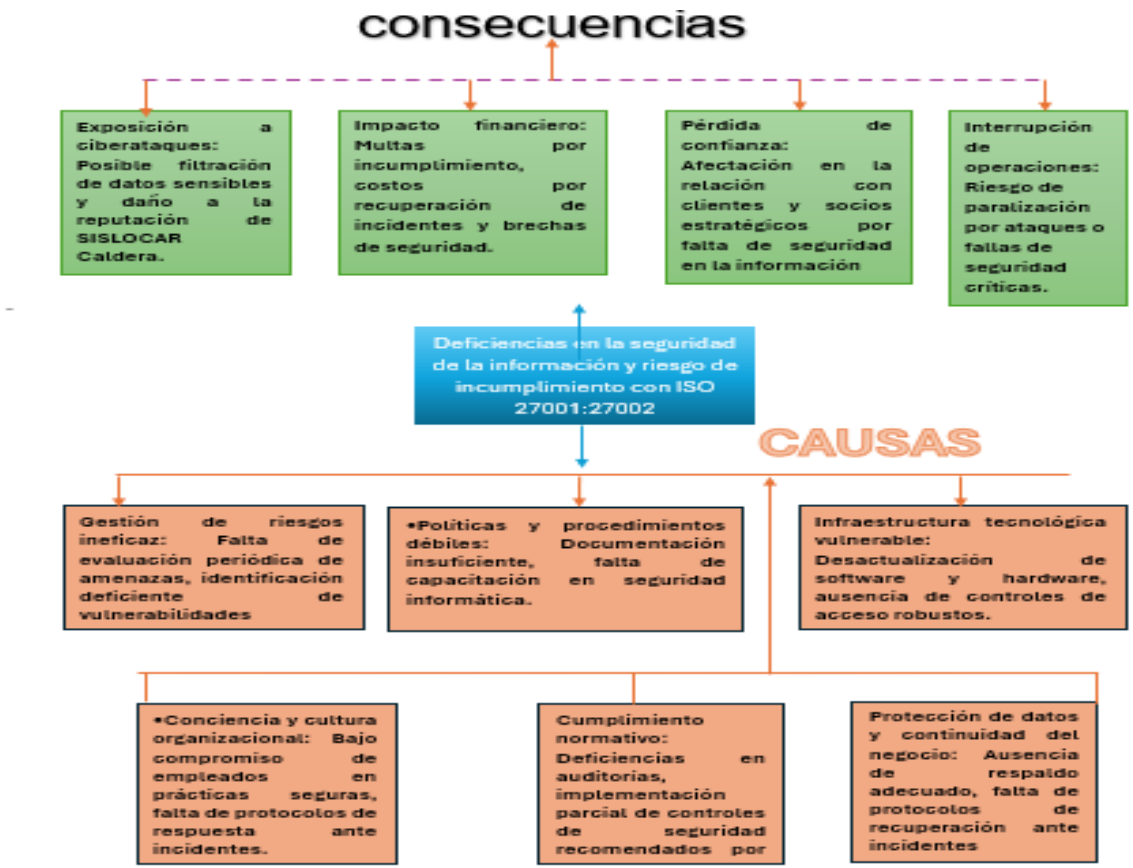
SISLOCAR, empresa especializada en la gestión de procesos aduaneros en el puerto de Caldera, Costa Rica, está cada vez más expuesta a riesgos de ciberseguridad debido a la digitalización y automatización de sus operaciones. Si bien estos procesos aumentaron la eficiencia operativa, también introdujeron nuevas vulnerabilidades en los sistemas de información de la empresa. La falta de un sistema de gestión de seguridad de la información integral y robusto alineado con estándares internacionales como ISO 27001 e ISO 27002 plantea una amenaza significativa para la integridad, confidencialidad y disponibilidad de los datos críticos de la empresa.

A medida que la tecnología continúa evolucionando, los ciberataques han aumentado en complejidad y frecuencia, afectando a empresas de todos los sectores. El sector aduanero en particular se encuentra en una posición vulnerable debido al alto valor de la información confidencial que procesa, como datos de clientes, registros de transacciones y documentación relacionada con importaciones y exportaciones. La situación se agrava en el caso de SISLOCAR, que, como empresa multinacional en un entorno altamente regulado, debe garantizar la seguridad de los datos de sus clientes y la continuidad de sus actividades comerciales para no poner en riesgo su reputación y posición en el mercado.

1.2.2 Diagrama Causa- Efecto

El siguiente diagrama, explicita en forma gráfica, las causas de los principales problemas detectados y los posibles efectos, aplicando la técnica, árbol del problema, con la finalidad de ofrecer una imagen sistemática de la situación analizada, mediante una estructuración lógica, que facilite la clara comprensión del contexto del problema investigado.

Figura N° 3. Árbol del Problema



Fuente: Elaboración propia (2025)

El diagrama anterior, representa la problemática detectada en la empresa involucrada, representando posibles deficiencias en el sistema de seguridad de la información, y organizando sus causas y consecuencias para una visión holística del problema en estudio, para la conducción eficiente de los procesos de indagación propuestos en este proyecto.

1.2.3 Problema General

El problema general del proyecto:

¿Cómo implementar mejoras de Seguridad de la información, alineadas con los estándares ISO/IEC 27001 y 27002 para mitigar y gestionar los riesgos cibernéticos en la empresa SISLOCAR Caldera S. ¿A, con un horizonte de ejecución en agosto de 2025?

1.2.4 Problemas Específicos

1. ¿Cuáles son los principales riesgos de ciberseguridad que enfrenta la empresa SISLOCAR, Caldera S. ¿A, específicamente en el contexto de sus operaciones y manejo de información confidencial?
2. ¿Cuáles son las debilidades en los mecanismos actuales de control de accesos y protección de datos sensibles, de políticas internas, tecnologías empleadas y prácticas vigentes en la empresa, SISLOCAR, Caldera S. ¿A, en el contexto de sus operaciones y manejo de información confidencial?
3. ¿Cómo optimizar la implementación de controles tecnológicos y auditorías de seguridad mediante el diseño de una propuesta de mejoras, para fortalecer la protección contra amenazas cibernéticas y mejorar la detección y prevención de vulnerabilidades?

1.3 Objetivos del Proyecto

Los objetivos de un proyecto se convierten en la brújula que dirige hacia a dónde debe llegar la indagación y define qué es lo que se quiere estudiar. Desde el punto de vista de Hernández et al (2018), “Son las guías del estudio y hay que tenerlos presentes durante todo su desarrollo”. (p. 81). Entonces, son los elementos que definen y direccionan el estudio.

En este apartado, se presenta un objetivo general Expresa la meta principal del estudio, el resultado global que se busca alcanzar. Debe ser claro, alcanzable y alineado con la problemática investigada y tres específicos que detallan las acciones a seguir, centrados en aspectos concretos que ayudan a operacional, el propósito general.

1.3.1 Objetivo General

Implementar mejoras de Seguridad de la información, alineadas con los estándares ISO/IEC 27001 y 27002 para mitigar y gestionar los riesgos cibernéticos en la empresa SISLOCAR Caldera S. A, con un horizonte de ejecución en agosto de 2025.

1.3.2 Objetivo Específico

1. Identificar los principales riesgos de seguridad de la información que enfrenta la empresa SISLOCAR Caldera S.A., mediante la evaluación de sus procesos operativos y del manejo de información confidencial, con el propósito de establecer un diagnóstico que sirva de base para la implementación de controles alineados con los estándares ISO/IEC 27001 y 27002.
2. Analizar las debilidades en los mecanismos actuales de control de accesos y protección de datos sensibles, mediante la revisión de políticas internas, tecnologías empleadas y

prácticas vigentes en la empresa, con el fin de orientar mejoras que reduzcan la exposición a riesgos cibernéticos.

3. Diseñar una propuesta de mejora del sistema de gestión de seguridad de la información, basada en los lineamientos de las normas ISO/IEC 27001 y 27002, que incluya controles específicos para el acceso y la protección de datos, y que permita mitigar los riesgos de accesos no autorizados y la vulneración de información crítica.

1.4 Alcances y Limitaciones

En este apartado, se exponen los alcances, limitaciones y exclusiones del proyecto, con la finalidad de ofrecer una delimitación clara del marco en el que se desarrolla la investigación. Dentro de los alcances, se exponen todos los aspectos inherentes al problema que se abordan, mientras que las exclusiones, señalan aspectos que no se cobijan bajo este estudio y que se convierten en oportunidades para otras investigaciones.

En cuanto a las limitaciones, se hace referencia a los factores que puedan inferir en libre flujo de la indagación y que puedan causar impacto en resultados finales. Se hace referencia a los aspectos temporales estructurados para la investigación.

1.4.1 Alcances

Este proyecto, aborda el sistema de seguridad de información, de la empresa SISLOCAR Caldera S. A, que se exponen a continuación:

1. Alcance temporal: El estudio se lleva a cabo durante el año 2025, con un cronograma específico para identificación de debilidades, análisis de riesgos y diseño de una propuesta de mejora del sistema de gestión de seguridad de la información.
2. Geográficamente, tiene un alcance en una empresa de logística con almacenes fiscales, ubicada en Caldera, en la provincia de Puntarenas, Costa Rica.
3. El primer entregable, diagnostica en forma integral, los principales riesgos de seguridad de la información que enfrenta SISLOCAR Caldera S. A, mediante el análisis de los procesos operativos relacionados con la gestión de información confidencial, incluyendo el almacenamiento, transmisión y acceso a datos sensibles, considerando los procedimientos internos, la infraestructura tecnológica y las prácticas de seguridad implementadas por la empresa. Tomando como referencia, los estándares internacionales ISO/IEC 27001 y 27002 para determinar el nivel de cumplimiento y las brechas existentes en la protección de la información.
4. El segundo entregable, identifica las posibles debilidades en los mecanismos actuales de control y protección de datos, mediante la revisión detallada de los procesos operativos y de las políticas de seguridad de la empresa. también se analiza las posibles vulnerabilidades que puedan intensificar los riesgos de ataques cibernéticos.
5. El entregable tres, propone mejoras estructurales en el sistema de gestión de seguridad de la información de la empresa, basada en los lineamientos de las normas ISO/IEC 27001 y 27002. La iniciativa busca fortalecer los mecanismos de acceso y protección de datos críticos, incorporando controles específicos que mitiguen los riesgos asociados a accesos no autorizados y vulneraciones de información sensible.

1.4.2 Exclusiones

1. Este proyecto no incluye una auditoría exhaustiva de cumplimiento normativo ni pruebas técnicas de penetración o evaluación de vulnerabilidades en los sistemas informáticos de la empresa.
2. No se aborda la capacitación del personal en seguridad de la información ni la implementación de soluciones tecnológicas específicas, ya que estas actividades quedarán fuera del alcance del presente análisis.
3. El estudio se enfoca exclusivamente en los riesgos internos derivados de la gestión de información y procesos operativos, dejando fuera aquellos riesgos externos asociados a amenazas globales, como ciberataques dirigidos o fraudes externos.
4. Este análisis no incluye la ejecución de pruebas técnicas de penetración o simulaciones de ataques informáticos sobre los sistemas de la empresa.
5. No aborda el desarrollo de nuevas herramientas de seguridad, ya que dichas acciones requerirán fases posteriores de ejecución.

1.4.3 Limitaciones del proyecto

El proyecto se sitúa dentro de la problemática sobre seguridad de la información, alineadas con los estándares ISO/IEC 27001 y 27002 para mitigar y gestionar los riesgos cibernéticos en la empresa SISLOCAR Caldera S. A, por lo tanto, los hallazgos no se pueden generalizar a otras empresas similares, ya que el problema es especifico dentro del contexto empresarial propuesto.

1.5 Cronograma del Proyecto

Niveles	Procesos	Temporalidad Meses / Semanas Septiembre				Octubre				Noviembre				Diciembre				Enero			
1	Visita a la empresa (solicitud de permisos, exploración de posibilidades)																				
	Planificación del proyecto (Antecedentes y justificación del proyecto)																				
	Definición del problema																				
	Objetivos del problema																				
2	Exploración bibliográfica (Respaldo teórico)																				
3	Elección de metodología para la investigación (enfoque fuentes de información, Técnicas y herramientas de recolección de datos, definición y operacionalización de variables, diseño de la investigacion, matriz de coherencia)																				
4	Diagnóstico (Descripción de la situación actual, recolección de datos, determinación de brechas)																				
5	Diseño y desarrollo del proyecto																				
6	Conclusiones y recomendaciones																				
7	Afinamiento del informe final (Revisión del uso correcto del lenguaje, bibliografía y anexos)																				

Fuente: Elaboración propia (2024)

CAPÍTULO II: MARCO TEÓRICO

Este apartado se reviste de importancia para la investigación, al convertirse en el espacio para proporcionar aspectos relevantes que conforman el esqueleto del quehacer indagativo. Aspectos conceptuales y teorías sustentadas, le ofrecen un sustrato confiable que respalda los nuevos hallazgos. Según Hernández et al. (2018), apoyados en Yedigis y Weinbach (2005),

> El marco teórico es una etapa y un producto. Una etapa que implica un proceso de inmersión en el conocimiento existente y disponible que debe estar relacionado con el planteamiento del problema (objetivos, preguntas, justificación, viabilidad y evaluación de las deficiencias de lo que se sabe del problema), y un producto, que a su vez es parte de un producto mayor: el reporte o informe de investigación (p.10).

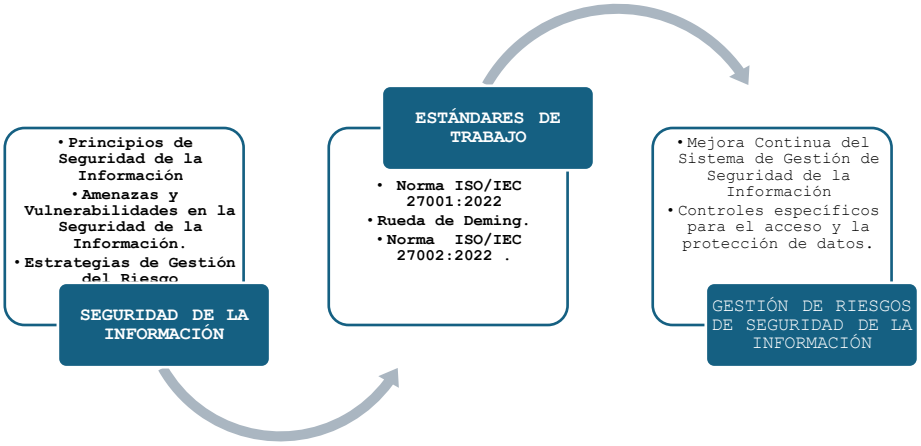
Entonces, el marco teórico es una construcción de un andamiaje de conocimientos existentes para respaldar las variables en estudio y lograr comprender el fenómeno del problema planteado. Permite comprender y ubicar en el contexto, aspectos relevantes que sirven como guía para el análisis de los datos obtenidos y contrastarlos con la realidad. Por tanto, en el contorno del proyecto, el estrato de fundamentos versa sobre los principios esenciales sobre la seguridad de la información, en medios digitales. Este abordaje, permite visualizar la importancia y el valor que se le confiere a los datos digitales, dentro del campo de la seguridad de la información.

Es necesario establecer conceptualizaciones básicas de los pilares fundamentales para la gestión de la seguridad de la información, no solo como escudo protector, sino también, como espacio de análisis que proyecten una mejora continua, visualizando la versatilidad y evolución de los ciberespacios. En la narrativa expuesta, se concatena las teorías medulares, con la realidad operativa de SISLOCAR Caldera S.A, con la finalidad de justificar la propuesta y a la vez, la impregne de humanismo, ética y realidad contextual, mediante la exploración de conceptos inherentes con el despeje de la incógnita que plantea el problema, ¿Cómo implementar mejoras de Seguridad de la información, alineadas con los estándares ISO/IEC 27001 y 27002 para mitigar y gestionar los riesgos cibernéticos en la empresa SISLOCAR Caldera S.A, con un horizonte de ejecución en agosto de 2025?

Por tanto, para constatar la pertinencia del problema analizado, el marco teórico, ofrece las teorías y conceptos que respaldan la idea de la investigadora, sus variables e indicadores. En la figura 4, se ofrece un diagrama con el contenido del este capítulo.

Figura N° 4

Organización del Marco Teórico



Fuente: Elaboración propia (2024).

2.1 Seguridad de la información

En un entorno digital en constante evolución, la seguridad de la información se ha convertido en un pilar esencial para la sostenibilidad y protección de las organizaciones. La creciente dependencia de los sistemas informáticos y la expansión de las redes han generado un ecosistema donde los datos no solo representan un recurso estratégico, sino también un activo cuya integridad, confidencialidad y disponibilidad deben ser resguardadas frente a riesgos emergentes.

Según lo expone Vega (2021). “La seguridad de la información es un concepto que se involucra cada vez más en muchos aspectos de nuestra sociedad hiperconectada, en gran parte como resultado de nuestra adopción casi ubicua de la tecnología de información y comunicación” (p. 9). El autor resalta la importancia que cobra, este tema, dentro de un mundo moderno interconectado y tecnificado. Por tanto, debe ser uno de los principales pilares adoptados por una empresa, que transcurre en este ambiente informático.

A este respecto se abordan diversos conceptos como, Triada CID, Política de seguridad de la información, análisis de brechas, inventario de activos, análisis de riesgos, Esteganografía, Vigenere, Vercrypt, Mason, Backus, Harding y AES Crypt. A continuación, se realiza una definición de algunos, fundamentados en el estudio realizado por Rozo y Suarez (2016)

1. **Triada CID:** Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su C-I-D: o Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. o Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. o Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de esta, por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
2. **Política de seguridad de la información**: conjunto de normas y procedimientos establecidos por una organización para regular el uso de la información y de los sistemas que la tratan con el fin de mitigar el riesgo de pérdida, deterioro o acceso no autorizado a la misma.
3. **Análisis de brechas:** identificación de riesgos, definición de controles, identificación de requisitos legales, regulatorios, contractuales.
4. **Inventario de activos**: un activo de información es un elemento que posee información. Entre activos de información encontramos las bases de datos, acuerdos y/o contratos, documentos del sistema, ficheros, aplicaciones, software de información, equipos informáticos.
5. **Análisis de riesgos**: tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.
6. **Esteganografía**: La esteganografía es la disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros normalmente multimedia, llamados portadores, de modo que no se perciba su existencia. Es una mezcla de artes y técnicas que se combinan para conformar la práctica de ocultar y enviar información sensible en un portador que pueda pasar desapercibido.

7. **Vigenere:** El cifrado Vigenère es un criptosistema simétrico, es decir, utiliza la misma clave para cifrar y descifrar. El cifrado Vigenère se asemeja mucho al cifrado César, pero su diferencia radica en que el primero utiliza una clave más larga para contrarrestar el gran problema del cifrado César: el hecho de que una letra sólo puede ser codificada de una forma. Para resolver este problema, se utiliza una palabra clave en lugar de un carácter simple.
8. **Vercrypt (Truecrypt):** Vercrypt, al igual que Truecrypt, cuando crea un nuevo Contenedor o Volumen, te da lo posibilidad de crear un Hidden Veracrypt (Truecrypt) Volume, o lo que es lo mismo: Un volumen oculto que sirve para tener los datos a salvo incluso cuando una persona se ve forzado a decir su contraseña.
9. **Mason**: El cifrado francmasón es un cifrado por sustitución simple que cambia las letras por símbolos. Sin embargo, el uso de símbolos no impide el criptoanálisis, y el criptoanálisis es idéntico al de otros métodos de cifrado por substitución simple. Llamado también "cifra Pigpen" este método de cifrado fue utilizado por los masones en el siglo XVIII para preservar la privacidad de sus archivos.
10. **Backup**: el backup o copia de seguridad, es la copia total o parcial de información importante como respaldo frente a eventualidades. La copia de seguridad debería ser guardada en un soporte almacenamiento diferente del original, para evitar que un fallo en el mismo pueda estropear el original y la copia.
11. **Acronis:** Acronis True Image es una aplicación para la creación de imágenes de disco, especial para crear sistemas de respaldos y recuperación de PCs. Es desarrollada por la empresa Acronis. Es una aplicación muy sencilla de usar, gracias a su interfaz que posee un claro asistente. Fue lanzado en 2002 y podía crear una imagen de la unidad que estaba siendo ejecutada sin tener que pasar al modo DOS. Las últimas versiones también permiten crear respaldos online de los datos. Soporta múltiples sistemas de archivos como ser NTFS, FAT16, FAT32, ext2, ext3, ReiserFS, Reiser.
12. **Linux Swap**; además también puede copiar cualquier otro sistema de archivos en modo raw, capturando una imagen de todos los sectores de un disco. Este modo también sirve para sistemas de archivos que se han corrompido.
13. **Hardening:** es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc.

Innecesarios en el sistema, así como cerrando puertos que tampoco estén en uso además de muchas otros métodos y técnicas.

14. **AES Crypt**: es un software de cifrado de archivos disponibles en varios sistemas operativos que utiliza el estándar de la industria estándar de cifrado avanzado (AES) para cifrar archivos de forma fácil y segura.

2.2 Principios de la Seguridad de la Información

La seguridad de la información se basa en tres principios fundamentales: confidencialidad, integridad y disponibilidad, los cuales garantizan la protección y el manejo adecuado de los datos en entornos digitales. En esta conceptualización, intervienen dos elementos inherentes uno del otro, la seguridad informática y la que resguarda la información. Ambas ramas se encuentran inmersas en el universo de la digitalización informativa. Aguilera (2011), mencionado en Espinoza (2020), expresa,

> Se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad. (p.4).

De acuerdo con lo expresado en el extracto anterior, la seguridad informática como disciplina, integra conocimientos interdisciplinarios en procura del diseño de propuestas y proyectos, que aseguren la protección digital, tanto de la información como de la infraestructura tecnológica, ante amenazas que puedan generarse a lo interno o a lo externo de la organización. Permite garantizar la confidencialidad, integridad y disponibilidad depurada de los datos en tránsito. En su accionar toma en cuenta principios fundamentales que se exponen a continuación.

El principio de **c**onfidencialidad busca restringir el acceso no autorizado a la información, asegurando que solo las personas con permisos adecuados puedan consultarla. Este aspecto es crucial en sectores como el financiero y el de salud, donde la privacidad es esencial. Vega (2021) lo define de la siguiente manera, “La confidencialidad es un concepto similar, pero no igual, a la privacidad. La confidencialidad es un componente necesario de la privacidad y se refiere a nuestra capacidad de proteger nuestros datos de aquellos que no están autorizados para verlos” (p. 12).

Para garantizar la confidencialidad, se implementan medidas como autenticación de usuarios, encriptación de datos y sistemas de control de acceso, con el propósito de evitar filtraciones y proteger la sensibilidad de la información.

Por su parte, la **i**ntegridad se relaciona con la precisión, consistencia y confiabilidad de los datos a lo largo de su ciclo de vida. Siguiendo con Vega (2021), explicita, "En cuanto a la integridad se refiere a la capacidad de evitar que nuestros datos se modifiquen de manera no autorizada o indeseable" (p. 13). De acuerdo con lo expuesto, este principio es protector y favorece, la toma de decisiones basada en información, para mantener la integridad de los datos, acción que es crucial, ya que asegura que los registros sean veraces y libres de modificaciones indebidas. Para ello, se emplean estrategias como auditorías, validación de datos y copias de seguridad, con el fin de minimizar errores y garantizar la fiabilidad de la información almacenada.

El tercer principio, disponibilidad, establece que los sistemas y la información deben estar accesibles para los usuarios autorizados cuando se requieran. Este factor es esencial en sectores como el comercio electrónico y la banca digital, donde la continuidad operativa depende del acceso oportuno a los recursos tecnológicos. Vega (2021) la define como, "La disponibilidad se refiere a la capacidad de acceder a nuestros datos cuando los necesitamos" (p. 13). Este principio se fortalece, mediante el uso de servidores redundantes, planes de recuperación ante incidentes y mantenimiento preventivo, asegurando que los sistemas funcionen de manera estable y sin interrupciones.

Estos principios conforman la base de una gestión eficaz de la seguridad de la información, permitiendo la protección de los activos digitales y la estabilidad de los procesos organizacionales tan necesarios para la salvaguarda de la información confidencial, eje fundamental para la operacionalizad de la empresa SISLOCAR. Se debe ofrecer un enfoque global, de las posibles amenazas para asegurar la confiabilidad de cada operación, cada cliente y cada dato que se genere dentro del entorno empresarial. Se debe reflexionar, sobre las consecuencias adversas que puedan generarse, cuando la confianza se vea vulnerada, especialmente en una empresa altamente digitalizada como la del objeto de estudio. Por tanto, se hace necesario, establecer las bases para visualizar las amenazas como riesgos y no como eventualidades, para el reconocimiento de la necesidad de implementar políticas competentes protectoras, no como normas aisladas, sino como

cultura organizacional, partiendo de estándares internacionales, hacia las practicas técnicas y humanas aplicables.

2.3 Amenazas y Vulnerabilidades en la Gestión de Seguridad de la Información

En la era digital, la protección de la información se ha convertido en un desafío esencial para organizaciones de todos los sectores. La seguridad de los datos enfrenta múltiples riesgos que pueden comprometer su integridad, accesibilidad y privacidad. Para abordar estos desafíos, es fundamental comprender las amenazas que pueden afectar los sistemas informáticos y reconocer las vulnerabilidades que exponen a las entidades a posibles incidentes de seguridad. En el contexto de la empresa SISLOCAR Caldera, se relaciona la teoría, con respecto a las amenazas de ciberseguridad que puedan ocurrir en las diferentes gestiones empresariales y que pongan en riesgo, la confidencialidad, probidad y disponibilidad de los datos, en forma robusta y oportuna. Por tanto, a continuación, se abordan aspectos relevantes del tema.

2.3.1 Principales Amenazas a la Seguridad de la Información

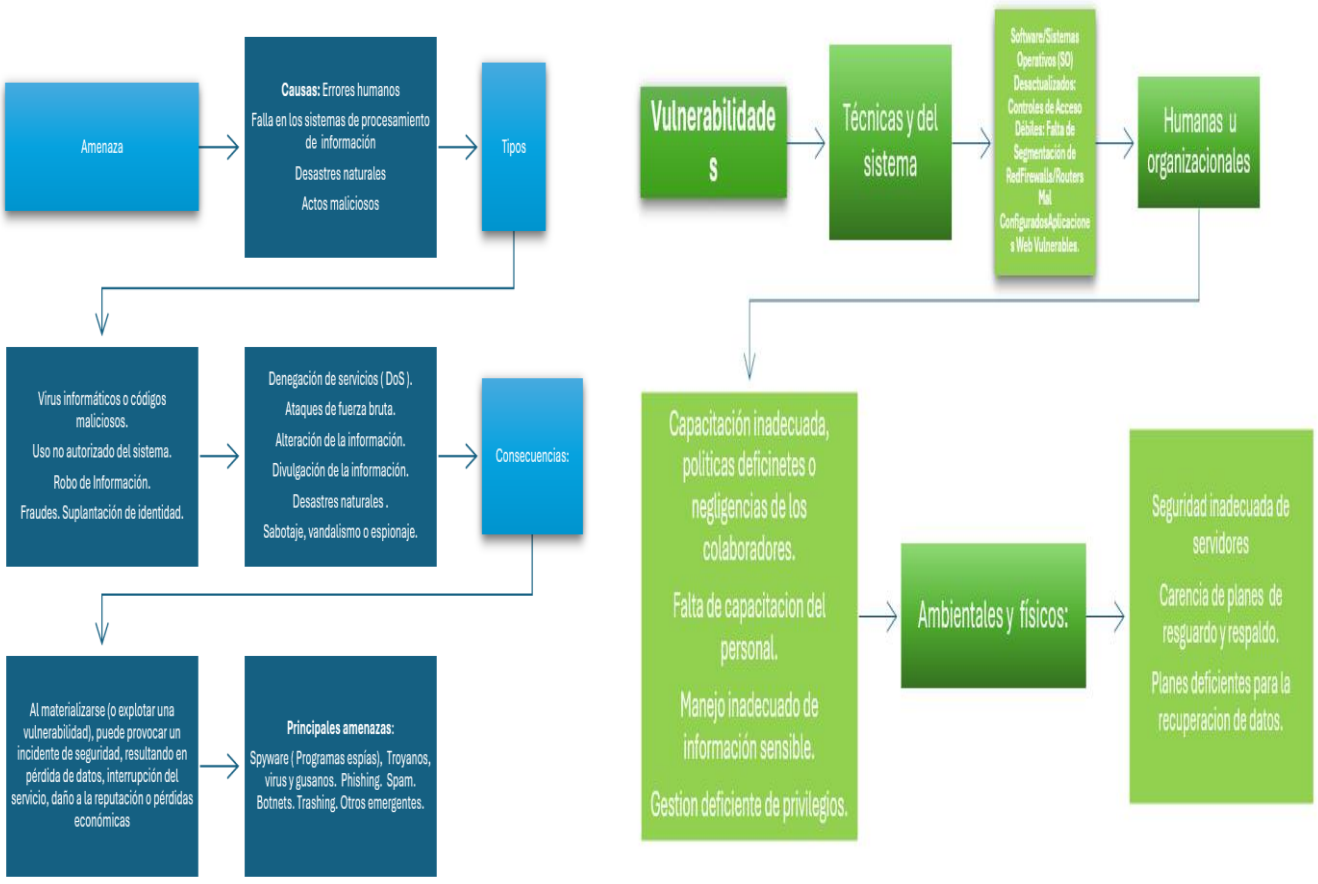
Es necesario cuestionarse en el campo de la ciberseguridad, ¿Qué es una amenaza?, con la finalidad de establecer una contextualización del concepto. En el campo de la información digital, se debe percibir como un problema que puede deteriorar el accionar de una empresa, provocando daños irreversibles, que provoquen la paralización de las operaciones y deteriorar la confianza de los clientes. Los sabotajes informáticos, se nutren de un ambiente vulnerable, que les facilite encontrar puntos débiles para cometer sus afectaciones. Para la empresa SISLOCAR, el activo, tránsito de datos, es esencial para la continuidad de operaciones que les garantice el posicionamiento dentro del comercio de servicios aduaneros, por tanto, el desglose de este tema, como teoría asociada con la práctica, permite ofrecer solidez a las estrategias organizacionales establecidas, que mitiguen cualquier brecha de seguridad informática. Tarazona (2009), expone,

> Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades. Las amenazas y vulnerabilidades están íntimamente ligadas y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar

ventajas de la vulnerabilidad y pueden venir de cualquier parte, interna o externa relacionada con el entorno de las organizaciones. (p. 1).

Lo expresado en el texto, establece una interacción determinante entre estos dos aspectos, que amenazan la seguridad de la información. Estas dos variables dependientes, se vinculan para afectar los procesos digitales de una empresa. La amenaza como tal es oportunista y sondea el camino inimaginado, para causar daño, mientras que la vulnerabilidad, se convierte en un sustrato idóneo para que el daño se desencadene. Basándose en la teoría expuesta por Tarazona (2009), se elabora la figura 5, que aporta información pertinente al tema.

Figura 5 Amenazas y vulnerabilidades



Fuente: Elaboración propia.

De acuerdo con lo reflejado en la figura expuesta, las amenazas a la seguridad de la información pueden provenir de diversas fuentes y adoptar múltiples formas. En la empresa SISLOCAR Caldera, se deben detectar de forma consecuente para lograr mitigar su embate contra la estabilidad de la organización. Según Check Point Software Technologies Ltd. (s.f), algunas de las más relevantes incluyen:

1. **Ataques cibernéticos dirigidos:** Métodos como phishing, ransomware y la explotación de fallos de seguridad buscan acceder ilegalmente a datos sensibles.
2. **Software malicioso:** Virus, troyanos y otros programas diseñados para infiltrar sistemas pueden comprometer el funcionamiento adecuado de las infraestructuras digitales.
3. **Riesgos internos:** Errores humanos, negligencia o el uso indebido de información por parte de empleados pueden generar brechas de seguridad significativas.
4. **Deficiencias en la protección tecnológica:** Configuraciones inapropiadas, falta de actualizaciones o políticas de seguridad ineficaces pueden facilitar accesos no autorizados.

2.3.2 Identificación y Evaluación de Vulnerabilidades

Los informes recientes evidencian un notable crecimiento en los ataques cibernéticos a nivel mundial, con un aumento del 38% en 2022 en comparación con el año anterior (Security Magazine, 2023). Este incremento se atribuye a la sofisticación creciente de los ciberdelincuentes, quienes han aprovechado vulnerabilidades presentes en herramientas digitales utilizadas por empleados remotos y entornos educativos.

Las vulnerabilidades en los sistemas de información pueden ser explotadas por actores malintencionados para acceder a datos restringidos. La gestión de riesgos implica identificar áreas débiles y aplicar medidas preventivas para fortalecer la seguridad digital. En concordancia con Sánchez (2018), entre las principales vulnerabilidades destacan:

1. **Gestión ineficiente de accesos:** Uso de contraseñas débiles, ausencia de autenticación multifactorial y permisos descontrolados pueden facilitar intrusiones.
2. **Falta de protocolos de encriptación:** La información transmitida sin cifrado es más susceptible a interceptaciones maliciosas.

3. **Software obsoleto:** Sistemas sin actualizaciones periódicas son más propensos a ser vulnerados por ciberdelincuentes.
4. **Desconocimiento en seguridad digital:** La falta de formación en buenas prácticas de ciberseguridad aumenta el riesgo de ataques exitosos.

Estrategias de Protección y Gestión de Riesgos

Para minimizar la exposición a amenazas, es imprescindible implementar estrategias de seguridad adaptadas a las necesidades de cada organización. El Centro Nacional de Seguridad Digital (2021) ofrece una definición acertada, sobre este aspecto.

> La gestión de riesgos de seguridad de la información es el proceso mediante el cual una organización identifica, evalúa y prioriza los riesgos que pueden afectar sus activos de información. Este proceso es esencial para asegurar la confidencialidad, integridad y disponibilidad de la información, permitiendo a la organización cumplir con sus objetivos estratégicos y operativos. (p. 4)

La cita describe la gestión de inseguridades de seguridad de la información como un proceso sistemático de identificación, evaluación y priorización de amenazas que pueden comprometer los activos digitales de una organización. En términos operativos, la correcta identificación de riesgos implica el uso de metodologías de reducción, transferencia, aceptación o evitación**,** dependiendo del nivel de exposición y los costos asociados. La integración de este proceso dentro de la arquitectura de seguridad contribuye a la protección de los datos, la resiliencia organizacional y el cumplimiento normativo.

Entonces, la gestión de la seguridad de la información requiere un enfoque integral que combine prevención, monitoreo y respuesta eficiente ante posibles amenazas. La protección de los datos no solo garantiza la operatividad de las organizaciones, sino que también contribuye a la confianza de los usuarios y la estabilidad del entorno digital.

Estándares de Trabajo

Los estándares de trabajo se conforman por un cumulo de principios, que dirigen los procedimientos y criterios aplicables, para la ejecución de tareas dentro de un campo profesional. Su finalidad es asegurar la eficiencia, calidad y cumplimiento de las normativas. Representan un conjunto de directrices establecidas para optimizar procesos, garantizar eficacia y promover la eficiencia dentro de una organización. Su aplicación permite definir criterios claros para la ejecución de tareas, asegurando uniformidad y alineación con normativas y mejores prácticas internacionales.

En el ámbito de seguridad informática, los estándares de trabajo son fundamentales para la implementación de políticas de protección de datos. La norma ISO/IEC 27001:2022 establece lineamientos para gestionar riesgos, implementar controles de seguridad y garantizar la integridad de la información. En el caso concreto, se hace alusión, a los referentes de la norma ISO/IEC 27001:2022 la que establece un marco para la gestión de la seguridad de la información y su impacto en la estandarización de las prácticas de seguridad.

Norma ISO/IEC 27001:2022

La norma ISO/IEC 27001:2022 representa un estándar internacional que establece un marco estructurado para la gestión de seguridad de la información, permitiendo a las empresas mitigar riesgos y garantizar la confidencialidad, integridad y disponibilidad de sus datos. Sus versiones han sido renovadas, para responder de forma precisa para la gobernanza de los controles de seguridad que respondan en forma eficiente, a las amenazas de seguridad de la información, emergentes. Según Garantía de Calidad de Red (NQA), (2024),

> La norma ISO 27001 se basa en el ciclo Planificar-Hacer-Verificar-Actuar (PDCA), también conocido como rueda de Deming o ciclo de Shewhart. El ciclo PDCA puede aplicarse no sólo al sistema de gestión en su conjunto, sino también a cada elemento individual para proporcionar un enfoque continuo en la mejora continua, (p. 7)

Según lo citado, se hace referencia a la mejora continua de la calidad en la seguridad de la información, para asegurar la eficiencia de una empresa, cuya dependencia directa consiste, en la

fidelidad de sus datos. Desde su primera versión, la norma ISO/IEC 27001 ha evolucionado para adaptarse al cambiante panorama de amenazas cibernéticas. La actualización de 2022 introduce mejoras en la evaluación de riesgos, el fortalecimiento de controles de seguridad y una mayor alineación con enfoques de resiliencia organizacional.

El modelo está basado en un enfoque racional para su desempeño y su perfeccionamiento en el tiempo. Primero se exige que el modelo siga una serie de prerrequisitos para que se establezca, a través de la fase denominada "Planear". Luego de establecido el modelo, se implementa y opera, siguiendo los lineamientos de la fase "Hacer". Luego que el modelo se ha implantado y está funcionando, se debe monitorear y revisar durante la fase "Revisar". En la figura N° 5, se ofrece una imagen ilustrativa de los pasos de la rueda de Deming.

Figura N° 6

Rueda de Deming

Fuente: Imagen tomada de NQA (2024).

De acuerdo con la figura anterior, se infiere que la seguridad de la información debe establecer procesos concatenados y dinámicos, mediante una estructura cíclica, que permite gestionar de forma estratégica los riesgos y optimizar la protección digital. Estos protocolos de acción convierten al proceso en una metodología flexible y adaptativa, dando la oportunidad a la empresa, para mantenerse a la vanguardia, en la detección, resistencia y solución de cualquier ataque interno o externo, de las bases de datos.

La estandarización bajo ISO/IEC 27001:2022 implica la adopción de metodologías y procedimientos que unifiquen la gestión de seguridad en distintos entornos. Algunos principios fundamentales incluyen:

1. **Enfoque basado en riesgos:** Se priorizan las amenazas más relevantes según su impacto en los activos de información.
2. **Gestión documental clara:** Se exige la creación de políticas de seguridad bien definidas, con procedimientos de acceso, cifrado y recuperación de datos.
3. **Cultura organizacional de seguridad:** La norma enfatiza la importancia de formar y concienciar a los empleados sobre ciberseguridad, promoviendo buenas prácticas y reduciendo riesgos derivados de errores humanos.

Norma ISO/IEC 27002:2022

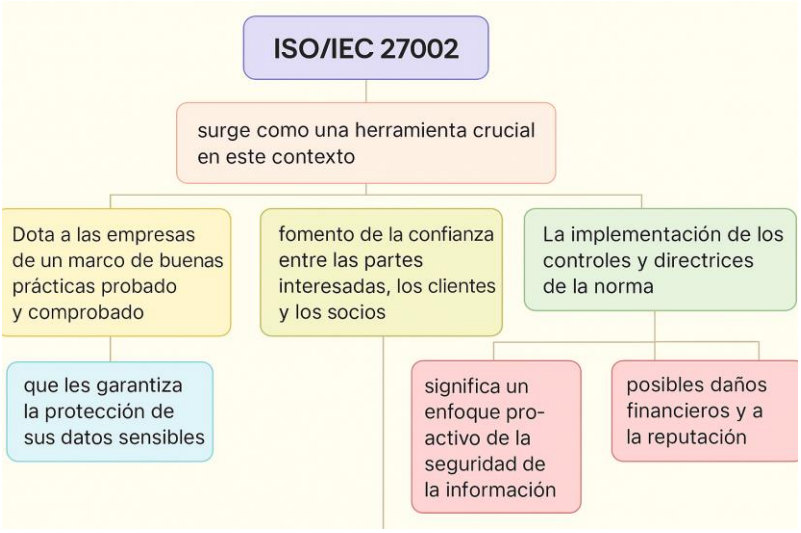
Al igual que la Norma ISO/IEC 27001, esta se convierte en un pilar fundamental para el establecimiento de la seguridad informática. Se estructura mediante reglas y técnicas, pero desde un enfoque de guía estratégica. Su finalidad es colaborar con las organizaciones, para mantener una protección eficiente de sus archivos digitales, de forma actualizada y respondiendo a los

diferentes tipos de ataque cibernéticos que surgen y modifican de forma divergente. De acuerdo con Internacional Standard (ISO) (2022), “ISO/IEC 27002 es una norma internacional que brinda orientación a las organizaciones que desean establecer, implantar y mejorar un sistema de gestión de seguridad de la información (SGSI) centrado en la ciberseguridad” (párr.),

En concordancia con lo citado, esta norma ofrece la oportunidad de mejoras continuas en el sistema informático de las empresas, ofreciendo detalles puntuales sobre la aplicación de controles dentro de la efectividad. En el contexto de globalización, la información de datos se convierte en el activo más importante de una empresa. Para garantizar su confidencialidad, integridad y disponibilidad, se recurre a la aplicación de esta norma. En la figura N° 6, se muestran las bondades y aportes de esta normativa.

Figura N 7.

Aportes de la Norma ISO/IEC 27002:2022



Fuente: Elaboración propia, datos tomados de ISO (2022)

De acuerdo con la imagen anterior, se denota la relevancia de la implementación de esta norma, para la mitigación de riesgos, asociados a ciberataques que puedan causar, fuga de información y accesos no autorizados. También le ofrece a la organización, una imagen de seguridad y solidez en el manejo y resguardo de la información, generando confianza entre los interconectados la gestión empresarial.

En un mundo divergente y evolucionado, la normativa ha adquirido el compromiso de renovar sus estructuras, en el año 2022, se optimiza para reducir el número de controles, cifrándose en:

1. **Controles organizacionales**: Definen políticas, roles y estrategias de seguridad.
2. **Controles de personas**: Enfatizan la formación y concienciación del personal.
3. **Controles físicos**: Protegen instalaciones y dispositivos contra accesos no autorizados.
4. **Controles tecnológicos**: Aseguran la seguridad de redes, sistemas y datos.

Sin embargo, estos controles no son fijos y estáticos, sino flexibles que se adaptan a las necesidades específicas de cada organización. Impulsa una defensa proactiva de la información, desde una visión de competitividad. Su protección no solo se centra en datos, sino que impulsa la resiliencia constante de la organización, en el campo de la seguridad de los datos inherentes con su gestión. De acuerdo con Internacional Standard (2022) se puede reconocer las características más sobresalientes de esta normativa que se exponen a continuación:

1. **Marco global de seguridad**: proporciona un conjunto detallado de directrices y buenas prácticas que abarcan varias dimensiones de la seguridad de la información.
2. **Gestión de riesgos**: permite a las organizaciones identificar, evaluar y gestionar eficazmente los riesgos para la seguridad de la información.
3. **Mayor confianza de las partes interesadas**: demuestra el compromiso de proteger los datos sensibles, lo que refuerza la credibilidad de la organización.
4. **Cumplimiento de la normativa**: asiste en el cumplimiento de diversos mandatos legales, contractuales y reglamentarios en materia de protección de datos.
5. **Resistencia operacional**: reduce la probabilidad de que se produzcan incidentes de seguridad que puedan trastocar las operaciones de la empresa.

6. **Ventaja competitiva**: en un mercado impulsado por los datos, contar con una sólida postura de seguridad de la información puede diferenciar a una organización de sus competidores.
7. **La norma incluye:** un gran abanico de temas de seguridad de la información, incluidos los relacionados con amenazas y vulnerabilidades de ciberseguridad.

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En la era de la digitalización, se debe reconocer la creciente oleada de riesgos de seguridad emergentes a consecuencia de la expansión e innovación tecnológica, en el área de la información y comunicación. Se recalca la importancia del cúmulo de datos en una empresa, como su activo principal, que dirige la toma de decisiones acertadas para la permanencia, eficiencia y calidad de los servicios que brinde la organización.

Partiendo de estas premisas, se hace necesario, establecer, renovar y mantener un sistema de gestión de seguridad de la información, para garantizar niveles adecuados de integridad, confidencialidad y disponibilidad de los activos informacionales. Las estrategias para la implementación de estas barreras protectoras requieren metodologías actualizadas, enfocadas a identificar, evaluar y abordar los riesgos asociados con los sistemas informáticos. De acuerdo con lo expuesto por El CNSD (2024),

> Una buena Gestión de Riesgos de Seguridad de la Información nos previene de:
>
> Amenazas Externas: Incluyen actores malintencionados como hackers, grupos de cibercriminales y estados-nación que buscan explotar las vulnerabilidades de la organización.
>
> Amenazas Internas: Empleados malintencionados o negligentes que pueden comprometer la seguridad de la información a través de acciones intencionadas o accidentales.
>
> Errores Humanos: Configuraciones incorrectas, envío de datos sensibles a destinatarios erróneos y fallos en el seguimiento de los protocolos de seguridad establecidos.

Vulnerabilidades Tecnológicas: Fallos en el software, hardware o infraestructura que pueden ser explotados por atacantes para comprometer los sistemas.

Eventos Naturales: Desastres naturales como terremotos, inundaciones y huracanes que pueden dañar la infraestructura de información y causar interrupciones operativas. (p. 4).

Lo expuesto en la cita anterior, demuestra la importancia de aplicar metodologías que permitan la gestión del riesgo en la información, desde una zona de seguridad y de prevención, para garantizar a la dinámica empresarial, la solidez en sus funciones y brindarle un escudo de confiabilidad y excelencia.

La gestión del riesgo en la seguridad de la información minimiza el impacto de amenazas y vulnerabilidades que puedan atacar el respaldo informativo que maneja la empresa. Se debe asegurar, la eficacia de la metodología aplicada, de forma que permita organizar, identificar, evaluar y mitigar de forma preventiva, los posibles ataques cibernéticos que paralicen la operación de la gestión empresarial. El CNSD (2024), apunta las siguientes razones de peso:

1. **Protección de Activos de Información**: La gestión de riesgos asegura que los activos críticos de información estén protegidos contra amenazas internas y externas. Esto incluye proteger la confidencialidad, integridad y disponibilidad de los datos.
2. **Cumplimiento Normativo:** Muchas industrias y sectores están sujetos a regulaciones estrictas sobre la gestión de información. Una gestión de riesgos efectiva ayuda a garantizar el cumplimiento de estas normativas y evita sanciones legales y financieras.
3. **Reducción de Vulnerabilidades**: Al identificar y evaluar las vulnerabilidades, las organizaciones pueden implementar controles para reducir el riesgo de explotación. Esto incluye la implementación de parches de seguridad, la mejora de la configuración de sistemas y la capacitación del personal.
4. **Mejora de la Resiliencia Organizacional**: La capacidad de una organización para resistir y recuperarse de eventos adversos se fortalece mediante la gestión de riesgos. Las organizaciones pueden desarrollar planes de contingencia y recuperación que les permitan continuar operando incluso en situaciones críticas.

5. **Toma de Decisiones Informadas**: La gestión de riesgos proporciona a la alta dirección una comprensión clara de los riesgos a los que se enfrenta la organización. Esto permite tomar decisiones informadas sobre la asignación de recursos y la priorización de medidas de seguridad. (p. 5).

Por tanto, la metodología implementada para estructurar barreras de protección sobre la información que maneja la empresa, contra ataques cibernéticos, requiere de estrategias que permitan identificar, las amenazas, evaluar vulnerabilidades y la toma de decisiones inteligentes para la aplicación de controles seguros y que permitan estar en constante renovación y actualizaciones de acuerdo con las amenazas emergentes.

Mejora Continua del Sistema de Gestión de Seguridad de la Información

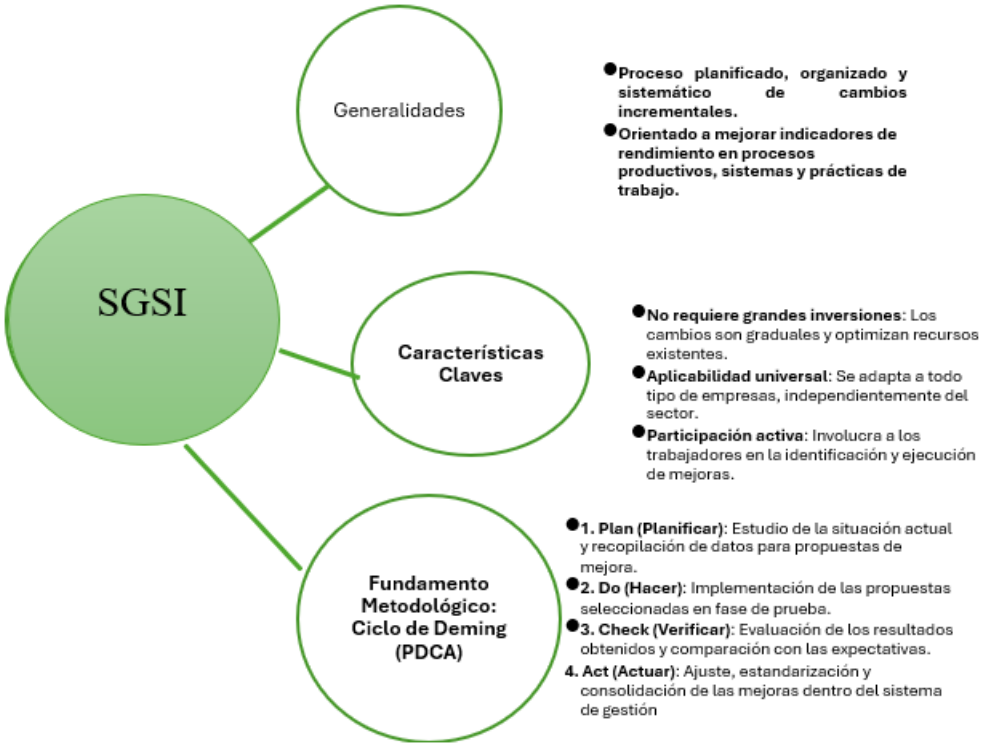
La mejora continua en el Sistema de Gestión de Seguridad de la Información (SGSI) es una necesidad técnica y un compromiso estratégico con la protección de los activos digitales y la confianza de quienes interactúan con la organización. En un entorno donde los riesgos evolucionan constantemente, adoptar un enfoque dinámico y proactivo permite fortalecer la resiliencia ante amenazas emergentes. “La mejora continua es una de las herramientas básicas para aumentar la competitividad en las organizaciones” (García y Prado , 2003, mencionado en Marín et al, 2014)

De acuerdo con la cita anterior, la (SGSI), es un proceso no se limita a implementar controles estáticos, sino que requiere una evaluación periódica de vulnerabilidades, una adaptación ágil a nuevas normativas y una cultura organizacional centrada en la seguridad. Se rige bajo los estándares internacionales existentes, entre los que se contempla, ISO/IEC 2700, definiendo los requisitos para implementar y mantener mejoras en el sistema de gestión de seguridad de la información, para la protección de datos sensibles.

También se recurre a la ISO/IEC 27002, normativa que establece un cumulo de buenas prácticas para el control y robustecimiento de la gestión de riesgos. En la figura N° 8, se presentan de forma resumida, las características de este proceso, para una visualización más comprensiva de la información.

Figura N° 8

Características de (SGSI)



Fuente: Elaboración propia (2024)

Según la imagen proporcionada, se observa la estructura metodológica, para la aplicación de la SGSI en las empresas, para poder disponer de todas sus bondades para asegurar la evolución progresiva y sostenida en la gestión del riesgo de la información, reforzando la seguridad organizacional sin generar grandes costos.

La mejora continua es, en esencia, la capacidad de aprender de cada incidente, fortalecer estrategias de prevención y perfeccionar la gestión de riesgos en un ciclo permanente de evaluación y ajuste. No se trata solo de reaccionar ante las amenazas, sino de anticiparse a ellas, consolidando un sistema que no solo proteja la información, sino que también genere confianza y estabilidad en el entorno digital.

Controles específicos para el acceso y la protección de datos

Este tipo de controles, se atañen a dinámica evolutiva de la tecnología, que no solo facilita la información, sino que puede convertirse en una amenaza cibernética que la dañe y le proporcione otro uso inadecuado. Entonces, el acceso a los datos debe basarse en el principio de mínimos privilegios. De acuerdo con Palo Alto Networks (s.f), " El principio del mínimo privilegio (PoLP) es un concepto relacionado con la seguridad de la información según el cual un usuario o entidad solo debe tener acceso a los datos, los recursos y las aplicaciones que necesite para llevar a cabo una determinada tarea" (párr. 1).

Entonces, este constructo, impregna la gestión de seguridad de la información, para proteger el activo de las empresas a ciberataques que afecten su operación. La pérdida económica, los robos de datos, el jaqueo de operaciones, por medio de ransomware, malware u otras amenazas, deben prevenirse con la implementación de normas de seguridad que permitan el acceso seguro y controlado, a la base de datos de la organización. Se exponen los principales controladores de acceso, según lo recomendado por el Instituto Nacional de Ciberseguridad (INCIBE), (2019), se exponen mecanismos para la protección de acceso a los datos.

1. **Autenticación de doble factor, RADIUS e IDS /IPS como mecanismos de protección de datos**

El fortalecimiento de la seguridad en los sistemas de información requiere la implementación de mecanismos robustos y complementarios. Uno de ellos es la autenticación de doble factor, que añade una capa adicional al tradicional ingreso con usuario y contraseña. Este segundo factor puede basarse en algo que el usuario posee (como un token o tarjeta inteligente) o algo que es inherente a él (como una huella dactilar). De esta forma, incluso si las credenciales

iniciales son comprometidas, el acceso no será posible sin la segunda verificación, aumentando significativamente la protección contra accesos no autorizados.

Por otro lado, el protocolo RADIUS (Remote Authentication Dial-In User Service) constituye una herramienta fundamental dentro de los sistemas AAA (Autenticación, Autorización y Contabilización). Este protocolo permite centralizar la gestión de acceso a los recursos de red, funcionando mediante la interacción entre un cliente, que transmite las credenciales del usuario, y un servidor, que valida dicha información y define los permisos correspondientes. Además, el servidor puede registrar datos relevantes sobre la sesión del usuario, facilitando el control y la trazabilidad.

Finalmente, los sistemas **IDS (Intrusion Detection System)** y **IPS (Intrusion Prevention System)** contribuyen al monitoreo y defensa de la infraestructura tecnológica. Mientras el IDS se enfoca en identificar comportamientos anómalos o configuraciones inusuales, notificando al personal de seguridad, el IPS va un paso más allá, al actuar directamente para prevenir posibles intrusiones. Estos sistemas son esenciales para anticiparse a amenazas y preservar la integridad de los datos y servicios digitales.

1. **Autenticación multifactor (MFA)**: Un requisito que combina contraseñas, códigos temporales, biometría o dispositivos de seguridad para garantizar que solo los usuarios autorizados ingresen.
2. **Gestión de identidades y accesos (IAM)**: Sistemas que verifican permisos de acceso y aseguran que las credenciales de los usuarios se actualicen de manera adecuada.
3. **Control de roles y permisos**: Definir perfiles de acceso diferenciados para empleados según sus funciones, evitando accesos innecesarios a datos sensibles.

La protección de datos permite asegurar la integridad y confidencialidad de estos, no es suficiente, regular el acceso a la información, sino que se necesita un plus, para el blindaje de la esta, que la protegen contra posibles amenazas. Estas medidas pueden ser:

1. **Cifrado de datos**: Aplicar algoritmos de cifrado tanto en tránsito como en almacenamiento impide que la información sea legible en caso de filtraciones.
2. **Monitoreo y auditoría**: Registrar cada intento de acceso y actividad permite identificar irregularidades en tiempo real.
3. **Políticas de seguridad y educación digital**: Capacitar a los usuarios sobre buenas prácticas reduce el riesgo de ataques por ingeniería social.

La clasificación de los activos de información, en el ámbito de la seguridad de la información, consiste en organizar los datos según su nivel de sensibilidad y el impacto que tendría para la organización su divulgación, alteración o destrucción no autorizada. Este proceso permite establecer los controles de seguridad básicos más adecuados para proteger dichos activos. Toda información puede ser categorizada en uno de los siguientes tres niveles de sensibilidad:

- **Nivel 1:** Información pública
- **Nivel 2:** Información interna
- **Nivel 3:** Información restringida

Términos básicos

1. **Ataque:** ISO 27001 describe el ataque como un intento de explotar vulnerabilidades para comprometer la confidencialidad, integridad o disponibilidad de un activo *(*Norma ISO/IEC 27001, 2022)
2. **Amenaza**

   Se define como cualquier incidente o condición que pueda comprometer la confidencialidad, integridad y disponibilidad de un activo (Norma ISO/IEC 27001, 2022)
3. **Análisis de riesgos:** ISO 31000 lo describe como un proceso sistemático e interactivo para analizar incertidumbres, fuentes de riesgo, consecuencias y probabilidad. (ISO 31000, 2018).
4. **Confidencialidad:** Según ISO/IEC 27000:2018, es la propiedad de que la información no sea divulgada a personas, entidades o procesos no autorizados *(*ISO/IEC 27000:201).
5. **Consecuencia:** En ISO 31000 se entiende como el resultado de un evento que afecta a los objetivos de la organización, (ISO 31000, 2018). **Contexto Externo**: Comprende los factores externos—económicos, sociales, legales, tecnológicos—que influyen en el riesgo *(ISO* 31000, 2018).
6. **Contexto interno**: Se refiere a factores internos como cultura, estructura, políticas y procesos organizacionales (ISO *31000, 2018).*
7. **Control:** Medida que modifica o regula el riesgo, como políticas, procesos, tecnología o estructuras organizacionales *(ISO* 31000, 2018 e ISO 27001, 2022)
8. **Disponibilidad:** Propiedad de estar accesible y utilizable cuando sea necesario, según ISO 27000:2018 (*ISO*/IEC 27000:2018).

9. **Enunciado de aplicabilidad**: Documento que define los controles aplicables al SGSI según el Anexo A de ISO 27001. *(ISO*/IEC 27001, cláusula 6.1.3, 2022).
10. **Evento:** Una ocurrencia o cambio en un conjunto de circunstancias, según ISO 31000. (ISO 31000, 2018).
11. **Gestión de riesgos**: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo, según ISO 31000 (ISO 31000, 2018).
12. **Gobierno de la seguridad de la información:** Sistema mediante el cual se dirigen y controlan las actividades de seguridad de la información, como define ISO 27001 *(*ISO/IEC 27001, 2022).
13. **Integridad:** Propiedad que asegura la exactitud y completitud de los activos, según ISO 27000:2018 (*ISO/IEC 27000:2018).*
14. **Ley de protección de Datos: Normativa**, como GDPR (UE 2018), que garantiza el derecho a la protección de datos personales. (Reglamento General de Protección de Datos, UE, 2018).

CAPÍTULO III: MARCO METODOLÓGICO

En este capítulo se describen las decisiones estratégicas y los pasos que se llevan a cabo para la recolección y el análisis de la información. Se presentan diversas perspectivas metodológicas que permiten orientar de manera sistemática el proceso investigativo. Este desarrollo metodológico se fundamenta en la definición propuesta por Balestrini (2006), quien señala que el marco metodológico "se refiere al conjunto de métodos, técnicas y protocolos instrumentales que permitirán obtener la información requerida en la investigación propuesta" (p. 33).

En consecuencia, se describen los procesos esenciales que permiten visualizar de manera estructurada la ruta para la construcción del conocimiento. Se precisan el enfoque metodológico adoptado, el tipo de estudio, el diseño de investigación, la definición y operacionalización de las variables, la caracterización de los participantes, las fuentes consultadas, los instrumentos aplicados y el tratamiento de los datos obtenidos

TIPO Y ENFOQUE DE LA INVESTIGACIÓN

Tipo de investigación

La determinación del tipo de investigación constituye un elemento esencial en la construcción del marco metodológico, ya que permite establecer la orientación epistemológica y las estrategias analíticas que guiarán el desarrollo del estudio. De acuerdo con la clasificación propuesta por la Universidad Hispanoamericana (2022), se identifican cuatro tipos fundamentales de investigación: básica, aplicada, analítica y de campo.

1. **La investigación básica:** tiene como propósito la ampliación del conocimiento científico, mediante la profundización en teorías existentes y el análisis conceptual de principios fundamentales.
2. **La investigación aplicada**: se enfoca en la utilización del conocimiento teórico en contextos específicos, con el objetivo de generar soluciones prácticas que respondan a necesidades concretas.
3. **La investigación analítica**: se caracteriza por el estudio comparativo de variables entre diferentes grupos o condiciones, lo que permite establecer relaciones significativas, validar hipótesis y formular nuevos modelos explicativos.
4. **La investigación de campo**: se desarrolla directamente en el entorno donde ocurre el fenómeno de estudio, permitiendo la recolección de información empírica de forma directa y contextualizada (Universidad Hispanoamericana, 2022, p. 20).

En el contexto de esta investigación, cuyo propósito es la implementación de mejoras en seguridad de la información alineado a ISO 27001:27002 para la Mitigación de Riesgos en la Empresa SISLOCAR Caldera S. A, se adopta un enfoque metodológico de tipo aplicado. Esto se debe a que se pretende trasladar el conocimiento teórico a la práctica organizacional, a fin de fortalecer la infraestructura de seguridad de la información y optimizar la confianza de los clientes mediante acciones concretas.

De manera complementaria, el estudio incorpora un componente analítico, al requerir la evaluación detallada de políticas, prácticas y datos internos de la organización, para identificar brechas, riesgos y oportunidades de mejora con relación al marco normativo, mediante una rigurosa exploración documental.

Asimismo, se integra un enfoque de campo, dado que la recolección de datos se realiza directamente en el contexto operativo de la empresa, mediante la interacción con el personal y la observación de las condiciones reales del entorno, lo que permite fundamentar las propuestas de intervención con evidencia empírica contextualizada

Enfoque de la Investigación

El enfoque de investigación representa la perspectiva metodológica desde la cual se abordan las variables y fenómenos objeto de estudio. En términos generales, se reconocen dos enfoques predominantes: el cuantitativo y el cualitativo (Universidad Hispanoamericana, 2022, p. 21).

El enfoque cuantitativo se caracteriza por la utilización de datos numéricos para describir, explicar y predecir fenómenos, haciendo uso de herramientas estadísticas para contrastar hipótesis y establecer relaciones entre variables. Por el contrario, el enfoque cualitativo privilegia la interpretación profunda de los significados, percepciones y experiencias humanas, centrándose en el análisis detallado de los contextos y en la comprensión de la realidad desde la perspectiva de los sujetos involucrados (Universidad Hispanoamericana, 2022, p. 21).

No obstante, en investigaciones de mayor complejidad, resulta pertinente adoptar un enfoque mixto, el cual combina estrategias cuantitativas y cualitativas con el fin de ofrecer una visión más amplia e integrada del objeto de estudio. De acuerdo con lo expresado por Hernández y Mendoza, (2018),

> Los métodos mixtos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos,

así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada (meta inferencias) y lograr un mayor entendimiento del fenómeno bajo estudio. (p. 651).

La definición brindada por los autores de la cita, destacan que los métodos mixtos no se limitan a combinar técnicas de enfoques cuantitativos y cualitativos, sino que, conforman un proceso riguroso y articulado, en los procesos de recolección y análisis de datos, desde la coherencia. Al referirse a la meta inferencias, logran establecer que el complemento de los modelos, permiten una comprensión profunda y completa del fenómeno, enriqueciendo los resultados finales.

En el caso de la presente investigación, por su naturaleza, se adopta un **e**nfoque mixto**.** La integración de técnicas cuantitativas permitirá recopilar y analizar datos objetivos sobre los niveles actuales de seguridad, facilitando la formulación y validación de hipótesis relacionadas con el desempeño del sistema. Paralelamente, se recurrirá a métodos cualitativos para explorar las percepciones, actitudes y prácticas del personal vinculado al proceso, lo cual permitirá comprender en profundidad los factores humanos y organizacionales que influyen en la seguridad de la información. Esta combinación metodológica favorecerá una comprensión holística del fenómeno, garantizando que tanto los aspectos medibles como aquellos de naturaleza interpretativa sean considerados para una implementación de mejoras en Seguridad de la Información, alineado a ISO 27001:27002 para la Mitigación de Riesgos en el contexto empresarial estudiado.

FUENTES Y SUJETOS DE INFORMACIÓN

La identificación de las fuentes y los sujetos de información constituye un componente esencial en el diseño metodológico, ya que permite delimitar con precisión el origen y la naturaleza de los datos que sustentan el análisis. Para conceptualizarlas, se recurre a Jaén (2019), quien acota, "En su acepción más amplia y genérica es todo objeto que contenga, produzca, proporcione o transfiera información" (p. 11).

Es destacable, que el autor anterior, separa las fuentes de información en tres categorías, la primera los objetos que puedan brindar datos relevantes, la segunda, el sujeto, que es el poseedor de conocimientos necesarios para la indagación y el tercero, la información como tal, compuesta por contenidos que permitan la ampliación del conocimiento.

Fuentes primarias

Hacen referencia los datos que se obtienen directamente de los sujetos involucrados, mediante la aplicación de instrumentos a actores clave involucrados en la gestión de la seguridad de la información dentro de la organización objeto de estudio. Estos aportes, contienen información genuina de primera mano, que no han sido interpretados ni evaluados por otras fuentes. La Universidad Hispanoamericana, (2022), las define como,

> Fuentes Primarias: en ellas se publican información precisa y directa sobre los resultados originales de la investigación. Están constituidas por las revistas de investigación y las patentes, además de investigaciones en primera instancia, resultados de entrevistas, encuestas, estudios, entre otros. (p. 22).

De acuerdo con lo expresado en la cita anterior, para el caso concreto de esta indagación, se recurre al personal del área administrativa, tecnología de la información y de seguridad de esta, dentro de la empresa. También la documentación existente, referente a la temática en estudio.

Entonces, se justifica la selección de las fuentes primarias para la investigacion, al responder de forma directa, a la obtención de la información que brinda cuerpo a la indagación, mediante una verisimilitud del problema en estudio, Los datos que se inquieren, se caracterizan por ser contextualizados y desde las perspectivas de los actores involucrados.

Fuentes Secundarias

Se derivan del análisis de documentos institucionales, normativas vigentes, registros técnicos y otros insumos que permiten contextualizar el fenómeno investigado. Desempeñan un papel crucial en la construcción de los nuevos conocimientos, ofreciendo un respaldo teórico. Departamento de Química Orgánica, Universidad Granada, (2004) mencionado en Universidad Hispanoamericana, (2022) explicita,

> Comprenden todas las publicaciones que recojan material que ha sido previamente publicado en fuentes primarias, es decir, resúmenes, revisiones, monografías, tratados específicos, tratados generales y libros de texto, entre otras. Son publicaciones que han sido validados sus conceptos e información por la comunidad científica y sociedad en general. (p. 22).

De acuerdo con la cita anterior, estas fuentes, que ya han sido gestionadas, deben ofrecer confiabilidad en cuanto a la información brindada, por tanto, se recurre a, artículos científicos, tesis, libros y estudios previos que abordan temáticas vinculadas a los Sistemas de Gestión de

Seguridad de la Información (SGSI), así como aspectos críticos de la ciberseguridad en entornos empresariales.

También se toman como referentes, Publicaciones técnicas y profesionales, estándares y normativas internacionales, particularmente el estándar ISO/IEC 27001:2022 y el ISO/IEC 27002:2022, los cuales constituyen la base normativa para el diseño, una propuesta de Implementación de Mejoras en Seguridad de la Información Alineado a ISO 27001:27002 para la Mitigación de Riesgos en la Empresa SISLOCAR Caldera.

Sujetos de información

La identificación de los sujetos de información se realiza considerando su implicación directa en la gestión, operación y uso de los sistemas de información de la empresa. Su participación es clave para obtener datos empíricos relevantes y confiables que permitan una comprensión integral del contexto organizacional.

Los participantes serán seleccionados según criterios de pertinencia funcional y conocimiento operativo sobre los procesos asociados a la seguridad de la información. En el caso específico del estudio en SISLOCAR Caldera S.A., se ha definido una población compuesta por personal técnico, operativo y administrativo, cuya experiencia y responsabilidades aportan insumos críticos para el diagnóstico y fortalecimiento del SGSI. La selección se fundamenta en su capacidad para ofrecer perspectivas complementarias que favorezcan la triangulación de datos y la validez del análisis. En la tabla 1, se categoriza los diferentes estratos de los sujetos de información.

Tabla 1. Perfil de los sujetos de información

Puesto Laboral	Cantidad	Profesión	Experiencia	Relación con el Tema
Director Ejecutivo	1	Cyber Security	Más de 20 años	Representante de la Alta Dirección de SISLOCAR Caldera S. A
Encargado de Seguridad de la Información	2	Cyber Security	Más de 15 años	Encargado de Seguridad de la Información en SISLOCAR Caldera S. A
Personal Operativo con acceso a sistemas	7	Logística	Más de 15 años	Proveen información sobre prácticas reales, vulnerabilidades cotidianas y cultura organizacional en SISLOCAR Caldera S. A

Fuente: Elaboración del investigador.

La información brindada en la tabla anterior sintetiza el perfil de los sujetos de información seleccionados para el aporte de los datos necesarios para la indagación, se considera su cargo, formación profesional, experiencia y vinculación directa con el problema en estudio, en el contexto de la empresa SISLOCAR Caldera S.A.

TÉCNICAS Y HERRAMIENTAS DE RECOLECCIÓN DE DATOS

Con el propósito de responder adecuadamente a las preguntas de investigación y alcanzar los objetivos planteados, se optará por una combinación estratégica de técnicas de recolección de datos, seleccionadas por su capacidad para proporcionar información confiable, válida y contextualizada sobre los aspectos más relevantes de la seguridad de la información en la empresa SISLOCAR Caldera S.A. El uso articulado de estas técnicas permite obtener un panorama integral del estado actual de la organización frente a los requerimientos de los estándares ISO/IEC 27001 y 27002. A continuación, se detalla cada una de las técnicas seleccionadas:

Matriz de Riesgo

La matriz de riesgo se convierte en una herramienta fundamental para diagnosticar la existencia de inseguridades en la estabilidad de la información. De acuerdo con su estructura, identifica, clasifica y evalúa las amenazas y vulnerabilidades existentes. Esta indagación se propone, identificar los principales riesgos de seguridad de la información que enfrenta la empresa SISLOCAR Caldera S.A., mediante la evaluación de sus procesos operativos y del manejo de información confidencial, con el propósito de establecer un diagnóstico que sirva de base para la implementación de controles alineados con los estándares ISO/IEC 27001 y 27002, esta técnica logra recopilar los datos necesarios, para la evaluación operativa de la organización.

Desde su estructura, se logra relacionar los activos de información, con las amenazas y vulnerabilidades existentes. Según Pirani Risk, (2024), el análisis y evaluación de riesgos basado en activos permite a las organizaciones identificar claramente todas aquellas amenazas que pueden impactar negativamente en los objetivos de seguridad, así como en la imagen y reputación de la empresa" (párr. 3). Entonces, desde esta perspectiva, se aplica esta herramienta, alineada con las normas ISO/IEC 27001 y 272002, para la recopilación de los datos necesarios para el diagnóstico.

Análisis de Brechas (Gap Analysis)

Este instrumento de Analisis de Brechas, se convierte en una herramienta estratégica, útil para comparar el estado actual de la empresa con su estado deseado, a la luz de las Normas ISO/IEC 27001 y 272002. Permite identificar aquellas áreas que requieren mejoras. Según Wright (2022) “El análisis GAP es una gran herramienta de análisis estratégico que nos ofrece un marco general

para definir no sólo dónde nos encontramos actualmente sino -más importante- dónde queremos estar y cómo vamos a llegar" (párr. 1).

Concordando con lo citado, se selecciona como herramienta idónea, para el análisis estratégico, para detectar falencias en ciertas áreas que requieran acciones correctivas, en los mecanismos actuales de control de accesos y protección de datos sensibles, mediante la revisión de políticas internas, tecnologías empleadas y prácticas vigentes en la empresa. De acuerdo con la guía brindada por Cobee Team, (2022), el análisis se desarrolla en fases, que se exponen a continuación.

1. **Comparación con ISO/IEC 27001 y 27002**
    a. Identificación de requisitos fundamentales y controles de seguridad.
    b. Análisis de brechas utilizando una matriz de cumplimiento.
    c. Evaluación del nivel de madurez de cada control de seguridad.
2. **Identificación de Áreas de Mejora**
    a. Priorización de brechas según impacto y criticidad.
    b. Identificación de recursos necesarios para el cumplimiento.
    c. Evaluación de riesgos asociados a las brechas detectadas.

Tabla 2. Matriz detección de brechas

Control de Seguridad	Estado Actual	Requisito ISO/IEC	Brecha Detectada	Acción Correctiva	Nivel de Prioridad
Gestión de accesos		Control 9.1 (ISO 27002)			
Protección de activos		Control 8.2 (ISO 27002)			
Gestión de incidentes		Control 16.1 (ISO 27002)			Alta

Fuente: Elaboración propia.

Entrevista Estructurada

Se implementa una entrevista estructurada dirigidas a actores clave dentro de la empresa, como el director ejecutivo, el Encargado de Seguridad de la Información y miembros del personal operativo con acceso a sistemas críticos. Según Folgueiras (2016)

> En la entrevista estructurada se decide de antemano que tipo de información se quiere y en base a ello se establece un guion de entrevista fijo y secuencial. El entrevistador sigue el orden marcado y las preguntas están pensadas para ser contestadas brevemente. El entrevistado debe acotarse a este guion preestablecido a priori. (p. 3).

En concordancia con lo expuesto en la cita, la herramienta se elabora a través de un guion, con preguntas previamente definidas, tanto cerradas como abiertas, lo que garantiza uniformidad en la aplicación y riqueza en las respuestas. Esta técnica permite:

1. Reconocer los riesgos cibernéticos más significativos desde el punto de vista de quienes lideran o ejecutan funciones estratégicas dentro de la organización.

2. Obtener percepciones institucionales en torno a las políticas actuales de seguridad, la cultura organizacional y el nivel de concienciación sobre la protección de información sensible.

Este instrumento es clave para la recolección de datos desde la experiencia de los responsables de los procesos operativos, para la identificación de prácticas inseguras y áreas de riesgo en la organización. Para alcanzar el objetivo en forma holística, recurre a una entrevista estructurada, para profundizar en riesgos específicos, con preguntas cerradas y abiertas, para obtener datos cuantitativos y cualitativos, necesarios para el estudio. En la tabla 3, se ofrecen los detalles de su estructura.

Tabla 3. Entrevista estructurada

Sección del cuestionario	**Objetivo**	**Descripción**
Datos Generales		
	Asegurar la inclusión del encuestado	Cualidades del entrevistado
Cuerpo del instrumento	Recolección de datos para el respaldo de cada variable en estudio.	4 ítems de respuesta abierta. 8 ítems de respuestas estructuradas

Fuente: Elaboración propia.

Análisis Documental

Este instrumento, permite examinar la documentación existente, para la revisión de políticas y normativas internas, sobre seguridad de la información, así como los procedimientos operativos y registros de incidentes previos, permitiendo identificar áreas vulnerables y patrones

de riesgo. También permite establecer relación, entre las propuestas de las normativas ISO/IEC 27001 y 27002 y las prácticas empresariales.

En relación con el diseño de la propuesta de mejoras del sistema de gestión de seguridad de la información, el análisis documental, relaciona las teorías expuestas en referentes internacionales, sobre las mejores prácticas, dándole credibilidad y viabilidad al modelo, alineado con los estándares relevantes. En la tabla 4, se presenta la matriz aplicable para este instrumento.

Tabla 4. Matriz análisis documental

Objetivo	Fuente documental	Criterios de análisis	Resultados esperados	Instrumentos de apoyo
Identificar los principales riesgos de seguridad de la información	Políticas internas de seguridad, procedimientos operativos, informes de auditoría, registros de incidentes previos.	Identificación de vulnerabilidades recurrentes, cumplimiento con estándares ISO/IEC 27001 y 27002, impacto en la operación.	Diagnóstico de riesgos y recomendaciones alineadas a normativas.	Matriz de riesgo, análisis de brechas (Gap Analysis), reporte de hallazgos.
Analizar las debilidades en los mecanismos actuales de control de accesos y protección de datos sensibles	Manuales de acceso, configuraciones de seguridad, logs de acceso, normativas internas sobre protección de datos.	Evaluación de la efectividad de los controles de acceso, detección de inconsistencias o prácticas obsoletas, análisis de cumplimiento.	Identificación de áreas de mejora en accesos y protección de datos sensibles.	Lista de verificación de controles de acceso, matriz de evaluación de seguridad, informe comparativo con estándares.
Diseñar una propuesta de mejora del sistema de gestión de seguridad de la información	Documentación de mejores prácticas, normativas ISO/IEC 27001 y 27002, informes de auditoría de referencia, estudios de casos sobre implementación de SGSI.	Comparación con estándares internacionales, viabilidad de implementación, impacto esperado en la reducción de riesgos.	Propuesta estructurada con controles específicos y estrategias de mitigación.	Matriz de mejoras del SGSI, cuestionario de evaluación de viabilidad, informe de alineación con normativas.

Fuente: Elaboración propia.

VARIABLES DE INVESTIGACIÓN

De acuerdo con la naturaleza del estudio, bajo un enfoque mixto, cuenta con variables y categorías de análisis, que emergen de los objetivos propuestos. De acuerdo con la Universidad Hispanoamericana (2022), mencionando a ORI,

> Las variables son nombres que damos a las variaciones que deseamos explicar. En un experimento, se denominan variables dependientes e independientes, respectivamente. Las variables son importantes de comprender pues son unidades básicas de información que se estudia e interpreta en una investigación. Los investigadores cuidadosamente analizan e interpretan los valores de cada variable para entender cómo se relacionan las cosas en un estudio descriptivo o lo que ha sucedido en un experimento. (p. 25).

A la luz de lo expuesto en la cita, las variables contienen las características que puedan causar variación dentro del estudio. Se convierten en propiedades del problema explorado, que pueden ser fluctuantes. Además, permiten la medición y la observación, para garantizar la validez de los resultados de la indagación. En este estudio, se cuenta con una variable, que emergen del objetivo cuantitativo y dos categorías de análisis, producto de los objetivos cualitativos. En la tabla 6, se define la variable de la investigación.

Tabla 5. Definición de la variable

Objetivo	Variables Asociadas	Descripción
Identificar los principales riesgos de seguridad de la información que enfrenta la empresa SISLOCAR Caldera S. A, mediante la evaluación de sus procesos operativos y del manejo de información confidencial, con el propósito de establecer un diagnóstico que sirva de base para la implementación de controles alineados con los estándares ISO/IEC 27001 y 27002.	**1** riesgos de seguridad de la información. 2. Procesos operativos. 3. Manejo de información confidencial, 4. Controles de seguridad alineados con ISO/IEC 27001 y 27002	Se busca identificar los riesgos más relevantes en la seguridad de la información de la empresa, evaluando sus procesos operativos y el manejo de datos sensibles. Esto permitirá establecer un diagnóstico detallado que sirva de base para la implementación de controles de seguridad alineados con los estándares internacionales ISO/IEC 27001 y 27002, garantizando la protección de los activos de información y la mitigación de amenazas.

Fuente: Elaboración propia (2025).

En cuanto a las categorías de análisis, estos elementos propios de la investigación con enfoque cualitativo permiten estructurar el estudio y definir qué es lo que se quiere investigar. Según Straus y Corbin, mencionados en Romero (2005), “Las categorías son conceptos derivados de los datos que representan fenómenos. Los fenómenos son ideas analíticas pertinentes que emergen de nuestros datos” (p. 5).

Por tanto, la cita hace énfasis en establecer una construcción conceptual de las categorías de análisis, para relacionarlas con el análisis sistemático y estructurado de los datos procedente, producto de ideas que emergen directamente de la información recaudada. En la tabla 7, se ofrece la definición de las categorías de análisis emergentes.

Tabla 6. Categorías de análisis

Objetivo	Categorías de análisis	Descripción
Analizar las debilidades en los mecanismos actuales de control de accesos y protección de datos sensibles, mediante la revisión de políticas internas, tecnologías empleadas y prácticas vigentes en la empresa, con el fin de orientar mejoras que reduzcan la exposición a riesgos cibernéticos.	1. **Políticas internas**: 2. **Tecnologías empleadas**: 3. **Prácticas vigentes.** 4. **Exposición a riesgos cibernéticos**:	Evaluación de normativas, procedimientos y cumplimiento organizacional en relación con el acceso y protección de datos. Revisión de herramientas y sistemas implementados para la gestión de accesos y protección de información sensible Análisis de metodologías operativas, roles y responsabilidades dentro del proceso de seguridad. Identificación de vulnerabilidades, amenazas y niveles de riesgo dentro del sistema actual
Objetivo	**Categorías de análisis**	**Descripción**
Diseñar una propuesta de mejora del sistema de gestión de seguridad de la información, basada en los lineamientos de las normas ISO/IEC 27001 y 27002, que incluya controles específicos para el acceso y la protección de datos, y que permita mitigar los riesgos de accesos no autorizados y la vulneración de información crítica.	**Normativas aplicables.** **Controles específicos.** **Implementación y gestión**: **Evaluación y mejora continua**	Principios y requisitos de las normas ISO/IEC 27001 y 27002 que guían la mejora. Identificación y selección de medidas de seguridad apropiadas para fortalecer el SGSI. Estrategias de adopción, capacitación y monitoreo de los controles propuestos. Mecanismos de retroalimentación y ajuste progresivo en el SGSI.

Fuente: Elaboración propia. (2025)

Las tablas anteriores, muestran la relación que mantienen los objetivos con sus respectivas variables o categorías de análisis, de acuerdo con su naturaleza metodológica, para una mayor comprensión, de los elementos explorados en el estudio y la producción de resultados finales de los nuevos conocimientos.

DISEÑO DE LA INVESTIGACIÓN

La naturaleza de este estudio se robustece con el enfoque mixto, que permite una visión integral del problema. Se busca analizar las debilidades actuales en los mecanismos de control de acceso y protección de datos, considerando políticas internas, tecnologías implementadas y prácticas operativas. También se propone diseñar una propuesta de mejora alineada con los estándares internacionales, específicamente ISO/IEC 27001 y 27002, incorporando controles precisos que fortalezcan el sistema de gestión de seguridad de la información. Según Trochim (2005), mencionado en Universidad Hispanoamericana (2022), el diseño de la investigación

> Es el pegamento que mantiene el proyecto de investigación cohesionado. Un diseño es utilizado para estructurar la investigación, para mostrar cómo todas las partes principales del proyecto de investigación funcionan en conjunto con el objetivo de responder a las preguntas centrales de la investigación. (p. 25).

Concordando con lo expresado en la cita anterior, el diseño de la investigacion se convierte en el mapa estructural que marca la ruta de la indagación, estableciendo las diferentes etapas desarrolladas y concatenando cada acción para mostrar la coherencia y alineación de las acciones en el proceso. En la figura 9, se muestra el diseño de esta indagación. Describiendo el proceso

que involucra el proyecto en SISLOCAR Caldera S. A, delineando las fases y etapas, las técnicas y herramientas aplicadas en cada una, y los resultados anticipados.

Figura N° 9. Diseño de la investigación

Fuente: Elaboración propia (2025).

MATRIZ DE COHERENCIA

En esta sección, se propone una matriz de coherencia que articula los diferentes elementos calves que integran el diseño de la investigación. Se alinean de forma horizontal, los objetivos del estudio, los entregables esperados, los instrumentos metodológicos utilizados y su relación con el sustrato teórico.

Esta matriz funciona como un organizador lógico y visual, que permite la comprensión con mayor claridad, sobre los procesos y su ligamen de orden lógica, en las acciones indagativa, por

tanto, no solo sirve como planificador, sino que demuestra la coherencia interna de la investigación. En la tabla 9, se muestra la matriz a la que se hace referencia.

Tabla 7. Matriz de coherencia

Objetivo	Entregable	Fase, parte o etapa de la metodología del proyecto que posibilita la realización del entregable	Técnicas/métodos de recolección de la información	Instrumentos	Temas relacionados para marco teórico
Identificar los principales riesgos de seguridad de la información que enfrenta la empresa SISLOCAR Caldera S.A., mediante la evaluación de sus procesos operativos y del manejo de información confidencial, con el propósito de establecer un diagnóstico que sirva de base para la implementación de controles alineados con los estándares ISO/IEC 27001 y 27002.	Informe de estado actual de los procesos operativos para la detección de los principales riesgos de seguridad de la información, que identifica áreas de mejoras, alineados con los estándares ISO/IEC 27001 y 27002.	Análisis de los procesos operativos para diagnosticar las causas de los principales riesgos de seguridad de la información, en la empresa SISLOCAR Caldera S. A	Entrevistas a personal clave, revisión documental, observación directa.	Matriz del Riesgo alineado con las Norma ISO/IEC 27001 y 27002 Análisis de Brechas (Gap Analysis) Matriz detección de brechas	Seguridad de la información, gestión de riesgos, normativas ISO/IEC 27001 y 27002, controles de seguridad, protección de datos, gestión de mejora continua.
Objetivo	**Entregable**	**Fase, parte o etapa de la metodología del proyecto que posibilita la**	**Técnicas/métodos de recolección de la información**	**Instrumentos**	**Temas relacionados para marco teórico**

		realización del entregable			
Analizar las debilidades en los mecanismos actuales de control de accesos y protección de datos sensibles, mediante la revisión de políticas internas, tecnologías empleadas y prácticas vigentes en la empresa, con el fin de orientar mejoras que reduzcan la exposición a riesgos cibernéticos	Informe de las debilidades de los controles de acceso y protección de datos sensibles.	Revisión de políticas internas y normativas existentes, con respecto a procedimientos, en relación con el acceso y la protección de datos de la empresa, mediante el análisis de sistemas implementados para establecer compatibilidad con la compatibilidad los estándares ISO/IEC 27001 y 27002.	Seguridad de la Información Estándares de Trabajo Gestión de Riesgos Sistema de Gestión de Seguridad de la Información	Matriz de evaluación de controles de acceso, análisis de brechas (Gap Analysis), listas de verificación, Entrevista estructurada. Revisión documental	Seguridad de la información. Gestión de accesos, normativas ISO/IEC 27001 y 27002. Estándares de trabajo. Gestión del riesgo. Principios de mínimo privilegio, autenticación y autorización. Riesgos cibernéticos, protección de datos sensibles, auditoría y monitoreo de accesos.
Objetivo específico	**Entregable**	**Fase, parte o etapa de la metodología del proyecto que posibilita la realización del entregable**	**Técnicas/métodos de recolección de la información**	**Instrumento**	**Temas relacionados para marco teórico**

Diseñar una propuesta de mejora del sistema de gestión de seguridad de la información, basada en los lineamientos de las normas ISO/IEC 27001 y 27002, que incluya controles específicos para el acceso y la protección de datos, y que permita mitigar los riesgos de accesos no autorizados y la vulneración de información crítica.	Documento de propuesta de mejora del SGSI, con controles específicos alineados a ISO/IEC 27001 y 27002.	Identificación de brechas y oportunidades de mejora, alineación con normativas internacionales, diseño de estrategias de implementación	Análisis de brechas (Gap Analysis), revisión documental, entrevistas con expertos, encuestas a usuarios, pruebas de vulnerabilidad	Matriz de mejora de controles de acceso, cuestionarios de evaluación de seguridad, informe de resultados de pruebas de vulnerabilidad. Revisión documental.	Seguridad de la información, gestión de riesgos, controles de acceso, normativas ISO/IEC 27001 y 27002, autenticación y autorización, estrategias de mitigación de riesgos, mejora continua del SGSI.

Fuente: Elaboración propia.

CAPÍTULO IV: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

El diagnóstico situacional de la empresa SILOSCAR Caldera S.A, pretende ofrecer una imagen panorámica que determina la situación actual sobre seguridad de la información, alineada con los estándares ISO/IEC 27001 y 27002, mediante la detección de los principales riesgos de ciberseguridad que enfrenta la compañía. Según Chaparro, mencionado en Universidad Hispanoamericana (2022), el diagnóstico se define como,

> […] la identificación, descripción y análisis evaluativo de la situación actual de la organización o del proceso en función de los resultados que se esperan y que fueron planteados en la misión. Es a la vez una mirada sistémica y contextual, retrospectiva y prospectiva, descriptiva y evaluativa. (p. 28).

De acuerdo con lo expresado en la cita anterior, se requiere de un análisis holístico, que contemple la operación administrativa, requiriendo de un diagnóstico técnico, de percepción y determinación de las brechas existentes, expresadas en las conclusiones. Entonces, no se puede limitar a meras descripciones, sino que debe trascender hacia un juicio crítico y estratégico, que contemple la naturaleza de la empresa, dentro de un contexto, con factores tanto externos como internos que inciden en su gestión.

Por tanto, el diagnóstico sigue una línea de retrospección y prospección, como clave para la identificación de patrones tanto en tiempo real como en lo futuro. Debe existir un equilibrio entre las observaciones y las valoraciones realizadas, para establecer parámetros que permitan la toma de decisiones estratégicas para apalancar la situación establecida en el problema, ¿Cómo implementar mejoras de Seguridad de la información, alineadas con los estándares ISO/IEC 27001

y 27002 para mitigar y gestionar los riesgos cibernéticos en la empresa SISLOSCAR Caldera S. ¿A, con un horizonte de ejecución en agosto de 2025?

Revisión de los Resultados

Fundamentado en los insumos obtenidos durante la fase de investigación, se presentan mediante tablas de Word y gráficos de Excel, los principales hallazgos, que permitan reflejar el estado actual de la empresa. Los resultados explicitados, surgen del análisis de datos cuantitativos y cualitativos, que revelan la dinámica y percepción del problema en estudio. Al integrar esta información, se procura construir un diagnóstico contextualizado que sirva como punto de partida para identificar brechas, necesidades prioritarias y oportunidades de mejora alineadas con los objetivos del proyecto. El examen se organiza mediante las variables emergentes de la investigación.

Diagnóstico Administrativo u Operativo

En la actualidad, la empresa SISLOCAR Caldera S.A, ofrece servicios logísticos para el bodegaje y transporte internacional de carga, contando con áreas de bodegaje, almacén fiscal y zonas Francas. Sus centros operativos se encuentran en las zonas de Caldera, sede principal, Limón, Heredia, Cartago y Alajuela. Sus servicios cuentan con multicanales, aéreos, terrestres y marítimos. Ofrece servicios de Logística de Terceros, (3 LP)

Gestiona la calidad de sus servicios, mediante la certificación ICONTEC (el Instituto Colombiano de Normas Técnicas y Certificación), quien le acredita la ISO 13485. También cuenta con el Sistema de Gestión Certificado IQNet, para garantizar que su sistema de gestión cumple

con la norma ISO 9001, respaldando la calidad de sus operaciones. En Caldera, cuenta con 65 colaboradores en planta, hasta el momento del diagnóstico.

Actualmente la empresa labora las 24 horas los 7 días de la semana, para responder a la gestión operativa requerida. El personal que aborda la Tecnología de la Información se conforma por 10 colaboradores, distribuidos según orden de roles desempeñados: 1 director ejecutivo, experto en informática, con más de 20 años de experiencia y represéntate de la Alta Gerencia de la empresa. Un Coordinador TI / SGSI, responsable de los enlaces con las diferentes jerarquías y de la dirección, planificación estratégica y auditorías internas.

Dos especialistas en informática, con 15 y 8 años de experiencia respectivamente, están encargados de la seguridad del sistema. Su función principal es velar por la protección de la información en tránsito dentro de la empresa. Además, se cuenta con un equipo de seis encargados de soporte técnico, responsables de atender las consultas de los distintos usuarios, gestionar accesos y resolver fallos en las estaciones de trabajo.

Capacidad Operativa de SISLOCAR Calder S.A

Con respecto a la capacidad operativa en SISLOCAR, se han identificado debilidades significativas en las competencias del personal técnico, especialmente en lo que respecta a la especialización necesaria para el mantenimiento y actualización de los controles normativos establecidos por los estándares ISO/IEC 27001 y 27002. Para el diagnóstico de esta dimensión, se validan las respuestas ofrecidas por los encuestados, en ellos ítems del 1 al 5 de la entrevista estructurada, (véase en el anexo 1 de este documento). También se aplica un instrumento que permite detectar las debilidades existentes que se expone en la tabla 8.

Tabla 8. Instrumento para detectar debilidades operativas

Instrumento	Descripción	Aplicación en SISLOCAR
Matriz de brechas (Gap Analysis)	Compara el estado actual vs. el estado deseado en competencias técnicas.	Identifica qué conocimientos faltan para cumplir con ISO/IEC 27001/27002.
Encuestas estructuradas	Recogen percepciones del personal sobre sus capacidades y necesidades.	Evalúan autodiagnóstico técnico y nivel de familiaridad con controles SGSI.
Análisis documental	Revisan cumplimiento normativo y desempeño técnico documentado.	Detectan desviaciones en la implementación de controles de seguridad.
Matriz de competencias	Mapea habilidades individuales frente a requerimientos normativos.	Permite visualizar brechas por rol y diseñar planes de formación.
Análisis de Brechas	Compara prácticas y capacidades con organizaciones similares.	Ayuda a dimensionar el rezago frente a estándares del sector.

Fuente: Elaboración propia.

Recurso Humano y Seguridad Informática

Durante la revisión de la gestión del recurso humano en SISLOCAR Caldera S.A., se identificó la ausencia de un programa estructurado de formación continua que asegure la capacitación sistemática del personal en temas clave de seguridad de la información. Si bien existen iniciativas puntuales de sensibilización, estas carecen de una planificación formal que defina frecuencias, metodologías y mecanismos de seguimiento.

En particular, no se observa una estrategia que promueva el entendimiento claro por parte de cada colaborador sobre su responsabilidad directa en la protección de los datos empresariales, ni tampoco se evidencia una articulación entre los contenidos formativos y los riesgos específicos que enfrenta la organización. El documento institucional vigente aborda la importancia de la capacitación, pero resulta insuficiente, ya que no contempla aspectos fundamentales como:

a) Periodicidad definida (semanal, mensual, anual)

b) Segmentación por perfiles o niveles de riesgo

Esto debilita la consolidación de una cultura organizacional centrada en la confidencialidad, integridad y responsabilidad colectiva sobre el manejo de la información. En la figura 10, se ofrece fotografías de uno de los módulos de capacitación al Recurso Humano, sobre seguridad informática, para observar el modelo.

Figura 10. Módulo de Capacitación

Fuente: Archivo organizacional.

Resultados del diagnóstico Operativo

Durante el proceso de diagnóstico, se identificó como un aspecto crítico la carencia de políticas y procedimientos formalizados en materia de seguridad de la información dentro de SISLOCAR. Aunque la alta dirección ha demostrado un compromiso firme, reflejado en su interés por alcanzar certificaciones especializadas, se requiere establecer con claridad los lineamientos y

documentar los procesos que regulen esta área para garantizar la alineación con estándares reconocidos a nivel internacional.

Como parte de esta iniciativa, se ha optado por implementar la plataforma OneDrive como herramienta para la gestión documental del Sistema de Gestión de Seguridad de la Información (SGSI), con el fin de mejorar el acceso, trazabilidad y control sobre los documentos institucionales vinculados al sistema. En SISLOCAR Caldera S.A., el ingreso a la planta física se realiza mediante un carné que contiene un código QR. Este sistema simplifica el acceso diario del personal, pero también presenta debilidades en la validación de identidad. No existen mecanismos que verifiquen de forma activa si la persona que porta el gafete es quien realmente debería ingresar, ni si su autorización sigue vigente.

Actualmente, es el personal de portería quien realiza la revisión, de forma visual. Verifican que el carné esté presente, pero no cuentan con herramientas automatizadas que les permitan confirmar si el código QR está activo, si corresponde al portador o si existen alertas relacionadas con el ingreso. El proceso depende en gran medida del criterio humano, lo que puede resultar insuficiente ante situaciones que exigen mayor precisión y control.

Existen riesgos asociados con este sistema de control, la falta de comprobación robusta representa un riesgo para la seguridad de la infraestructura tecnológica y operativa. Sin mecanismos complementarios como validación biométrica, autenticación secundaria o monitoreo automatizado de accesos, se abre la puerta a ingresos no autorizados que podrían comprometer áreas críticas.

Diagnóstico Técnico:

El diagnóstico técnico a empresa SISLOCAR Caldera S. A, agrupa los hallazgos del diagnóstico aplicado, con respecto a las brechas de seguridad de la información, mediante la valoración de la capacidad técnica y lógica de TI. Siendo el objetivo general del proyecto, implementar mejoras de Seguridad de la información, alineadas con los estándares ISO/IEC 27001 y 27002 para mitigar y gestionar los riesgos cibernéticos en la empresa, no se considera necesario, realizar un análisis específico de la infraestructura física de la organización, sino, centrarse en la capacidad técnica y la logística que requiere la aplicación de las normativas mencionadas.

La Infraestructura tecnológica en SISLOCAR Caldera S.A.

La empresa cuenta con una infraestructura híbrida: un servidor físico ubicado dentro de sus instalaciones en un espacio acondicionado para resguardar los equipos TI, y servicios complementarios en la nube que fortalecen la disponibilidad operativa. El servidor actúa como el núcleo de procesamiento de datos, mientras que la nube brinda soporte para el almacenamiento, acceso remoto y respaldo documental. Los accesos y operaciones están gestionados mediante políticas internas y GPOs (Group Policy Objects), lo que permite controlar permisos, roles y actividad de usuarios conforme a los criterios establecidos para la gestión de riesgos. A continuación, se detallan algunos elementos:

A. Servicios en la nube

La nube brinda soporte principalmente para:

a) Respaldo automático de documentos administrativos

b) Acceso remoto a ciertos módulos operativos

c) Herramientas básicas de colaboración digital

B. Sistemas Core

a) El **ERP** gestiona finanzas, contabilidad y recursos empresariales.

b) El sistema de **logística operativa** organiza los procesos de distribución y transporte.

Ambos están alojados en el servidor local, pero cuentan con funciones extendidas en la nube para escalabilidad y continuidad. En la siguiente tabla, se presenta el inventario tecnológico.

Tabla 9

Inventario Tecnológico

Tipo de equipo	Cantidad estimada	Desempeño operativo
Servidores físicos	1	Uno para Sistema de Gestión de Seguridad de la Información (SGSI) y ERP; otro para respaldos y trazabilidad de operaciones
Servidores virtuales / contenedores	3	La segmentación de servicios críticos implica una vigilancia especializada sobre entornos virtualizados que alojan funciones esenciales para la operación institucional. Esta estrategia permite distribuir de forma aislada servicios como correo electrónico, autenticación con el objetivo de fortalecer la gestión de la seguridad.
Estaciones administrativas	15	Personal de logística, contabilidad, atención al cliente y dirección
Estaciones operativas almacén	/ 10	Control de inventario, trazabilidad, escaneo de mercancías
Dispositivos móviles (tablets, escáneres)	8	Uso en campo para trazabilidad, entregas y control de rutas

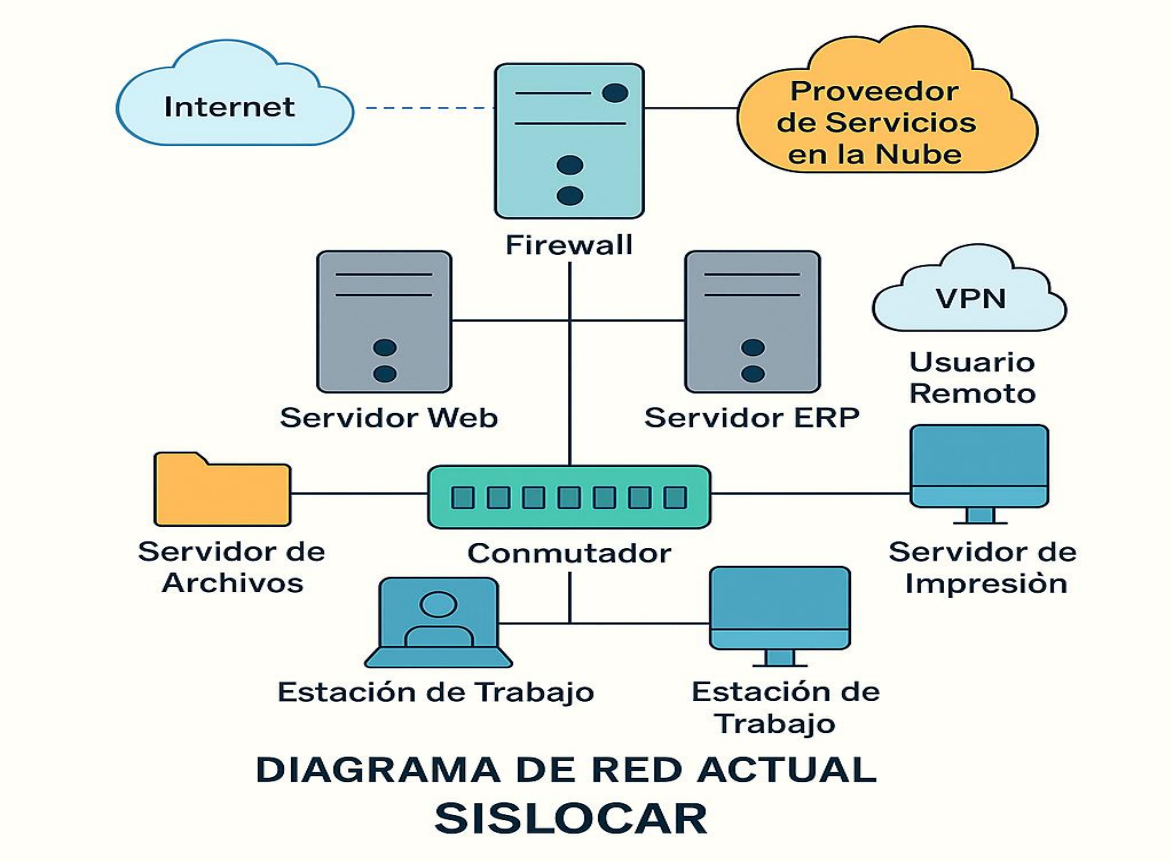
Tipo de equipo	Cantidad estimada	Desempeño operativo
Firewalls / dispositivos de red	2	Protección perimetral y segmentación de red
Equipos de respaldo (NAS / discos externos)	3	Almacenamiento segmentado para SGSI, operativos y administrativos

Fuente: Datos de la empresa.

Diagrama de Red Actual

La representación de la arquitectura tecnológica aplicada en las operaciones logísticas de SISLOCAR Caldera S. A, ofrece un esquema claro que permite visualizar los componentes claves de la red. En la figura 5, se ofrece un diagrama que ofrece una lectura holística, sobre la trama operativa del sistema.

Figura N° 11. Diagrama de Red



Fuente: Elaboración propia.

El diagrama presenta el punto de entrada al acceso de internet, protegido por un firewall de red perimetral, regulador de la afluencia del tráfico. De este sistema de seguridad, salen conexiones hacia un proveedor en la nube para el alojo de servicios complementarios y respaldos y un VPN, para que el usuario remoto, pueda conectarse al sistema. Con respecto a la infraestructura principal, el firewall, se conecta con un servidor web y un núcleo de gestión administrativa y operativa.

En la red interna, los servicios se entrelazan mediante un conmutador, que sirve para distribuir la conexión, hacia un servidor de archivos, uno de impresión y dos estaciones de trabajo. A continuación, se presentan los dispositivos de red con sus respectivas versiones, que operan dentro del sistema informático de la empresa, mediante la tabla 5 explicitando los dispositivos, estado actual y los rangos de soporte.

Tabla 10. Dispositivos de la Red

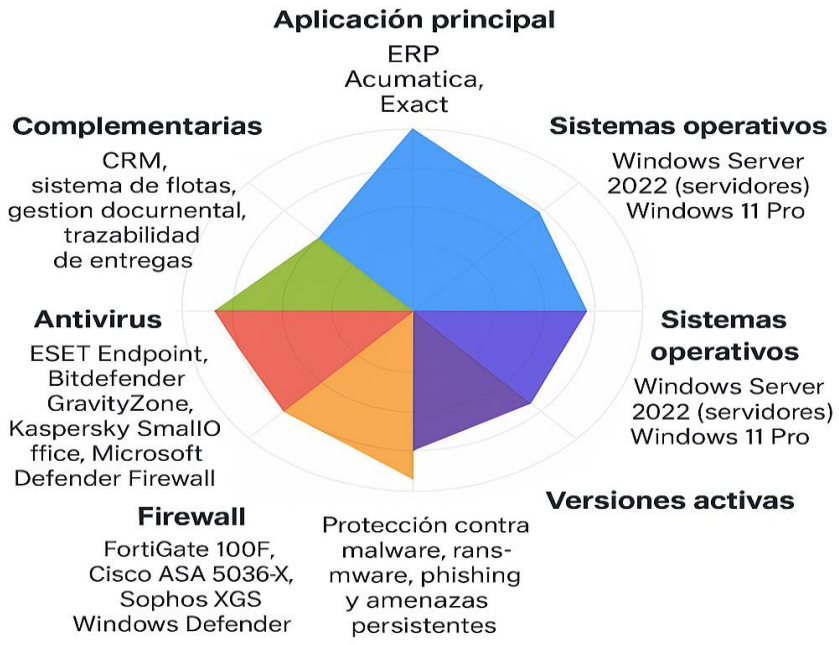
Dispositivo / Software	**Estado en 2025**
Windows Server 2022	Con soporte activo
Cisco Catalyst 2960-X	Soporte limitado / transición
FortiGate 100F	Soporte activo
Synology NAS DS1823xs+	Soporte activo
OpenVPN Access Server	Soporte activo
Windows Server 2022 como sistema operativo principal para servidores, y **Windows 11 Pro** en estaciones de trabajo.	Soporte activo
Cisco ASA 5506-X	Fin de soporte cercano
MikroTik RB4011	Soporte activo
TP-Link VX220 / Huawei HG8145V5	Soporte variable según proveedor ISP

Fuente: Elaboración propia.

De acuerdo con la tabla anterior, en general, los dispositivos se encuentran tecnológicamente activos. Existen algunos que requieren atención inmediata para su actualización, mediante una evaluación estratégica, para evitar que sean excluidos del soporte. Se hace necesario una evaluación del desempeño de cada uno de los módulos, para detectar si están dentro de la necesidad de emigrar hacia una actualización más acorde con la realidad tecnológica y sus exigencias en el contexto de la empresa.

Otro aspecto que se destaca en el entorno tecnológico es la gama de aplicaciones establecidas y que son claves para la operación y seguridad de la gestión empresarial. En el siguiente mapa de color tipo telaraña, se exponen las aplicaciones con las que cuenta la empresa, la aplicación principal y sus respectivas versiones.

Gráficos 1. Principales aplicaciones



Fuente: Archivo Organizacional, SISLOCAR Caldera S. A. Nota: Color azul, alto nivel de cobertura. Color verde, cobertura moderada. Color rojo, cobertura sólida. Color naranja, nivel medio alto. Color morado: Cobertura alta.

Con respecto al área de ciberseguridad, se nota que actualmente se están utilizando varios antivirus al mismo tiempo, como ESET Endpoint, Bitdefender GravityZone, Kaspersky SmallOffice y Microsoft Defender, lo cual refleja una estrategia algo dispersa en cuanto a protección. Aunque cada uno tiene sus ventajas, esta variedad puede generar conflictos o duplicidades en la gestión de amenazas. Por eso, sería recomendable evaluar la posibilidad de unificar las herramientas, lo que ayudaría a tener un sistema de defensa más eficiente y alineado.

Por otro lado, mediante los firewalls, se han implementado soluciones como FortiGate 100 F, Cisco ASA 5036-X, Sophos XGS y Windows Defender. En general, estas plataformas ofrecen una arquitectura bastante sólida, lo que permite seguir mejorando el sistema operativo y mantener una buena protección a nivel de red. Los sistemas operativos que se están utilizando, Windows Server 2022 en los servidores y Windows 11 Pro en las estaciones de trabajo, están actualizados y activos, lo que contribuye a la estabilidad del entorno tecnológico y asegura una buena compatibilidad con las aplicaciones que se usan en la empresa.

Mediante el instrumento aplicado, para el análisis de brechas, (Gap Analysis), se diagnostican áreas sensibles técnico-operativas aplicadas en la empresa SISLOCAR Caldera S.A, tomando en cuenta aspectos como, el soporte técnico interno, infraestructura de TI y madurez operativa. El diagnóstico arroja resultados que interpretan la situación actual de la empresa en el espacio técnico, permitiendo la detección de debilidades en los mecanismos actuales de control de accesos y protección de datos sensibles.

Para la aplicación del análisis de brechas, se aplicó una matriz para detectar brechas, que consta de tres fases mediante un enfoque estructurado y en relación con los requisitos establecidos por ISO/IEC 27001 y 27002, para la identificación de áreas de mejora y formulando recomendaciones estratégicas. A continuación, se expone las acciones aplicadas a través de la metodología trifásica.

1. **Levantamiento de Información**

    a) Revisión documental (políticas, procedimientos, registros de seguridad).

    b) Entrevistas con responsables de la gestión de seguridad.

    c) Aplicación de cuestionarios para evaluar el cumplimiento de controles clave.

2. **Comparación con ISO/IEC 27001 y 27002**

    a) Identificación de requisitos fundamentales y controles de seguridad.

    b) Análisis de brechas utilizando una matriz de cumplimiento.

    c) Evaluación del nivel de madurez de cada control de seguridad.

3. **Identificación de Áreas de Mejora**

    a) Priorización de brechas según impacto y criticidad.

    b) Identificación de recursos necesarios para el cumplimiento.

    c) Evaluación de riesgos asociados a las brechas detectadas.

Tabla 11. Análisis de Brechas (Gap Analysis)

Control de Seguridad	Estado Actual	Requisito ISO/IEC	Brecha Detectada	Nivel de Prioridad
Gestión de accesos	Parcialmente implementado	Control 9.1 (ISO 27002)	Deficiencia en monitoreo de accesos	Alta

Protección de activos	Implementado	Control 8.2 (ISO 27002)	Sin inventario actualizado	Media
Gestión de incidentes	No implementado	Control 16.1 (ISO 27002)	Falta procedimiento formal	Alta

Fuente: Elaboración propia.

Como patrón general, se logra descubrir, una tendencia hacia el repunte del riesgo, que va en aumento y que requiere de una intervención inmediata, mediante la instauración de políticas administrativas y operativas que sirvan para la mitigación de las amenazas percibidas, tomando en cuenta, los diferentes frentes críticos determinados.

Ante este escenario, se detectan oportunidades de mejoras para la gestión el riesgo de la información, mediante la aplicación de recursos estratégicos para atender las debilidades identificadas en el acceso y gestión de incidentes relacionados con la protección de la información, reduciendo la exposición a los ataques cibernéticos. Se visualiza la necesidad de fortalecer las acciones de respaldo de los datos, mediante mecanismos sólidos que aseguren la permanencia y protección de estos, recurso valioso para el buen desempeño empresarial.

Se hace necesario, mantener a disposición la información de la organización, de forma que se asegure que su contenido, permanezca integro y que pueda ser recuperado sin complicaciones ante cualquier eventualidad. Esto implica establecer políticas claras sobre las copias de seguridad, definir qué datos son críticos, establecer con qué frecuencia se realiza el respaldo, y elegir medios confiables para almacenarlos, ya sea en servidores locales o en la nube.

Además, es clave que esas copias de seguridad estén cifradas, se verifiquen de forma periódica y que el proceso para restaurarlos sea ágil y efectivo, en línea con los niveles de servicio que la institución espera. En la figura 12, se presenta un resumen de las brechas detectadas en el diagnóstico realizado.

Figura N° 12. Principales Brechas Detectadas

Fuente: Elaboración propia.

Entonces, en cuanto al impacto operativo de las brechas, según la figura 1, se encuentran debilidades significativas sobre aspectos técnicos medulares que ponen en riesgo la seguridad de la información, detectándose, accesos no controlados, ausencia de protocolos para la gestión de incidentes y la necesidad de fortalecer la actualización continua del capital humano, responsable de los mecanismos de defensa ante ciberamenazas , acorde con la constante evolución de las tácticas, técnicas y procedimientos de actores maliciosos. Todo esto, compromete el cumplimiento con buenas prácticas internacionales, como las delineadas por ISO/IEC 27001 y 27002.

Capacidad Técnica - Operativa de SISLOCAR Calder S.A

Con respecto a la capacidad operativa en SISLOCAR, se han identificado debilidades significativas en las competencias del personal técnico, especialmente en lo que respecta a la especialización necesaria para el mantenimiento y actualización de los controles normativos establecidos por los estándares ISO/IEC 27001 y 27002. Para el diagnóstico de esta dimensión, se validan las respuestas ofrecidas por los encuestados, en ellos ítems del 1 al 5 de la entrevista estructurada, (véase en el anexo 1 de este documento). También se aplica un instrumento que permite detectar las debilidades existentes que se expone en la tabla 12.

Tabla 12. Instrumento para detectar debilidades operativas

Instrumento	Descripción	Aplicación en SISLOCAR
Matriz de brechas (Gap Analysis)	Compara el estado actual vs. el estado deseado en competencias técnicas.	Identifica qué conocimientos faltan para cumplir con ISO/IEC 27001/27002.
Encuestas estructuradas	Recogen percepciones del personal sobre sus capacidades y necesidades.	Evalúan autodiagnóstico técnico y nivel de familiaridad con controles SGSI.
Análisis documental	Revisan cumplimiento normativo y desempeño técnico documentado.	Detectan desviaciones en la implementación de controles de seguridad.
Matriz de competencias	Mapea habilidades individuales frente a requerimientos normativos.	Permite visualizar brechas por rol y diseñar planes de formación.
Análisis de Brechas	Compara prácticas y capacidades con organizaciones similares.	Ayuda a dimensionar el rezago frente a estándares del sector.

Fuente: Elaboración propia.

De acuerdo con las herramientas aplicadas, se detectan en el proceso de evaluación de la capacidad operativa del equipo técnico de SISLOCAR, se ha identificado una serie de brechas que limitan el cumplimiento normativo y la sostenibilidad del Sistema de Gestión de Seguridad de la Información (SGSI). Estas brechas afectan directamente la alineación institucional con los

estándares ISO/IEC 27001 y 27002, y requieren intervenciones estratégicas tanto a nivel interno como externo.

En primer lugar, se observa que el conocimiento del personal sobre la norma ISO/IEC 27001 es parcial y no está respaldado por certificaciones formales. Esta baja especialización técnica incide en la capacidad para interpretar e implementar adecuadamente los controles normativos, necesarios en la protección de la información en el entorno TI. La gestión de controles de seguridad presenta debilidades que ponen en riesgo la capacidad para anticiparse a vulnerabilidades y amenazas emergentes, comprometiendo la estabilidad del SGSI.

Otro hallazgo importante se refiere a la documentación y trazabilidad de los procesos vinculados a la seguridad de la información. Actualmente, los registros de documentación y trazabilidad de las gestiones informáticas realizadas carecen de estandarización, lo que genera una falta de evidencia operativa y dificulta la auditoría de los controles existentes. Se evidencia la ausencia de una metodología definida, lo que impide evaluar de forma estructurada la exposición institucional ante amenazas.

Esta carencia genera una vulnerabilidad operativa considerable, ya que no permite tomar decisiones informadas ni establecer planes de mitigación eficaces. Se recomienda adoptar una metodología reconocida de análisis de riesgos y capacitar al personal en su aplicación práctica y contextualizada.

Finalmente, se detecta que el soporte externo especializado, cuando existe, es eventual y carece de una estrategia formal. Esta situación limita el aprovechamiento de alianzas estratégicas, outsourcing o consultorías que podrían acelerar la implementación del SGSI y compensar

temporalmente las brechas técnicas internas. En respuesta, se sugiere diseñar un plan de soporte técnico externo que establezca claramente los momentos, las modalidades y los actores clave para complementar las capacidades institucionales en las fases iniciales del proyecto.

Aunque existe una disposición general para avanzar en la implementación del SGSI, no se ha documentado de manera estructurada la dimensión y alcance de dichas debilidades, lo cual limita la visibilidad institucional sobre los riesgos asociados y ralentiza la toma de decisiones estratégicas.

Estas deficiencias se evidencian en la falta de registros que den cuenta de los niveles de formación actual en normativas de seguridad, la ausencia de planes de desarrollo profesional alineados con estándares internacionales, y la escasa sistematización de resultados en evaluaciones técnicas previas. Este vacío documental impide dimensionar correctamente la brecha de capacidades frente a los requerimientos del SGSI, y destaca la necesidad de establecer mecanismos de soporte tanto internos como externos.

En este sentido, se vuelve imprescindible incorporar estrategias complementarias que contemplen modalidades como subcontrataciones**,** consultoría especializada o alianzas interinstitucionales, al menos durante las fases iniciales del proceso. Estas soluciones pueden ser clave para asegurar el cumplimiento normativo, robustecer la capacidad instalada, y generar una curva de aprendizaje que permita al equipo técnico asumir progresivamente un rol más autónomo y especializado.

Políticas Implementadas Para la Gestión del Riesgo Informático

Las políticas actualmente implementadas en SISLOCAR Caldera S.A. para prevenir incidentes informáticos no deseados se consideran aceptables en términos generales, pero presentan debilidades importantes en áreas esenciales definidas por los estándares ISO/IEC 27001 y 27002. No se observa la implementación de autenticación multifactor, lo que deja al descubierto, la sensibilidad de los datos, ya que la creación de contraseñas se genera al cumplir los requisitos establecidos para dicho proceso.

También sobresale la ausencia de calendarización periódica, para la revisión de las políticas establecidas, su debido cumplimiento y las fragilidades que presentan. Los sistemas de alerta ante intentos de ingresos fallidos, aplicando únicamente las contraseñas, presentan brechas de efectividad y riesgos de ataques irreversibles. Entre las directrices vigentes se incluyen:

a) **Política de acceso a sistemas**: Define niveles de privilegio y autorizaciones por usuario, pero no contempla validaciones dinámicas ni autenticación multifactor.
b) **Política de respaldo de información**: Establece rutinas básicas de copia de seguridad, aunque sin cifrado ni revisión automatizada de integridad.
c) **Política de uso aceptable de recursos tecnológicos**: Regula el comportamiento del usuario frente a los dispositivos, pero carece de controles para descargas no autorizadas o navegación en sitios de riesgo.
d) **Política de respuesta ante incidentes**: Define una acción inicial reactiva ante fallos evidentes, aunque no cuenta con registros sistemáticos que faciliten la trazabilidad ni el aprendizaje organizacional.

e) **Política de monitoreo de sistemas**: Está limitada al seguimiento superficial de actividades, sin correlación cruzada de eventos ni alertas en tiempo real.

En cuanto a la trazabilidad de eventos fortuitos que comprometan la integridad de la información sigue siendo parcial. La ausencia de registros detallados y correlación de datos dificulta el análisis post-incidente. Además, se detecta un riesgo latente de fuga de información sensible a través de descargas maliciosas, especialmente desde terminales expuestos o redes compartidas.

Además, se aplica una política de contraseñas que sigue las Directivas de Grupo (GPO), gestionadas de forma centralizada mediante Active Directory. Esta configuración permite establecer criterios claros y obligatorios para el acceso a los sistemas operativos en entornos Windows, como la longitud mínima de las contraseñas, su complejidad, el historial que evita reutilizaciones y el período de expiración. Estas medidas no solo fortalecen la seguridad, sino que también brindan a los usuarios un marco predecible y confiable para el manejo de sus credenciales. No obstante, no se designa un servidor que cumpla la función de controlador de dominio.

Asegurar esta concordancia entre la infraestructura y las políticas aplicadas no solo garantiza la operatividad técnica, sino que también refleja un compromiso con la coherencia institucional y la protección de los datos, estableciendo parámetros técnicos obligatorios como la longitud mínima de la contraseña, la complejidad requerida, el historial de contraseñas y el tiempo de expiración.

Longitud mínima de contraseñas (12 a 16 caracteres).

a) Complejidad de caracteres (combinación de mayúsculas, minúsculas, números y símbolos)

b) Periodicidad de cambio cada 3 meses
c) Historial de contraseñas reutilizadas
d) Bloqueo temporal ante intentos fallidos sucesivos

Estas medidas son aplicadas de forma forzosa en los equipos integrados al dominio, lo que garantiza un nivel aceptable de seguridad en el acceso a la información corporativa gestionada internamente. Sin embargo, existen puntos vulnerables, que se perciben en la limitada cobertura de esta política hacia otros sistemas y plataformas que operan fuera del dominio corporativo, en procesos específicos, incluyendo bases de datos de terceros, plataformas logísticas y herramientas en la nube, no están integradas a la gestión de Active Directory. Como resultado:

a) El ingreso a estas aplicaciones se realiza mediante credenciales definidas localmente por cada usuario o proveedor.
b) No existen restricciones técnicas unificadas sobre la complejidad ni vigencia de las contraseñas.
c) No se controla el uso de contraseñas débiles, repetidas o compartidas entre cuentas.

Este escenario abre la posibilidad de filtraciones, acceso indebido o explotación de vulnerabilidades a través de credenciales inseguras. Así mismo, La falta de estándares unificados para credenciales en aplicaciones externas puede derivar en accesos no autorizados, afectación a la trazabilidad de eventos de seguridad, y en escenarios críticos, fuga de información a través de ataques de fuerza bruta o descargas maliciosas

Concluyendo, el diagnóstico técnico, ofrece la oportunidad de implementar un plan estructurado, que atienda las brechas detectadas y fortalezca la gobernanza tecnológica, la

formación del personal y la adopción de soluciones técnicas organizadas y coherentes con el entorno de la organización. La metodología aplicada, debe considerar,

Diagnóstico de percepción

El diagnóstico de percepción le permite al investigador, reconocer las perspectivas e interpretaciones cualitativas, del personal que mantiene injerencia con flujo de información de la empresa SISLOCAR Caldera S.A sobre aspectos medulares para obtener una panorámica más subjetiva pero que dote de pertenencia la propuesta para la solución del problema planteado. Se aplica una encuesta estructurada, que consta de ítems de respuestas cerradas y abiertas, Se exploran áreas específicas, políticas y procedimientos de seguridad y prácticas organizacionales.

El análisis se presenta de forma categórica, mediante tablas elaboradas en Word y graficadas en Excel, sin recurrir al cálculo numérico como fuente de información, sino en lograr establecer frecuencias, recurrencias y patrones en las respuestas abiertas. Los datos se especifican de las consultas aplicadas a la población seleccionada que se describe en la siguiente tabla, 13.

Tabla 13. Población y muestra

Puesto Laboral	**Población Total (F.A)**	**Población % (F.R)**	**Muestra Seleccionada (F.A)**	**Muestra % (F.R)**
Director Ejecutivo	1	10 %	1	10 %
Coordinador de Tecnologías de Información	1	10 %	1	10 %
Personal operativo con acceso a sistemas	6	60 %	6	60 %
Encargados de seguridad del sistema	2	20 %	2	20 %
Totales	**10**	**100 %**	**10**	**100 %**

Nota: F.A = Frecuencia absoluta. F.R = Frecuencia relativa.

Tabla 14

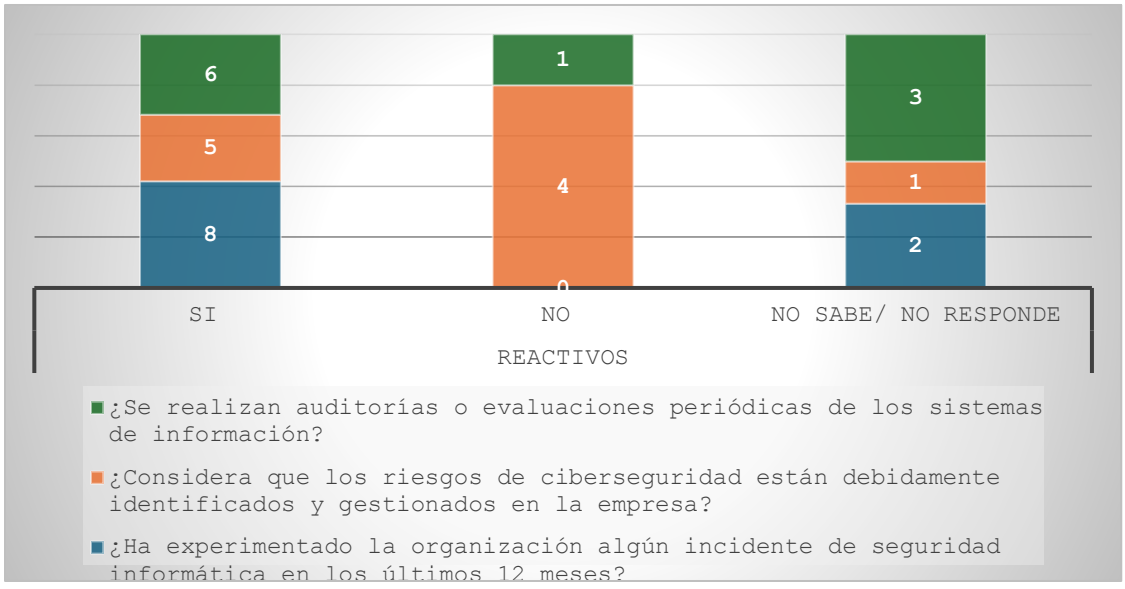
Riesgo Cibernético (Respuestas de los tres perfiles)

¿Ha experimentado la organización algún incidente de seguridad informática en los últimos 12 meses?

Ítem	Reactivos		
	Si	**No**	**No sabe/ no responde**
¿Ha experimentado la organización algún incidente de seguridad informática en los últimos 12 meses?	8	0	2
¿Considera que los riesgos de ciberseguridad están debidamente identificados y gestionados en la empresa?	5	4	1
¿Se realizan auditorías o evaluaciones periódicas de los sistemas de información?	6	1	3

Fuente: Elaboración propia.

Gráficos 2. Datos de la tabla 14



Fuente: Datos de la tabla 14.

De acuerdo con el análisis de los datos proporcionados por los tres perfiles encuestados, se identifican percepciones relevantes que revelan aspectos críticos de la gestión de seguridad

informática. Los participantes reconocen la ocurrencia de incidentes maliciosos y riesgos cibernéticos que comprometen el manejo de la información en la empresa.

Un grupo minoritario de respuestas, concretamente tres participantes, también señala la existencia de brechas informativas, atribuibles a la falta de socialización interna. Esto sugiere que la información clave no se transmite de manera eficiente ni oportuna entre el talento humano, limitando la capacidad de respuesta ante amenazas emergentes.

Respecto a la percepción sobre la gestión institucional de los riesgos de ciberseguridad, las opiniones están divididas. Esta polarización evidencia deficiencias en la implementación de estrategias para proteger los datos sensibles y otros activos digitales. La confianza organizacional parece debilitada, producto de una gestión que carece de estructura formal y visibilidad operativa.

Desde el enfoque del personal operativo, se manifiesta una preocupación generalizada por la recurrencia de ciberataques, lo que apunta a un entorno vulnerable y expuesto. Esta situación subraya la necesidad urgente de reforzar los controles relacionados con la gestión de incidentes, conforme a la recomendación del control A.16.1.1 de la norma ISO/IEC 27001. Ello implica establecer procedimientos claros para la identificación, análisis y respuesta oportuna ante eventos de seguridad, integrando estrategias alineadas de manera sistemática al Sistema de Gestión de Seguridad de la Información.

Con respecto a la gestión del riesgo, las percepciones expuestas, permiten reconocer una divergencia entre el director ejecutivo y el equipo de seguridad, referente a las estrategias aplicadas. Esto se fundamenta en las respuestas ofrecidas en ítem 5, por el sujeto 1, que corresponde a este, según los perfiles descritos en la tabla 5, sobre la población encuestada,

resumen de respuestas que se ofrecen en la tabla 15 expuesta a continuación. Esta disparidad, puede leerse como una oportunidad, para revisar e implementar estrategias establecidas en el 5.7, (Evaluación continua del riesgo de seguridad de la información), y el 5.8, (Resiliencia de la información), para asegurar que el SGSI, cumpla con lo establecido en las normativas, **(**A.6.1.2 y el A.17.1.2**),** para la efectividad de prácticas sobre prevención, recuperación y continuidad operativa.

Tabla 15. Constructos de respuestas abiertas (tres perfiles)

Ítem; 5, Desde su experiencia, ¿cuáles considera que son los principales riesgos cibernéticos que enfrenta la empresa?				
Población				
Director técnico/ 1	**Coordinador de Tecnologías de Información / 1**	**Personal operativo con acceso a sistemas / 6**	**Encargados de seguridad del sistema / 2**	**Total / 10**
S. 1 "Posiblemente un poco de descuido sobre el tema o tal vez, deficientes y exposición por uso compartido de credenciales"	S.2 "Falta de trazabilidad de eventos críticos y monitoreo en tiempo real".	S.3 Desde mi experiencia podría mencionarte los accesos no autorizados.	S.4 Accesos no controlados a datos sensibles	S.5 Uso de contraseñas débiles y sin rotación periódica
S,6 Falta de atención sobre las políticas de seguridad por parte del personal	S.7 Ausencia de autenticación multifactorial en accesos críticos	S.8 Poca conciencia sobre clasificación y manejo de la información	S.9 Falta de auditorías para la detección de errores en los controles aplicados	S.10 Softwares obsoletos para la detección de infecciones, para evitar malware, y con eso, pérdida de datos críticos.

Fuente: Elaboración propia.

Después de codificadas las categorías, utilizando el método axial-descriptivo, y su clasificación, mediante la herramienta ATLAS. ti, en la tabla 16, se presentan las unidades de significado encontradas.

Tabla 16. Propuesta de códigos y unidades de significado

Participante	Unidad de Significado	Código Propuesto
S.1	"Descuido sobre el tema" / "uso compartido de credenciales"	Cultura de seguridad débil; Riesgo por credenciales
S.2	"Falta de trazabilidad de eventos críticos"	Falta de trazabilidad y monitoreo
S.3	"Accesos no autorizados"	Control de acceso insuficiente
S.4	"Accesos no controlados a datos sensibles"	Exposición de datos sensibles
S.5	"Contraseñas débiles y sin rotación periódica"	Gestión de autenticación deficiente
S.6	"Falta de atención sobre políticas de seguridad"	Bajo conocimiento de políticas de seguridad
S.7	"Ausencia de autenticación multifactorial"	Medidas de acceso insuficientes
S.8	"Poca conciencia sobre clasificación y manejo de la información"	Gestión inadecuada de información
S.9	"Falta de auditorías para detección de errores en controles aplicados"	Falta de revisión y mejora continua
S.10	"Software obsoleto para detección de infecciones" / "riesgo de pérdida de datos críticos"	Riesgo por sistemas no actualizados; Protección deficiente contra malware

Fuente: Elaboración propia.

Amparado a los patrones emergentes de la tabla anterior, se identifican 5 áreas según los códigos propuestos, Cultura de seguridad débil, Gestión de accesos deficiente, Exposición y clasificación inadecuada de la información, Falta de trazabilidad y monitoreo e infraestructura tecnológica vulnerable, cada una de ellas se describen en concordancia con la percepción expresada por los encuestados.

1. **Cultura de seguridad débil**: Se evidencian patrones de cultura organizacional, con fuertes debilidades referente a la seguridad de la información, vicios peligrosos como la

permisividad en el uso compartido de credenciales y aparente desconocimiento o incumplimiento de políticas internas, se interpretan como desconexión con las normativas sobre seguridad, establecidas en ISO/IEC 27001 y 27002.

2. **Gestión de acceso deficiente:** las gestiones operativas de la empresa se ven permeadas por débiles controles de acceso, haciendo hincapié, en la ausencia de autenticación multifactor, la rotación de credenciales y el control sobre accesos no autorizados, a recursos críticos.
3. **Exposición y clasificación inadecuada de la información:** se refleja una baja madurez en la gestión y clasificación de la información, evidenciándose la ausencia de esbozos formales de etiquetado, segmentación y aplicación de controles.
4. **Falta de trazabilidad y monitoreo:** Se expresa, que la trazabilidad y monitoreo de la gestión de la información, son escasos y esporádicos, sin ninguna planificación constante y evolutiva. Se refleja que el SGSI, no empata con la filosofía de mejora continua.
5. **Infraestructura tecnológica vulnerable:** se percibe que el sistema existente en la empresa es obsoleto, y que necesita ser robustecido, a través de hardware y software, que establezcan capas defensivas para evitar la pérdida de datos, infecciones persistentes y vulnerabilidad no parcheadas.

De acuerdo con este análisis, se observa y denota la necesidad de implementación de controles técnicos, mediante una reingeniería cultural, que interiorice la importancia del resguardo de la seguridad de uno de los valores más destacables de la empresa, la información.

Tabla 17. Constructo de respuestas abiertas (tres perfiles)

Ítem 6. ¿Qué tipo de amenazas informáticas cree que podrían tener mayor impacto sobre los sistemas críticos de SISLOCAR
POBLACIÓN

Director técnico/ 1	**Coordinador de Tecnologías de Información / 1**	**Personal operativo con acceso a sistemas / 6**	**Encargados de seguridad del sistema / 2**	**Total / 10**
S. 1 “Las amenazas que podrían tener mayor impacto, podrían ser los ataques de ransomware, suplantación de identidad (phishing), denegación de servicios (Dos), o también la posible fuga de información por vulnerabilidades que no han sido gestionadas aún”.	S. 2 “Ransomware, phishing, denegación de servicio y fuga de datos por vulnerabilidades no gestionadas”	S. 3 “Intrusiones a través de exploits de día cero no parcheados”	S. 4 “Ataques internos por empleados con privilegios mal gestionados”	S. 5 “Vulnerabilidades en sistemas heredados que no reciben soporte.
S, 6 “Conexión de dispositivos no autorizados a la red”.	S. 7 “Malware evasivo en entornos sin protección proactiva”.	S. 8 “Amenazas persistentes avanzadas (APT)”.	S. 9 “Accesos remotos sin cifrado ni controles robustos”	S. 10 “Configuraciones erróneas en firewalls o políticas perimetrales”

Fuente: Elaboración propia.

Tabla 18. Matriz de Concurrencia (Amenazas vs. Dimensiones de Riesgo)

ID Participante	**Cita**	**Código 1**	**Código 2**	**Código 3**
S.1	Ransomware, phishing y denegación de servicios.	Ransomware	Phishing	Denegación de servicio
S.2	Explotación de vulnerabilidades sin parches (día cero).	Vulnerabilidades sin parche		

S.3	Accesos internos maliciosos por privilegios elevados.	Accesos no autorizados	Privilegios mal gestionados	
S.4	Ingeniería social enfocada en robo de credenciales.	Ingeniería social	Robo de credenciales	
S.5	Vulnerabilidades en sistemas heredados que no reciben soporte.	Sistemas obsoletos	Vulnerabilidades sin parche	
S.6	Conexión de dispositivos no autorizados a la red.	Dispositivos no autorizados	Accesos no controlados	
S.7	Malware persistente en entornos sin protección proactiva.	Malware evasivo	Protección antimalware deficiente	
S.8	Amenazas persistentes avanzadas (APT).	APT	Persistencia prolongada	
S.9	Accesos remotos sin cifrado ni controles robustos.	Accesos remotos inseguros	Falta de cifrado	
S.10	Configuraciones erróneas en firewalls o políticas perimetrales.	Configuraciones inseguras	Fallas en controles perimetrales	

Fuente: Elaboración propia.

De acuerdo con los patrones establecidos en la tabla anterior, emergen una serie de patrones que se detectan a través de la codificación axial- descriptiva, la que permite organizar de forma agrupada y sistemática, los datos ofrecidos por los encuestados. Con esta relación, se pueden inferir, las siguientes apreciaciones, relacionadas con la situación interna de la empresa y su relación con el manejo, resguardo y gestión de la seguridad informática, expresadas en la figura 13.

Figura N° 13. Amenazas emergentes según la apreciación de los encuestados

Fuente: Elaboración propia según patrones emergentes.

La figura anterior, permite visualizar, desde el punto de vista de los encuestados, que existen riesgos en las tácticas y normas aplicadas para la detección de ataques activos, permitiendo que vectores como, ransomware, phishing y ataques de denegación de servicio, puedan convertirse en una amenaza de impacto operativo. Se debe fortalecer de forma temprana, estrategias para establecer una cultura de ciberseguridad en la organización.

También se enfatiza en la debilidad de las técnicas de seguridad aplicadas, permitiendo la creación de ambientes vulnerables, al contar con software sin parches fundamentándose en la codificación de respuestas, ofrecidas en la tabla 17. Los sujetos 1 y 2, correspondientes respectivamente, al director ejecutivo y al coordinador de Tecnologías de información, al mencionar la existencia de vulnerabilidades no gestionadas oportunamente, sugieren equipamientos y aplicaciones sin parches. El resto de encuestados, hacen referencia a falencias en el soporte que requieren protección y actualizaciones oportunas.

A través del diagnóstico, fundamentado en la percepción de los involucrados, se detecta la existencia de gestiones referentes a parches, en los sistemas operativos, detectándose esa falencia, en el antivirus y la plataforma de gestión, de la información. El ciclo de soporte técnico se convierte en una acción de vital importancia, ya que requiere de actualizaciones y mejoras continuas, para la prevención de ataques mal intencionados.

Haciendo referencia a la cultura de la gestión del riesgo, que debe fortalecer la empresa, se denota la necesidad de establecer conductas de ciberresilencia humana, con estrategias de refrescamiento y aplicabilidad eficiente de los conocimientos que posee el recurso humano y que le agregan un plus a la organización. Por tanto, se deben eliminar los accesos privilegiados o mal gestionados, aplicando accesos remotos con cifrados de seguridad.

Tabla 19. Constructo de respuestas abiertas (tres perfiles)

Ítem 10. ¿Cómo describe la cultura de seguridad de la información dentro de la empresa?				
POBLACIÓN				
Director técnico/ 1	**Coordinador de Tecnologías de Información / 1**	**Personal operativo con acceso a sistemas / 6**	**Encargados de seguridad del sistema / 2**	**Total / 10**
S. 1	S. 2	S. 3	S. 4	S. 5
“Actualmente es un poco estructurada y con bajo nivel de sensibilización, ya que no existen mecanismos formales de educación ni buenas prácticas difundidas entre el personal encargado”.	“Se ha logrado establecer una línea base de gobernanza en seguridad de la información. Existen roles definidos y la alta dirección reconoce su importancia estratégica”.	“La cultura actual es incipiente; la mayoría de los colaboradores no identifica los riesgos derivados de malas prácticas digitales ni existe entrenamiento recurrente en protocolos de seguridad”.	“La empresa cuenta con espacios formativos anuales y boletines mensuales de concienciación. Aunque aún no están integrados en el plan estratégico, representan avances sostenibles”.	“A pesar de contar con políticas documentadas, no existe apropiación práctica de dichas políticas entre los usuarios, y el lenguaje utilizado no es accesible para todos los niveles operativos”
S, 6	S. 7	S .8	S. 9	S. 10

“Se observan buenas prácticas puntuales en algunas unidades de TI, especialmente en gestión de accesos y manejo de incidentes, lo que demuestra núcleos de madurez localizados”.	“La rotación frecuente del personal y la ausencia de procesos de inducción en ciberseguridad provocan una desconexión entre políticas formales y hábitos reales de protección de la información”.	“Hay evidencia de una mentalidad de cumplimiento más que de concienciación; se priorizan auditorías y certificaciones sin un compromiso genuino con la mejora cultural continua”	“No existen canales formales de reporte de incidentes ni se han realizado campañas de simulación de ataques, lo que indica baja preparación y capacidad de respuesta a amenazas reales”.	“Se percibe una cultura reactiva más que preventiva. Los controles se ejecutan después de los incidentes y no hay métricas claras de sensibilización o desempeño en ciberseguridad”.

Fuente: Elaboración propia (2025).

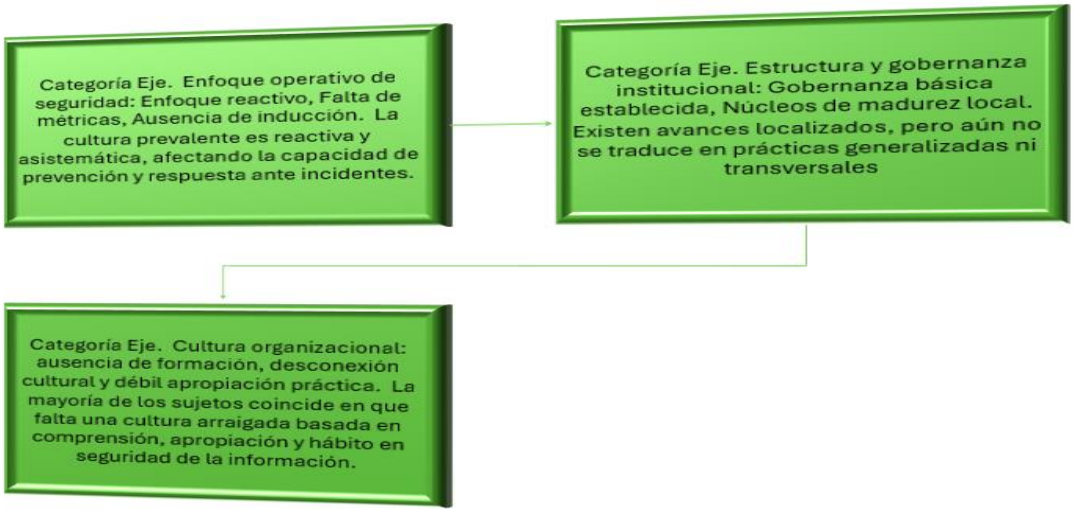
Tabla 20. Codificación de los datos de la tabla 19

Código	Frecuencia	Ejemplo
Ausencia de formación	5	“No existen mecanismos formales de educación” (S1, S3, S5)
Enfoque reactivo	2	“Los controles se ejecutan después de los incidentes” (S10)
Débil apropiación práctica	2	“No existe apropiación práctica de políticas” (S5, S8)
Desconexión cultural	2	“No hay integración entre políticas y comportamiento” (S7, S10)
Gobernanza básica establecida	1	“Se ha logrado establecer una línea base de gobernanza” (S2)
Núcleos de madurez local	1	“Buenas prácticas puntuales en TI” (S6)
Formación incipiente	1	“Espacios formativos anuales y boletines mensuales” (S4)

Fuente: Elaboración propia.

Después de establecidas las categorías emergentes en las respuestas de los encuestados, se reagrupan por temática, surgiendo eje categóricos y códigos de relación, que se exponen en la figura 14.

Figura 14. Patrones emergentes



Fuente: Elaboración propia.

La figura anterior, muestra la interpretación de los patrones emergentes, de acuerdo con las percepciones expuestas en las respuestas brindadas por los encuestados, siendo el patrón dominante, una cultura débil de la organización. También predomina la apreciación, de existir un marco político de operación inestable, que permite la improvisación.

A pesar de que algunos sujetos expresan que existe madurez técnica, en cuanto a las técnicas directivas, esa apreciación no es generalizada, considerando la mayoría, que existen algunas zonas que se presentan roles de gobernanza, no es una acción que transversalice la operación de la organización. Se deben concatenar las matrices de acción para establecer una cultura organizacional sólida para fortalecer la seguridad informática en todas sus áreas operativas.

Tabla 21. Mejoras en la seguridad cibernética

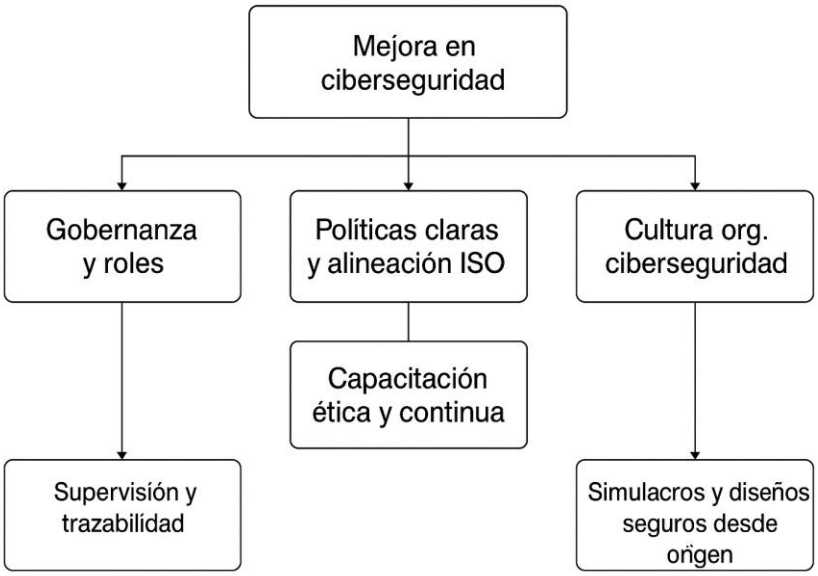
Sujeto	Respuesta
S.1	"Es necesario establecer una política clara y formal de seguridad de información, reforzar los controles técnicos y desarrollar un programa de capacitación continua…"
S. 2	"Debería implementarse una estrategia nacional de ciberseguridad aplicable a todas las instituciones, con estándares mínimos, auditorías periódicas y cursos obligatorios."

S. 3	"Falta sensibilización real. Las capacitaciones deben ser contextualizadas, y no solo técnicas: incorporar la ética digital y escenarios de toma de decisiones sería clave."
S. 4	"Urge fortalecer las políticas de acceso y uso de recursos digitales. Además, los usuarios deberían ser certificados anualmente en competencias básicas de ciber higiene."
S. 5	"Debería haber una mayor integración entre las políticas internas y las normativas internacionales ISO/IEC. Además, es vital tener procesos de respuesta documentados."
S. 6	"Las prácticas están desactualizadas. Se requieren simulaciones regulares de ciberataques, políticas con enfoque de riesgo, y mejoras en la trazabilidad de incidentes."
S. 7	"Se debe consolidar una cultura de la ciberseguridad. No basta con normativas: hay que incorporar la seguridad desde el diseño en todos los sistemas y procesos."
S. 8	"La formación es deficiente. Deberían incluirse módulos gamificados roles de respuesta ante incidentes y aprendizaje colaborativo desde el onboarding de empleados."
S. 9	"Hay debilidad en la supervisión. Las organizaciones necesitan responsables formales en ciberseguridad, métricas claras y evaluación continua de las prácticas existentes."
S. 10	"Se requiere una gobernanza más sólida: con liderazgo desde la alta dirección, definición de roles, y alineación de la ciberseguridad con los objetivos estratégicos."

Fuente: Elaboración propia.

Con fundamento en la información que se explicita en la tabla 21, surgen, desde la apreciación de los encuestados, diferentes áreas, que, bajo su consideración, deben sufrir mejoras, para gestionar una cultura de seguridad cibernética en la empresa, que le garantice la actualización continua y la perdurabilidad en el tiempo y el mercado, resguardando con sigilo, la información sensible que gestiona. En la figura 15, se muestra un esquema de ideas, que expone las consideraciones manifestadas.

Figura N° 15. Áreas de mejora



Fuente: Elaboración propia.

La información plasmada en la figura anterior expresa una preocupación compartida por parte del talento humano que labora en la empresa, sobre la necesidad de establecer políticas que establezca marcos normativos sólido y estratégicos, alineados con normativas internacionales como ISO/IEC. En lo expuesto por los sujetos, se evidencia una brecha en la gobernanza digital y la falta de integración de las políticas organizacionales hacia las diferentes áreas de gestión de la información.

Otro aspecto relevante, consiste en la percepción de vacíos en la capacitación continua y contextualizada del talento humano y la inducción necesaria para que se adopten a los roles y contexto laboral. Se expresan falencias en los módulos de formación continua, en temas esenciales como las habilidades actitudinales y un proceso pedagógico centrado en el protagonismo y metacognición del individuo, de forma humanizada y sostenible.

También expresan la necesidad de establecer controles técnicos y trazabilidad mediante la renovación continua de las herramientas tecnológicas, las auditorias periódicas para la detección

temprana de algún bache y la aplicación de simulacros para evaluar el proceso de respuesta. En cuanto a la cultura organizacional, se percibe la necesidad de instaurar una cultura organizacional sensibilizadora, para que los colaboradores, puedan comprometerse con la visión, misión y valores de la empresa, protegiéndola de los eventos fortuitos de ataques cibernéticos.

Conclusiones del Diagnóstico

Si bien es cierto, en el diagnóstico se detectaron brechas significativas que ponen en riesgo la gestión de la seguridad de la información sensible manejada en la empresa, también se detectan fortalezas que permiten observar la oportunidad contextual para la aplicación de una propuesta de mejora del sistema de gestión de seguridad de la información. En la tabla de doble entrada que se expone a continuación, se extractan esos componentes detectados y que sirven como base para la toma de decisiones, en cuanto a la mejora continua.

Tabla 22. Cuadro de triple entrada (brechas vs. Fortalezas)

Área evaluada	Fortalezas	Brechas o debilidades
Gobernanza y cultura organizacional	-Disposición institucional al diagnóstico - Reconocimiento del valor de la información como activo	- Cultura de seguridad débil - Marcos políticos inestables - Roles de gobernanza no definidos ni transversales
Gestión de accesos	- Identificación clara de zonas críticas - Intención de mejorar los controles	- Controles débiles - Ausencia de autenticación multifactor - Credenciales compartidas o sin rotación periódica
Normativa y políticas internas	- Conocimiento básico sobre ISO/IEC 27001 y 27002. - Iniciativas para alinearse con marcos normativos internacionales	- Falta de formalización de políticas internas - Desalineación con buenas prácticas - Tendencia a la improvisación
Clasificación de la información		- Baja madurez en la gestión de la información - Ausencia de esquemas de etiquetado, segmentación y control

Trazabilidad y monitoreo	- Conciencia sobre la importancia del monitoreo	- Inexistencia de trazabilidad regular - Ausencia de auditorías periódicas - SGSI desvinculado de mejora continua
Infraestructura tecnológica	- Aplicación de herramientas de diagnóstico - Identificación de necesidades de actualización	- Sistemas obsoletos - Falta de herramientas automatizadas - Capas defensivas débiles ante amenazas
Capacitación del personal	- Disposición del personal a participar - Reconocimiento de la necesidad de formación técnica continua	- Falta de módulos formativos integrales - Déficit en habilidades actitudinales - Ausencia de enfoque metacognitivo y contextualizado
Gestión de incidentes	- Identificación de incidentes como prioridad	- Carencia de protocolos claros - Ausencia de simulacros y tiempos de respuesta definidos
Alineación estratégica	- Aplicación de percepción cualitativa como insumo estratégico	- Disparidad entre perspectivas directivas y técnicas - Falta de cohesión entre decisiones operativas y modelo de gestión del riesgo

Fuente: Elaboración propia.

El sondeo integral realizado a SISLOCAR Caldera S.A. permite detectar de forma objetiva y con visión holística, las brechas críticas existentes en la seguridad de la información. Se versó en dos perspectivas puntuales, administrativa-operacional y técnico-funcional. Al aplicar metodologías como la Matriz de Riesgos, Análisis de Brechas (Gap Analysis), todas alineadas con las normas internacionales ISO/IEC 27001 y 27002, se descubren procesos claves, necesarios para el diseño de una propuesta, que realmente responda a los vacíos sobre procesos clave, capacidades técnicas, gestión de accesos, incidentes y políticas organizacionales.

Se logra detectar, espacios marcados y críticos de riesgo digital, pero que se convierte en oportunidad valiosa para restructura la efectividad de la gestión actual y empoderar la gestión del riesgo en la seguridad de la información, en la organización. La corrección de estos baches

visualizados, fortalecen la resiliencia y el bloque común de defesa contra ciber amenazas propias del medio operativo de los datos digitalizados. Es a través de la madurez institucional, que se logra instaurar, reflejos de confianza para garantizar la perdurabilidad operativa.

La situación actual de la empresa contrasta con el modelo deseado, para la mejora de brechas detectadas en las diferentes áreas técnicas-organizacionales y operativas de la organización. Dentro de los principales hallazgos que arroja el diagnóstico, se pueden establecer dimensiones que versan sobre la gobernanza. Según Gómez (2025), la define,

> La gobernanza de la ciberseguridad se refiere a un conjunto de reglas, procedimientos y prácticas que guían la forma en que una organización protege sus datos y sistemas. Garantiza que las iniciativas de ciberseguridad se ajusten a los objetivos de la organización y cumplan con los requisitos legales o del sector. Este marco ayuda a mantener las estrategias de ciberseguridad organizadas y eficaces. (párr. 7).

De acuerdo con lo que establece la definición citada, es necesario empatar con esas reglas establecidas por las normas internacionales, ISO/IEC 27001 y 27002, para instaurar un frente de defenssa que evolucionen junto con las metodologías evolucionadas de las amenazas y ataques mal intencionados que atenten contra la seguridad de los datos que generan la acción empresarial.

También se detectan otras áreas sensibles, que emergen por medio del análisis técnico-operativo, visualizando brechas significativas, que abordan aspectos como la cultura organizacional y la gestión operativa de la información. Todas estas falencias, aumentan la inseguridad organizacional, mediante el riesgo cibernético, limitando la capacidad de respuesta y la efectividad del SGSI.

Debe consensuarse en entre todo el aparato técnico- administrativo y operativo, la necesidad de establecer programas de mitigación proactiva, para hacerle frente a las amenazas constantes de los ciberatacantes, quienes renuevan constantemente su modo de operar. Con la detección de las zonas vulnerables detectadas, se puede establecer un modelo deseado, que permita actualización y monitorio continuo, alineado con las normativas internacionales. Según la CNSD (2024) explica,

> La gestión de riesgos no se trata de eliminar completamente todos los riesgos, ya que esto es prácticamente imposible. En su lugar, se enfoca en entender y definir una tolerancia al riesgo adecuada para la organización, desarrollando estrategias efectivas para abordar estos riesgos y mantener un equilibrio adecuado entre la seguridad y las oportunidades de negocio. (p.4).

Entonces, ante la premisa anterior, la gestión del riesgo no hace referencia a encapsular a la empresa, dentro de un círculo de protección, que no le permita gerenciar sus sistemas operativos, sino, que incluye el fortalecimiento de la seguridad de la información que se manejan mediante una intervención integral y siempre listos para detectar y detener las amenazas emergentes.

El diagnóstico refleja una situación crítica pero factible de correcciones, para asegurar la instauración de normativas que respalden la gestión del riesgo y la subsanación de áreas vulnerables detectadas en a la empresa SISLOCAR Caldera, S.A, para asegurar sus áreas técnico-administrativas y de operación, fortaleciéndolas con herramientas establecidas en las normas 27001:2022 y 27002:2022.

Detección de Brechas

De acuerdo con la Universidad Hispanoamericana (2022), "La determinación de brechas es un proceso crítico para entender la distancia entre la situación actual de una organización y el modelo de operación que se desea alcanzar. En consecuencia, en SISLOCAR Caldera S. A, se evalúan los procedimientos actuales y las prácticas de seguridad de la información gestiona en la empresa, en comparación con cada cláusula de la norma ISO/IEC 27001:2022: tomando en cuenta, el entorno empresarial.

1. Contexto de la Organización,
2. Liderazgo,
3. Planificación,
4. Evaluación del Desempeño,
5. Operación, Mejora.

El objetivo de esta acción consiste en identificar las áreas que presenten oportunidades de mejora y poder determinar las acciones necesarias para el logro de los estándares deseados con el fin de brindarle una herramienta a SISLOCAR, para la adopción de medidas que sean efectivas y logren subsanar las brechas detectadas.

Cláusula de ISO/IEC 27001:2022	**Situación Actual en SISLOCAR**	**Brecha Identificada**	**Acciones Recomendadas**
Contexto de la Organización	SISLOCAR se encuentra en una etapa de análisis de sus prácticas y procedimientos relacionados con la seguridad de la información. Existe voluntad empresarial de aplicar mejoras de estrategias y liderazgo	Ausencia de un SGSI estructurado, falta de políticas y procedimientos formales de seguridad de la información, y falta de integración de herramientas existentes en un marco de gestión estructurado.	Impulsar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) de forma transversal, partiendo del respaldo institucional de la alta dirección y permeando todas las instancias técnicas y operativas de

	en esta materia. Aún no se han establecido formalmente políticas, controles, ni procesos operativos que den soporte estructurado a la gestión de seguridad. Actualmente, la empresa hace uso de tecnologías avanzadas como Microsoft Azure, Elasticsearch y Jira para sus operaciones, sin embargo, no dispone de un Sistema de Gestión de Seguridad de la Información (SGSI) implementado. A pesar de esta ausencia, la percepción del equipo sobre la importancia de la seguridad informática es favorable, lo que representa una oportunidad para institucionalizar buenas prácticas mediante la documentación y normalización de los procedimientos relacionados con la protección de los activos informacionales.		la organización. Establecer, formalizar y dejar por escrito políticas y procedimientos que regulen la seguridad informacional. Asimismo, incorporar las plataformas tecnológicas existentes dentro de la arquitectura del SGSI, garantizando su articulación funcional bajo principios normativos.
Liderazgo	Aunque la estructura gerencial de SISLOCAR, muestra un fuerte compromiso con la seguridad de la información, actualmente no existe una integración formal del SGSI en los procesos de negocio de la organización. Las responsabilidades en materia de seguridad de la información no están oficialmente definidas ni asignadas.	Falta de integración formal del SGSI en los procesos de negocio, y ausencia de roles y responsabilidades claramente definidos para la seguridad de la información.	Formalizar la incorporación del Sistema de Gestión de Seguridad de la Información (SGSI) como parte integral de los procesos corporativos, asegurando su alineación funcional con los objetivos del negocio. Establecer una distribución clara de funciones y atribuciones en materia de seguridad

			informacional, tanto en los niveles directivos como en las áreas operativas. Además, promover un entorno organizacional orientado a la protección de la información, impulsado desde el liderazgo ejecutivo como eje cultural y estratégico.
Planificación	Existe un fuerte compromiso por parte de SISLOCAR, con respecto a la planificación de la seguridad de la información dentro de sus actividades, carece de un enfoque estructurado y documentado para la gestión de objetivos y riesgos de seguridad de la información. No se han realizado evaluaciones de riesgos ni se han definido objetivos de seguridad de la información.	Falta de evaluación de riesgos de seguridad de la información y de un plan de tratamiento de riesgos. Ausencia de objetivos de seguridad de la información y de un plan para alcanzarlos.	Llevar a cabo un análisis exhaustivo de los riesgos asociados a la seguridad de la información, considerando las amenazas, vulnerabilidades y niveles de impacto en función del contexto institucional. A partir de esta evaluación, construir un plan estructurado de tratamiento de riesgos que contemple medidas correctivas, preventivas y de mejora continua. Establecer objetivos de seguridad alineados con la misión y metas organizacionales, garantizando coherencia estratégica. Registrar sistemáticamente tanto el desarrollo del proceso como sus hallazgos, y adoptar una visión proactiva que anticipe escenarios críticos y fortalezca la resiliencia informacional.
Soporte	Aunque SISLOCAR demuestra un compromiso institucional con la seguridad de la información, aún no	Falta de recursos adecuados para el SGSI, falta de formación y concienciación en seguridad de la información,	Diseñar e implementar un programa sistemático de formación y sensibilización que fortalezca el

	dispone de mecanismos formales que aseguren la asignación eficaz y sostenida de recursos para el desarrollo y sostenibilidad del Sistema de Gestión de Seguridad de la Información (SGSI). La organización carece de un programa estructurado de capacitación y sensibilización dirigido a fortalecer la cultura de seguridad entre sus colaboradores. Además, los canales de comunicación sobre temas informacionales y la administración documental vinculada al SGSI presentan debilidades que podrían comprometer su implementación y eficacia operativa. Si deseas, puedo ayudarte a vincular esta sección con cláusulas específicas de ISO/IEC 27001 o generar indicadores para evaluar progresos en gobernanza, formación o comunicación institucional. Me encantaría afinarlo contigo.	comunicación ineficaz sobre seguridad de la información, y control insuficiente de la información documentada.	entendimiento y la aplicación de prácticas seguras en el entorno organizacional. Garantizar la asignación adecuada y continua de recursos financieros, tecnológicos y humanos que respalden la operatividad y evolución del Sistema de Gestión de Seguridad de la Información (SGSI). Establecer mecanismos de comunicación claros y eficaces que faciliten la difusión de políticas y procedimientos relacionados con la seguridad informacional. Además, consolidar un sistema organizado para la gestión de la información documentada vinculada al SGSI, que asegure su trazabilidad, integridad y disponibilidad.
Operación	SISLOCAR aún no ha establecido mecanismos operativos específicos que permitan gestionar la seguridad de la información de forma sistemática dentro de sus procesos cotidianos. La organización no dispone de procedimientos	Ausencia de procesos operacionales para la gestión de riesgos de seguridad de la información y falta de integración de estos procesos en las operaciones diarias.	Diseñar e instaurar protocolos operativos orientados a la identificación, gestión y tratamiento de los riesgos que afectan la seguridad de la información institucional. Integrar estos procedimientos dentro del flujo

	definidos para la identificación, análisis y tratamiento de los riesgos informacionales, ni se evidencia una articulación funcional entre la gestión de riesgos y las actividades operativas. Esta brecha limita la capacidad institucional para prevenir, mitigar y responder proactivamente ante incidentes relacionados con la seguridad informacional.		cotidiano de trabajo, asegurando su aplicabilidad en las prácticas operativas del día a día. Establecer mecanismos de seguimiento y evaluación continua que permitan medir la eficacia de las acciones implementadas, así como realizar ajustes oportunos que fortalezcan la resiliencia del entorno informacional.
Evaluación del Desempeño	Actualmente, SISLOCAR no dispone de estructuras formales que permitan evaluar y supervisar de manera sistemática el rendimiento de su gestión en seguridad de la información. No se han establecido indicadores clave de desempeño que faciliten el seguimiento de logros o brechas en esta materia. Asimismo, la organización carece de un programa de auditoría interna que permita verificar la eficacia de los controles implementados, ni cuenta con un proceso definido para la revisión ejecutiva del Sistema de Gestión de Seguridad de la Información (SGSI), lo que limita su capacidad de mejora continua y ajuste estratégico.	Falta de indicadores de rendimiento para la seguridad de la información, ausencia de un programa de auditoría interna y falta de revisiones de la dirección del SGSI.	Diseñar e incorporar indicadores clave de rendimiento que permitan evaluar de forma objetiva la eficacia de las medidas adoptadas en materia de seguridad de la información. Establecer un programa sistemático de auditorías internas enfocado en verificar la conformidad y el cumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI), así como detectar oportunidades de mejora. Además, consolidar un proceso estructurado de revisión ejecutiva del SGSI que se desarrolle periódicamente, orientado a evaluar resultados, tomar decisiones estratégicas y alinear los objetivos de seguridad con las metas organizacionales.

Mejora	Actualmente, SISLOCAR no ha definido un mecanismo formal que permita asegurar la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). La organización no cuenta con un sistema funcional para el registro, seguimiento y resolución de no conformidades ni de incidentes vinculados a la seguridad informacional. Asimismo, no se ha institucionalizado un proceso periódico de revisión que facilite la evaluación, actualización y adaptación del SGSI conforme a cambios tecnológicos, normativos u organizacionales, lo que limita su capacidad de evolución sostenida.	Ausencia de un proceso de mejora continua, falta de mecanismos para el manejo de no conformidades e incidentes de seguridad, y carencia de un proceso de revisión y adaptación del SGSI.	Diseñar un sistema institucional que permita el registro estructurado y la gestión eficaz de no conformidades e incidentes relacionados con la seguridad de la información. Establecer procedimientos orientados al análisis de causas raíz, con el fin de aplicar medidas correctivas que aborden no solo los síntomas, sino los factores subyacentes. Consolidar un proceso continuo de evaluación del Sistema de Gestión de Seguridad de la Información (SGSI), que incorpore la revisión periódica de los objetivos establecidos y su ajuste conforme a cambios tecnológicos, regulatorios o de contexto organizacional, garantizando su vigencia y pertinencia.

Fuente: Tabla 23 identificación de brechas (2025).

Esta matriz, se convierte en una hoja de ruta para la empresa SISLOCAR Caldera S.A, al señalar las acciones necesarias para ajustar los procesos y alinearlos a las normas estándar ISO/IEC 27001:2022. Tanto las brechas detectadas como las acciones recomendadas deben ser revisadas y ajustadas continuamente en concordancia con la evolución de la empresa.

CAPÍTULO V: PROPUESTA DE PROYECTO

Desarrollo de la Propuesta del proyecto

En esta sección, se presenta la propuesta que tiene como objetivo, implementar mejoras integrales en la seguridad de la información de la empresa SISLOCAR Caldera S.A., ordenadas con los lineamientos establecidos por las normas ISO/IEC 27001 y 27002. Se explicitan detalles y enfoques estratégicos estructurados para con base a los objetivos propuestos y las debilidades detectadas en el diagnostico, se pueda estructurar una solución técnica y operativa, para mitigar la vulnerabilidad y reforzar la protección y gobernanza de la información de la empresa.

Cada sección, se estructura fundamentada en los entregables propuestos, estableciendo las relaciones que sostienen los objetivos específicos, con los hallazgos del diagnóstico y la meta planteada, modelo deseable para implementar mejoras de Seguridad de la información, alineadas con los estándares ISO/IEC 27001 y 27002 para mitigar y gestionar los riesgos cibernéticos en la empresa SISLOCAR Caldera S. A, con un horizonte de ejecución en agosto de 2025.

Además, la propuesta se fundamenta en los hallazgos y debilidades que requieren fortalecerse y el fundamento teórico que los respalda. Cada metodología aplicada, cuenta con la valoración y juicio, mediante estándares de cualificación y cuantificación, que garanticen la confiabilidad de la solución propuesta. Cabe esclarecer, que, en este apartado, el investigador se enfoca, en aquellos aspectos que mantienen una estructura básica para su aplicación, en cuanto a políticas y asesorías, por no ser soporte de esta propuesta, solo se ofrecen recomendaciones puntuales, en la sección correspondiente.

El diseño aplicado a la propuesta se fundamenta en la estructura metodológica que se explicita, en el capítulo III de este documento, para lograr cumplir el objetivo general del proyecto, Implementar mejoras de Seguridad de la información, alineadas con los estándares ISO/IEC 27001 y 27002 para mitigar y gestionar los riesgos cibernéticos en la empresa SISLOCAR Caldera S. A, con un horizonte de ejecución en agosto de 2025.

Fase I: Análisis del Contexto Actual

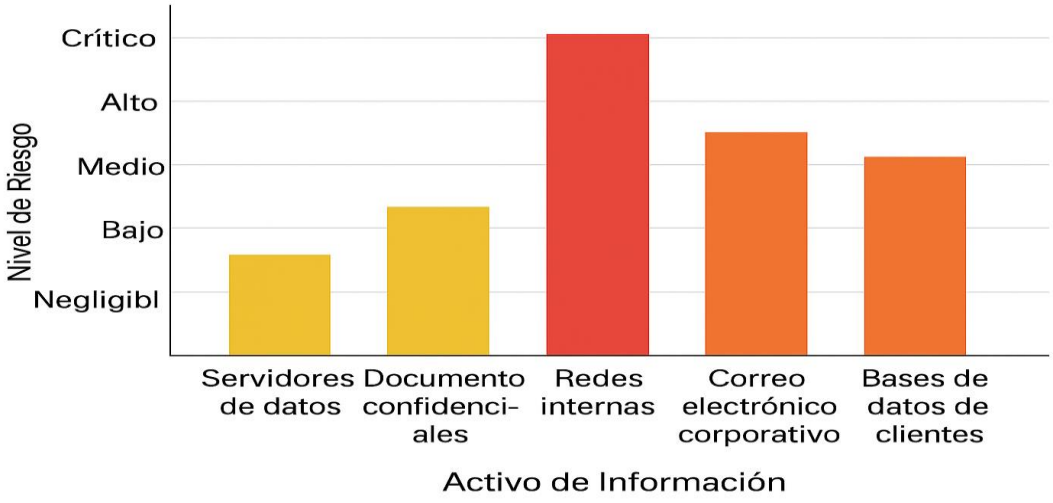
La primera etapa de este proyecto responde al objetivo, Identificar los principales riesgos de seguridad de la información que enfrenta la empresa SISLOCAR Caldera S.A., mediante la evaluación de sus procesos operativos y del manejo de información confidencial, con el propósito

de establecer un diagnóstico que sirva de base para la implementación de controles alineados con los estándares ISO/IEC 27001 y 27002.

Asociando este objetivo con el diagnóstico inicial, se identifican diversas debilidades que requieren una intervención técnica y operativa. La ausencia de mecanismos de autenticación multifactor (MFA) expone la información contenida en el sistema informático, generando vulnerabilidades que podrían ser explotadas para accesos no autorizados. Otra práctica que representa un riesgo es el acceso compartido entre usuarios, sin procesos regulares de renovación o control, lo que debilita la trazabilidad y la responsabilidad individual.

Además, se evidencia la necesidad de fortalecer la gestión del riesgo en la TI, por carencias detectadas en las políticas aplicadas para la clasificación y etiquetado de los datos, conforme al nivel de sensibilidad. Esta omisión limita la capacidad de proteger adecuadamente los datos confidenciales. También identifican vacíos en los mecanismos de control y segmentación de acceso, los cuales permiten puntos de entrada que podrían comprometer de forma significativa la integridad y la confidencialidad de la información gestionada por la empresa. Al aplicar la Matriz de riesgos estructurada con base en los activos de información, amenazas y vulnerabilidades, siguiendo un enfoque alineado con ISO/IEC 2700, se obtienen los siguientes resultados, que pueden visualizarse en el gráfico 2.

Gráfico 2. Matriz de riesgos estructurada con base en los activos de información, amenazas y vulnerabilidades, siguiendo un enfoque alineado con ISO/IEC 2700,

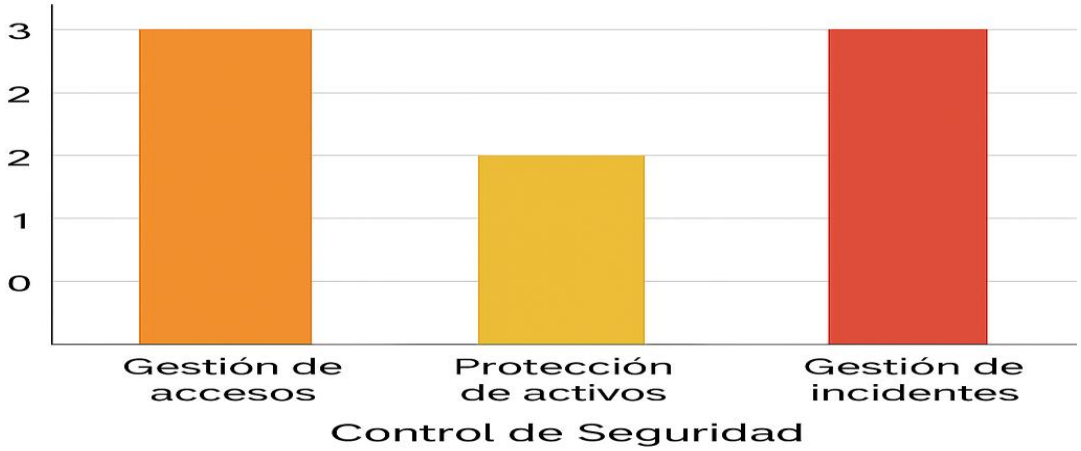


Fuente: Elaboración propia.

En concordancia con la información brindada en el grafico anterior, se logran establecer oportunidades de mejoras, en el contexto de la empresa SISLOCAR, mediante la implementación de estrategias para fortalecer las redes internas y la gestión documental, mediante el manejo ético y la trazabilidad del trasiego de datos. También se debe prestar atención a la infraestructura técnica, la que requiere una gestion adecuada que fortalezca los protocolos de seguridad y la concientización del recurso humano a cargo. Entonces, se debe concatenar la trazabilidad en los procesos y un enfoque de mejora continua. La ausencia de una matriz de seguimiento, valoración y mejoras, para los procesos de Gestión de Seguridad de la Información (SGSI), impide la detección de fallas y la subsanación, así como la prevención de estos eventos en forma oportuna.

En el diagnostico procesado, se aplica el Análisis de Brechas (Gap Analysis) con el objetivo de determinar los riesgos y vulnerabilidades existentes, de acuerdo con los lineamientos de la norma ISO/IEC 27001, detectando así, los activos más comprometidos según sea el nivel de amenaza. En el grafico 3, se logra visualizar el estado actual del contexto empresarial, en cuanto a las brechas detectadas.

Gráfico 3. Brechas detectadas



Fuente: Elaboración propia.

La información que brinda el gráfico anterior determina la necesidad de establecer áreas de mejoras y sostener en alerta, aquellas que están bien desarrolladas. SISLOCAR Caldera, posee un sistema de gestion de acceso estable, pero que puede aceptar mejoras funcionales. Se perciben falencias en la protección de activos, peligrando su exposición a situaciones indeseadas, si no se refuerzan los controles. También se aprecia la necesidad de establecer un equilibrio entre el sistema de seguridad y todos los elementos que confluyen en su fortalecimiento. Los protocolos y controles deben alinearse a las normas estándares establecidas, asegurando la protección del TI en la organización.

Metas Propuestas

Para el abordaje de las debilidades detectadas en el diagnóstico, con respecto a la gestión del riesgo y seguridad de la información confidencial que presenta la empresa SISLOCAR Caldera S.A. la propuesta considera una serie de factores que implementen un sistema ágil y actualizado para el resguardo de datos importantes en la gestión de los datos manejados por la organización.

Fundamentado en lo expuesto en el marco teórico de este proyecto, respecto a la importancia de esta metodología y según lo expuesto por, El Centro Nacional de Seguridad Digital (2021) ofrece una definición acertada, sobre este aspecto.

> La gestión de riesgos de seguridad de la información es el proceso mediante el cual una organización identifica, evalúa y prioriza los riesgos que pueden afectar sus activos de información. Este proceso es esencial para asegurar la confidencialidad, integridad y disponibilidad de la información, permitiendo a la organización cumplir con sus objetivos estratégicos y operativos. (p. 4).

De acuerdo con lo establecido en la cita anterior, que expresa la necesidad de identificar, evaluar y priorizar los riesgos que vulneren los datos gestionados en la empresa. Bajo estos fundamentos, se diseñan las metas propuestas, para ofrecer un proceso de subsano a las situaciones detectadas. En la tabla de triple entrada, número 23, se armonizan dichos aspectos.

Tabla 23. Correlación de aspectos de la propuesta

Datos del diagnóstico	**Metas Planteadas**	**Diseño deseado**
Controles débiles: Ausencia de autenticación multifactor	Implementar autenticación multifactor en todos los sistemas críticos: Autenticación multifactor (MFA) con tokens OTP o apps TOTP	Arquitectura de seguridad basada en roles y control de acceso, según ISO 27002 A.5.17. Cada usuario, debe tener una tarjeta digital, que le autorice el acceso para ingresar únicamente en las funciones que le corresponden. Se aplica una arquitectura de roles, asignando permisos de acuerdo con el puesto que desempeñe la persona,

		evitando el acceso libre a información que no le corresponde.
Credenciales compartidas o sin rotación periódica.	Recomendar políticas de gestión de contraseñas, incluyendo rotación y control de acceso: Directivas de Grupo (GPO) en Active Directory. Gestores de contraseñas (KeePass, Password Manager Pro)	Aplicación de políticas de gestión de identidades y autenticación robustas, de acuerdo con lo establecido en ISO 27002 A.5.17, A. 8.3. Se debe gestionar la seguridad de la información, mediante sistemas de autenticación como, como contraseñas, PINs, claves de cifrado y otros mecanismos que permiten el acceso a sistemas informáticos.
Datos del diagnóstico	**Metas Planteadas**	**Diseño deseado**
Baja madurez en la gestión de la información: Ausencia de esquemas de etiquetado, segmentación y control	Implementar la clasificación y etiquetado de la información según su nivel de sensibilidad mediante el establecimiento de una taxonomía clara.	Catálogo de activos y taxonomía de clasificación de la información, mediante la instauración de un esquema de clasificación basada en los niveles de confidencialidad, integridad y disponibilidad de los datos gestionados. Sistema de gestión de riesgos con matriz de criticidad. (Se deben documentar quienes tienen acceso a la información, realizando revisiones periódicas y otorgando el mínimo privilegio necesario) Todo de acuerdo con lo establecido por ISO 27002 A. 5.12, A. 8.2
Inexistencia de trazabilidad regular - Ausencia de auditorías periódicas	Integrar el ciclo Deming (Planificar-Hacer-Verificar-Actuar) al SGSI para asegurar mejora continua.	Propuesta de auditoría anual con indicadores de desempeño - Plan de mejora continua con revisión trimestral de acuerdo

- SGSI desvinculado de mejora continua	con las normas ISO 27001 y 27002.

Fuente: Elaboración propia.

De acuerdo con la tabla anterior, la propuesta establecer una serie de pasos para la implementación del diseño deseado, que logre subsanar desde la práctica técnica, operativa y administrativa, las debilidades detectadas en el diagnostico. El modelo propuesto pretende convertirse en un sistema de mejora continua en la protección de la información, en la empresa SISLOCAR Caldera S.A. A continuación, se explicitan cada una de las metas propuestas, relacionándolas con aspectos del marco teórico que sustenta esta tesis.

Implementar Autenticación Multifactorial en Todos los Sistemas Críticos

El objetivo de esta propuesta se orienta, al fortalecimiento de la seguridad de acceso a la información mediante la implementación progresiva de autenticación multifactorial en todos los sistemas críticos de SISLOCAR, garantizando la protección de datos sensibles, la trazabilidad de usuarios autorizados y el cumplimiento de estándares internacionales como ISO/IEC 27001 y 27002.

De acuerdo con el diagnóstico realizado, se detectó falencias, en los sistemas de inventarios, plataformas de gestión de proveedores, control de acceso digitales, plataforma integrada de gestión de atención al cliente. Los autenticadores propuestos, multifactor (MFA) con tokens OTP o aplicaciones TOTP, que consiste en establecer más de un factor de verificación e identidad del usuario. Existe diversidad de técnicas, como códigos temporales, huellas digitales y otros que evolucionan conforme a la necesidad de protección de los datos.

El modelo deseado, se fundamenta en la Arquitectura de seguridad, fundamentada en roles y control de accesos relacionados con ISO 27002 A.5.17. Esta metodología, consiste en un enfoque estructurado que asigna los permisos de acceso, de acuerdo con el rol que desempeña cada miembro de la estructura jerárquica de la organización y la autorización de operaciones, según el rol que desempeñe.

La funcionalidad del modelo consiste en la minimización de accesos innecesarios, fundamentados en el principio del mínimo privilegio, teoría expuesta en el marco conceptual de este documento. Facilita las auditorias y trazabilidad de acceso, automatizando la gestión de los permisos necesarios, para el ingreso a la base de datos de la organización. En la siguiente tabla, se presenta la matriz operativa de la propuesta.

Tabla 24. Plan de Implementación de Autenticación Multifactorial (MFA) – SISLOCAR Caldera S.A.

Objetivo General: Fortalecer la seguridad de los sistemas críticos mediante la autenticación multifactorial, garantizando trazabilidad, protección de datos sensibles y cumplimiento de estándares internacionales ISO/IEC 27001 y 27002.

Brecha Detectada	Acción Correctiva	Responsable	Recursos Requeridos	ISO/IEC 27001:2022 – Control	Dominio
Credenciales compartidas y sin rotación	Asignar credenciales únicas y seguras	Área de TI / RRHH	Azure AD, políticas de GPO	A.5.17, A.5.15	Controles de Acceso
Contraseñas débiles o sin cambio periódico	Forzar contraseñas seguras y su renovación cada 90 días	Seguridad Informática	Software de gestión de políticas	A.5.17, A.8.2	Autenticación y Gestión de Identidades
Primer acceso sin actualización	Activar cambio obligatorio en primer login	Área de TI	Política de inicio de sesión	A.5.17	Gestión de Identidades

Objetivo General: Fortalecer la seguridad de los sistemas críticos mediante la autenticación multifactorial, garantizando trazabilidad, protección de datos sensibles y cumplimiento de estándares internacionales ISO/IEC 27001 y 27002.

Brecha Detectada	Acción Correctiva	Responsable	Recursos Requeridos	ISO/IEC 27001:2022 – Control	Dominio
Uso de cuentas genéricas	Prohibir credenciales compartidas, campañas de concientización	Comunicaciones Internas / TI	Material educativo, reuniones	A.6.3, A.7.2	Concienciación y Recursos Humanos
Falta de trazabilidad	Implementar registros de eventos en plantilla alineada a ISO	TI / Auditoría	Plantilla digital, SIEM	A.5.18, A.5.34	Monitorización de Seguridad
Falta de gestión centralizada	Integrar Azure AD como gestor único	Área de Infraestructura	Licencias Azure, capacitación	A.5.15, A.8.3	Gestión de Accesos e Infraestructura

Fuente: Elaboración propia.

Tabla 25. Indicadores de Seguimiento (KPIs)

KPI	Métrica	Meta de Ejecución	Frecuencia
% de sistemas críticos con MFA habilitada	Nº sistemas protegidos / Total sistemas	≥ 90% al cierre Q2 2025	Trimestral
% de cuentas con credenciales únicas	Nº cuentas únicas / Total cuentas	100%	Mensual
Nº de eventos de autenticación registrados	Logs acumulados	100% registro en eventos de acceso crítico	Mensual
Nº de auditorías de credenciales privilegiadas realizadas	Auditorías ejecutadas	≥ 1 revisión anual completa	Anual
% de usuarios que completaron capacitación en MFA	Usuarios capacitados / Total usuarios	≥ 95%	Semestral
Tiempo de respuesta ante incidentes de acceso	Promedio de resolución	< 48 horas	En tiempo real

Fuente: Elaboración propia.

Relacionando el modelo con el control A.5.17 de ISO/IEC 27002, la que establece que se debe gestionar la autentificación de la información, de forma segura, aplicando herramientas informáticas como claves criptográficas, tokens o datos biométricos, mediante la exigencia de alinear los mecanismos de legitimación al acceso, con el rol que desempeña el colaborador en la empresa. Por tanto y al amparo de ese control, la empresa SISLOCAR Caldera S.A, debe:

1. **Asignar credenciales únicas y seguras a cada usuario**: Cada usuario debe recibir un nombre único, evitando denominaciones genéricos o compartidos

2. **Contraseñas seguras desde el inicio:** Generar contraseñas con no menos de 15 caracteres, combinando letras, números y símbolos. El cambio de esta será obligatorio, en caso de sospechas de amenazas. Se debe cambiar el código de acceso, con una periodicidad de no menos de 90 días. Se debe realizar una revisión anual de las llaves digitales por lo menos una vez al año, para comprobar su seguridad, haciendo énfasis en las cuentas con privilegios elevados.

3. **Primer acceso con cambio obligatorio:** Cada cliente recibe un usuario y debe cambiar la contraseña de forma inmediata. El sistema forzará este cambio, verificando que la nueva contraseña, cumpla con los criterios de seguridad.

4. **Evitar credenciales compartidas:** Prohibir el uso de cuentas genéricas. La acción debe responder única y exclusivamente a un usuario especifico, concientizando al beneficiario, sobre la responsabilidad de la seguridad y trazabilidad de la credencial extendida.

5. **Gestión centralizada de credenciales:** Se debe usar un gestor de identidades, (Azure AD), que responde al entorno tecnológico de la organización. Se deben revocar de forma oportuna, las credenciales en casos de incidentes detectados.

6. **Registro de Eventos**: Los eventos que sucedan en la autenticación se registran en una plantilla diseñada para ese efecto, alineada con los requisitos de la norma ISO/IEC 27001. A continuación, se expone la plantilla recomendada.

Plantilla de Registro de Eventos de Autenticación, SISLOCAR SGSI

Fecha y hora del evento: [AAAA-MM-DD HH:MM:SS]

Usuario: [nombre. Usuario]

ID de sesión: [ID único generado]

Ubicación geográfica: [País / Ciudad / IP geolocalizada]

Dispositivo: [Tipo / SO / Navegador]

Tipo de evento: [LOGIN_SUCCESS / LOGIN_FAILURE / LOGOUT / MFA_TRIGGER / PASSWORD_CHANGE]

Método de autenticación: [Contraseña / MFA / Token / Biometría]

Dirección IP: [IPv4 / IPv6]

Resultado: [Éxito / Fallo / Bloqueo]

Descripción técnica: [Detalles del evento, errores, códigos]

Evaluación de riesgo: [Bajo / Medio / Alto]

Acción tomada: [Ninguna / Alerta enviada / Cuenta bloqueada / Revisión manual] Responsable de revisión: [Nombre del auditor interno]

7. Protección de la transmisión y almacenamiento de credenciales: Se aborda con medidas técnicas estructuradas y específicas que permiten garantizar la confidencialidad, integridad y disponibilidad de la información generada. Para este efecto, se toman acciones puntuales que se exponen en la siguiente matriz.

Tabla 26. Matriz de acciones para proteger credenciales según ISO/IEC 27001:2022

Aspecto	***Medidas aplicadas***
Transmisión segura	- Usar canales cifrados (ej. TLS/SSL) para enviar contraseñas o tokens.
	- Evitar el envío por correo electrónico en texto plano.
Almacenamiento seguro	- Aplicar técnicas de hash criptográfico (ej. bcrypt, PBKDF2) para contraseñas.
	- No almacenar contraseñas en texto claro.
	- Usar módulos de seguridad certificados (HSM) para claves criptográficas.
Asignación de credenciales	- Generar contraseñas únicas y no adivinables.
	- Cambiar credenciales predeterminadas al instalar sistemas.
Gestión de eventos	- Registrar eventos relacionados con autenticación en sistemas seguros.
	- Mantener registros confidenciales y accesibles solo a personal autorizado.
Responsabilidad del usuario	- No compartir credenciales.
	- Cambiar contraseñas tras incidentes o sospechas de compromiso.
	- Usar contraseñas robustas y únicas para cada servicio.

Fuente: datos tomados de ISO/IEC 27001:2022.

8. Establecer procedimientos para revocar accesos: Cuando ya no se necesiten este tipo de credenciales, se debe identificar los eventos que causen esta condición, ya sea por cese laboral, cambio de rol, conclusión de proyectos temporales o asignaciones especiales, o incumplimiento de las políticas de seguridad. Esta gestión integra los siguientes procesos:

A) Notificación Formal: Esta se realiza mediante el llenado del siguiente formulario:

1. Información General de la Solicitud

a) Nombre del solicitante:
b) Departamento / Unidad Organizativa:
c) Cargo actual:
d) Fecha de solicitud:
e) Código interno (si aplica):

2. Justificación Formal

☐ Cese laboral (adjuntar carta de finalización del vínculo laboral)
☐ Cambio de puesto (adjuntar resolución administrativa o circular interna)
☐ Finalización de proyecto temporal (incluir código y nombre del proyecto)
☐ Incumplimiento de políticas del SGSI (referencia a protocolo específico)
☐ Otro motivo (describir y adjuntar documentos de respaldo).

3. Recursos Tecnológicos y Físicos a Revocar

☐ Correo electrónico.
☐ Acceso a sistemas SGSI, ERP, CRM, servidores internos
☐ Llaves físicas / tarjetas magnéticas / biométricos
☐ Equipos asignados (modelo, código de inventario)
☐ Credenciales digitales (tokens, certificados, VPN)
☐ Otros activos (especificar): _____

4. Fechas Clave

- Fecha del evento que origina la revocación: ____
- Fecha solicitada para ejecución: ____ (máximo 24 horas después del evento)

5. Validación Técnica y Documentación

- Nombre del responsable de TI/Security:
- Firma digital o aprobación electrónica:
- Evidencia de ejecución (logs, capturas, registros en Bitácora SGSI)

B. Verificación por Seguridad de la Información de SISLOCAR: Esta verificación se realiza aplicando la plantilla institucional diseñada para la validación y cierre del proceso de revocación de accesos.

Sección 1: Verificación Final

- **a) Nombre del Verificador/a: _____**
- **b) Observaciones Adicionales:**
- **c) Firma Digital y Número de Registro SGSI: _____**

Sección 2: Acciones Técnicas Ejecutadas

Acción	**Responsable Técnico**	**Fecha Ejecución**	**Evidencia Adjunta**
d) Realizar backups necesarios			☐ Logs ☐ Capturas
e) Eliminar/deshabilitar usuarios			☐ Logs ☐ Capturas
f) Revocar certificados/credenciales			☐ Logs ☐ Capturas

Acción	Responsable Técnico	Fecha Ejecución	Evidencia Adjunta

Tipo de evidencia registrada:

☐ Logs del sistema

☐ Capturas de pantalla

☐ Confirmaciones por correo

☐ Bitácora SGSI

☐ Otros: _____

Sección 3: Retroalimentación y Mejora Continua

- **Incidencias detectadas en el proceso:**
- **Recomendaciones para mejora de protocolo:**
- **¿Se ha informado al equipo responsable sobre estas recomendaciones?** ☐ Sí ☐ No
- **Registro de capacitación continúa relacionada con este procedimiento:**

  ☐ Fecha: //____

  ☐ Tema abordado: _____

  ☐ Participantes: _____

Políticas de Gestión de Contraseñas

En esta fase de la propuesta, se establece el objetivo de recomendar políticas robustas de gestión de contraseñas en SISLOCAR, garantizando prácticas seguras de creación, almacenamiento, uso y renovación, en concordancia con los controles de autenticación definidos por ISO/IEC 27001 y 27002, y promoviendo una cultura organizacional de responsabilidad en el acceso a la información.

Se recomienda establecer una política para la gestión de contraseñas, concordante con buenas prácticas internacionales propuestas en ISO/IEC 27001 y 27002. En la siguiente matriz, se visualizan las acciones a seguir en la implementación de las normativas. En la siguiente matriz, se operacionalizan los procesos.

Tabla 27. Operacionalización de las acciones de gestión de contraseñas

Componente	Objetivo del Plan	Acciones Concretas	Responsable	Recursos Requeridos	Referencia a Control ISO/IEC 27001:2022	Control/Dominio ISO 27001:2022	Indicador de Seguimiento (KPI)
3.1 Creación de Contraseñas	Garantizar la generación segura, única y robusta de contraseñas para todo acceso a sistemas críticos.	- Implementar reglas de complejidad - Forzar autenticación multifactor - Establecer directrices en inducción y formación	Líder de Seguridad TIC	Guías de configuración Plataformas MFA Materiales de capacitación	A.9.2.4 - Gestión de credenciales de usuario	A.9 Control de acceso	% de cuentas con contraseñas que cumplen estándar % de sistemas con MFA habilitado Evaluaciones post-capacitación
3.2 Almacenamiento	Garantizar que las contraseñas se almacenen de forma segura y no sean recuperables en texto plano.	- Encriptar contraseñas - Utilizar sistemas con hash y sal - Auditar ficheros y bases de datos	Equipo de Infraestructura	Software de cifrado Herramientas de auditoría	A.10.1 - Criptografía A.8.2.2 - Protección de datos en reposo	A.10 Criptografía A.8 Protección de activos	% de contraseñas cifradas correctamente % de sistemas con hash validado Alertas por hallazgos en auditoría
3.3 Renovación	Definir políticas de renovación periódica de contraseñas y reforzar su cumplimiento	- Establecer ciclos automáticos de renovación - Sensibilizar a usuarios sobre riesgos	Líder de Gobernanza SGSI	Plataforma de gestión de identidades Boletines internos de sensibilización	A.9.4.3 - Uso de credenciales	A.9 Control de acceso	% de usuarios que renuevan contraseña dentro del plazo Incidencias por incumplimiento Retención de

Componente	Objetivo del Plan	Acciones Concretas	Responsable	Recursos Requeridos	Referencia a Control ISO/IEC 27001:2022	Control/Dominio ISO 27001:2022	Indicador de Seguimiento (KPI)
	para reducir riesgos de compromiso.	- Monitorear incumplimientos					mensajes formativos
3.4 Uso de Contraseñas	Establecer prácticas seguras de uso, evitando compartir contraseñas o su reutilización en sistemas personales.	- Implementar controles para detectar uso indebido - Promover campañas educativas - Incluir cláusulas en políticas institucionales	Comité de Cultura Digital	Sistema de monitoreo de eventos Recursos formativos Apoyo legal	A.7.2.2 - Concienciación sobre seguridad A.13.1.1 - Protección de redes	A.7 Recursos humanos A.13 Seguridad de comunicaciones	% de usuarios capacitados sobre uso responsable % de incidentes relacionados con uso indebido Integración en auditorías internas

Fuente: Datos tomados de la norma ISO/IEC 27001 y 27002.

Baja Madurez en la Gestión de la Información

Haciendo referencia a la gestión de la información, se plantea el objetivo: Mejorar progresivamente la madurez en la gestión de la información en SISLOCAR, fortaleciendo la estructura documental, la trazabilidad de los datos y la capacidad de análisis, mediante la implementación de políticas claras, herramientas tecnológicas adecuadas y una cultura organizacional orientada al uso estratégico de la información. Se recomienda el etiquetado de la información, para vigorizar los activos informativos.

Todo el proceso se ajusta a los controles A. 5.12 y la A. 5.13, de la norma ISO/IEC 27001:2022. La primera interfaz, expone la necesidad de utilizar criterios prestablecidos para la agrupación de la información gestionada, para evitar el riesgo. Consecuentemente, la A. 5. 13, establece la identificación de los datos digitales, mediante el rotulado adecuado.

En la propuesta se persigue, la implementación de clasificación y etiquetado de la información mediante el establecimiento de una taxonomía que considere, el nivel de sensibilidad, para su clasificación, La metodología propuesta para este proceso se establece en etapas que correlacionen procesos estructurados y sistemáticos.

1. Fase 1. Identificación de activos de información, (sistemas y bases de datos).
2. Fase 2. Creación de una taxonomía de clasificación de la información, de acuerdo con su nivel de sensibilidad. (publica, interna, confidencial, altamente confidencial).
3. Fase 3. Etiquetado de la información, aplicando el software del sistema ECM (Enterprise Content Management).
4. Fase 4. Definición de controles, (cifrado, control de acceso, trazabilidad y respaldo de la información).

En el contexto de la Fase 3 que mencionas el etiquetado de la información mediante un sistema ECM, SISLOCAR tendría que adquirir o integrar una solución ECM, que le permita no solo el almacenaje de documentos, sino también, el control de los ciclos de vida de estos, con el fin de asegurar una Esto sería clave para asegurar una gestión documental robusta.

En respuesta de las inconsistencias arrojadas en el diagnóstico, se propone la instauración de estrategias de ciberseguridad, atinentes a la prevención de pérdida o fuga de datos sensibles en la organización. El modelo deseado se fundamenta em el sistema Prevención de Pérdida de Datos (DLP) para el monitoreo de fluctuación de datos en correos y dispositivos electrónicos para la prevención de filtraciones indeseadas.

Tabla 28. Matriz operativa para la clasificación y etiquetado de la información

Fase	Objetivo del Plan	Acciones Concretas	Responsable	Recursos Requeridos	Referencia ISO/IEC 27001:2022	Control/Dominio ISO 27001:2022	Indicador de Seguimiento (KPIs)
1. Identificación de activos	Mapear todos los sistemas y bases de datos que contienen información institucional relevante.	- Inventariar activos - Clasificar según criticidad - Validar propietarios - Documentar ubicación y accesos	Área de Infraestructura	Herramientas de inventario Plantillas de registro	A.5.9 - Inventario de información A.8.1.1 - Inventario de activos	A.5 Liderazgo A.8 Protección de activos	% de activos registrados % de propietarios validados % de activos clasificados por criticidad
2. Creación de taxonomía de clasificación	Establecer una tipología que defina el nivel de sensibilidad (pública, interna, confidencial,	- Diseñar criterios - Validar con stakeholders - Aprobar con comité de gobernanza - Incorporar en	Comité de Gobernanza SGSI	Documentación guía Sesiones con equipos clave	A.5.7 - Clasificación de información A.5.8 - Etiquetado	A.5 Liderazgo	% de áreas con criterios definidos % de aprobación formal % de usuarios

	altamente confidencial).	políticas organizativas					capacitados en clasificación
3. Etiquetado con sistema ECM	Etiquetar toda información institucional en función de la taxonomía definida utilizando el sistema ECM.	- Configurar metadatos - Integrar etiquetas - Automatizar según tipo de documento - Validar consistencia	Equipo de Gestión Documental	Licencia de sistema ECM Guía de configuración. De acuerdo con la razón social de SISLOCAR Caldera S.A. Cuya actividad principal es la gestión de almacenamiento fiscal, ofreciendo	A.5.8 - Etiquetado A.8.2.3 - Protección de datos procesados	A.8 Protección de activos	% de documentos etiquetados % de etiquetas correctas % de automatización implementada

				soluciones para el bodegaje de almacenamiento de mercadería, se hace necesario, la implementación de una licencia de sistema ECM, para mejorar la trazabilidad documental, mediante el etiquetado,			

				clasificación, y localización oportuna de los datos en tránsito. Además, refuerza la seguridad y control de acceso, a la data de la organización, de acuerdo con lo establecido por ISO/IEC 27001.			

4. Definición de controles	Aplicar medidas técnicas y organizativas para proteger la información según su nivel de sensibilidad.	- Cifrado por nivel - Control de acceso basado en roles - Trazabilidad de modificaciones - Respaldo periódico	Líder de Seguridad TIC	Software de cifrado Sistemas de monitoreo Soluciones de respaldo	A.10 - Criptografía A.9 - Control de acceso A.12.4.1 - Registros de auditoría	A.9 Control de acceso A.10 Criptografía A.12 Operaciones	% de datos cifrados % de accesos basados en rol % de trazabilidad activa % de respaldos validados

Fuente: Elaboración propia.

Trazabilidad Irregular

Las falencias detectadas en la gestión del riesgo en el trasiego y manejo de la información en SISLOCAR Caldera S. A, presentan inconsistencias en la transversalización de eventos, acceso y modificaciones que se aplican a la información gestionada. Esto impide la verificación de eventos, en tiempo y forma, para mitigar los embates de las amenazas cibernéticas.

Para la salvaguarda de esta debilidad, se le recomienda a la organización, la planificación de revisiones programadas, en forma trimestral, mediante auditorías internas o externas, que le permitan visualizar las desviaciones, brechas o intentos de alteración, de forma oportuna para la toma de decisiones optimas.

Se diseña un plan de mejora continua, con revisión trimestral, alineado con lo establecido en las normas ISO/IEC 27001:2022 **y** ISO/IEC 27002:2022, para el fortalecimiento de SGSI de SISLOCAR Caldera S.A. En dicha propuesta, se integra también el ciclo Deming, abordado en el capítulo II de este documento, como referente teórico. Los procesos y fases se exponen en la matriz de la tabla 29, de la propuesta diseñada para la implementación de la mejora continua.

Tabla 29. Matriz operacional para clasificación y trazabilidad de activos

Fase PDCA	Objetivo Específico	Actividades Clave	Indicador SMART	Responsable	Recursos Requeridos	Controles ISO/IEC 27001:2022	Dominio ISO/IEC 27001:2022
Planificar	Establecer mecanismos de trazabilidad confiable y verificable mediante registros automatizados	- Identificar activos - Clasificar la información - Evaluar riesgos con matriz de criticidad	Aumentar al 98% la trazabilidad efectiva de activos críticos con registros automatizados	Área de Infraestructura	Inventario digital Plantillas de clasificación Herramientas de evaluación	A.5.9, A.8.1.1, A.6.1.2	A.5, A.6, A.8
Hacer	Implementar controles para trazabilidad, clasificación y capacitación del personal	- Etiquetar activos - Clasificar activos con taxonomía - Capacitar en ciberseguridad - Recomendar módulos formativos	- 100% de activos clasificados según sensibilidad - Implementar 4 módulos de formación sobre seguridad	Líder SGSI / RRHH	Software ECM Guía taxonómica Materiales didácticos	A.5.7, A.5.8, A.6.1.2, A.7.2.2, A.18.2.2	A.5, A.6, A.7, A.18
Verificar	Validar trazabilidad y realizar revisión periódica para	- Simulacros de respuesta - Revisión de indicadores - Verificación de	Realizar 4 revisiones trimestrales del SGSI, documentando	Comité de Seguridad SGSI	Informes de auditoría Protocolos de simulacro	A.12.4.1, A.14.2.9, A.5.8	A.5, A.12, A.14

Fase PDCA	Objetivo Específico	Actividades Clave	Indicador SMART	Responsable	Recursos Requeridos	Controles ISO/IEC 27001:2022	Dominio ISO/IEC 27001:2022
	detectar ajustes y amenazas	trazabilidad - Generar informes con hallazgos	hallazgos y acciones correctivas		Panel de indicadores		
Actuar	Actualizar taxonomías y controles según hallazgos para mejora continua del SGSI	- Revisar políticas - Rediseñar procesos críticos - Documentar acciones correctivas	Revisar y actualizar el 100% de las taxonomías de clasificación y controles del SGSI	Dirección SGSI	Actas de revisión Planes de acción Documentación normativa	A.5.6, A.5.7, A.5.8, A.18.2.2	A.5, A.18

Fuente: elaboración propia.

Fase II. Control de Acceso y Protección de Datos

Esta fase 2, el diagnóstico aplicado para la detección de debilidades en los mecanismos actuales de control de acceso y protección de datos, en la empresa SISLOCAR Caldera S.A. Responde al objetivo propuesto: Analizar las debilidades en los mecanismos actuales de control de accesos y protección de datos sensibles, mediante la revisión de políticas internas, tecnologías empleadas y prácticas vigentes en la empresa, con el fin de orientar mejoras que reduzcan la exposición a riesgos cibernéticos.

En esta propuesta de mejora, del sistema de gestión de seguridad de la información, basada en los lineamientos de las normas ISO/IEC 27001 y 27002, se promueve la inclusión de controles específicos para el acceso y la protección de datos, con la finalidad de mitigar los riesgos de accesos no autorizados y la vulneración de información crítica. Se fundamenta en la creación documental, de elementos necesarios para convertir en efectivo, el SGSI de la organización.

Política de Seguridad de la Información

La empresa SISLOCAR Caldera S. A, reconoce a través de sus jerarquías de mando superior, la necesidad de contar con un sistema operativo, que resguarde la información virtual, fundamental para la continuidad de sistema de negocio aplicado. También consienten en la necesidad de obtener beneficios bipartitos, tanto para la organización como para la clientela, accionistas y otros integrados, de un entorno informático, robusto. Es importante asegurar una política eficiente que garantice la continuidad del proceso comercial.

De acuerdo con lo expuesto en el apartado teórico de este proyecto, la Norma Internacional para la Seguridad de la Información, ISO/IEC 27001:2022, define un sistema de Gestión de Seguridad de la información, (SGSI), basado en la aplicación de las mejores prácticas reconocidas

en el ámbito mundial. Parte de una conciencia por parte de la organización, para adquirir un compromiso en la aplicación de gestiones que aseguren la protección, la confidencialidad, integridad y disponibilidad de los datos, en la operación empresarial.

Requisitos de Seguridad de la Información

SISLOCAR Caldera S.A, se compromete a establecer y mantener claridad, sobre los requisitos y aplicabilidad de estos, para la gestión del riesgo de la información, de forma inherente a su ADN comercial. Su preocupación se dirige, hacia el mantenimiento del SGSI, robusto y en constante monitoreo, mediante el cumplimiento de los requisitos estatutarios, regulatorios y contractuales, niveles indispensables integrados en la planificación organizacional. También inserta la importancia de socializar la información, con el talento humano referente.

Para la implementación de los objetivos sobre la seguridad de la información gestionada en la organización, se recurre a un ciclo alineado con la planificación presupuestaria de SISLOCAR, con la finalidad de obtener el financiamiento presupuestario para la ejecución de las acciones emergentes de los propósitos planeados. En la matriz de la tabla 30, se expone la hoja de ruta operacional.

Tabla 30. Matriz Mejora Continua del SGSI

Fase PDCA	Objetivo Específico	Actividades Clave	Indicadores SMART	Responsable	Recursos Requeridos	Controles ISO/IEC 27001:2022	Dominio ISO/IEC 27001:2022
Planificar	Alinear el SGSI con buenas prácticas y certificarlo bajo ISO/IEC 27001:2022	- Revisión de políticas existentes - Diagnóstico normativo - Identificación de métricas relevantes - Revisión de procesos y controles actuales	Alcanzar el 100% de alineación documental con ISO/IEC 27001:2022 Identificar brechas de conformidad en <30 días	Líder SGSI / Dirección	Documento normativo Históricos de métricas Guías ISO	A.5.1, A.5.2, A.9.1.1, A.5.6	A.5 Liderazgo A.9 Control de acceso
Hacer	Implementar políticas específicas en materia de seguridad de la información	- Redacción de políticas: • Uso Aceptable • Teletrabajo • Móviles • Computación en	Crear y aprobar 100% de políticas de seguridad aplicables Integrarlas en el SGSI institucional	Comité de Redacción / Jurídico	Normativa interna Modelos de política Capacitaciones	A.5.1, A.6.1.1, A.13.2.1, A.14.1.1	A.5, A.6, A.13, A.14

Fase PDCA	Objetivo Específico	Actividades Clave	Indicadores SMART	Responsable	Recursos Requeridos	Controles ISO/IEC 27001:2022	Dominio ISO/IEC 27001:2022
		la nube • Criptografía • Software malicioso • Respaldo • Proveedores					
Hacer	Asegurar la aplicación transversal de la política de seguridad a todos los públicos internos y externos	- Comunicación organizacional - Capacitaciones regulares - Revisión de contratos - Inclusión de cláusulas normativas en onboarding	100% de empleados capacitados anualmente 100% de contratos actualizados con cláusulas de seguridad	RRHH / Área Legal	Módulos de formación Portal de aprendizaje Plantillas contractuales	A.7.2.2, A.6.3.1, A.18.1.1	A.6, A.7, A.18

Fase PDCA	Objetivo Específico	Actividades Clave	Indicadores SMART	Responsable	Recursos Requeridos	Controles ISO/IEC 27001:2022	Dominio ISO/IEC 27001:2022
Verificar	Medir, revisar y ajustar las métricas relevantes del SGSI mediante monitoreo periódico	- Recopilación de datos - Análisis de efectividad - Generación de informes - Validación con dirección	Realizar 1 revisión anual de métricas Actualizar indicadores al menos 1 vez por año con evidencia documentada	Comité SGSI / Dirección	Dashboards Historial de métricas Plantillas de evaluación	A.9.2.1, A.12.4.1, A.5.8	A.5, A.9, A.12
Actuar	Establecer mecanismos participativos para la mejora continua del SGSI, involucrando a partes interesadas	- Reuniones periódicas - Recolección de ideas - Evaluación por comité de gestión - Priorización de mejoras	Incorporar al menos 3 propuestas de mejora cada año al SGSI Realizar 100% de reuniones programadas	Dirección SGSI / Comité Gestión	Formato de propuesta Actas de reunión Sistema de priorización	A.5.3, A.5.6, A.10.1.1	A.5, A.10

Fuente: Elaboración propia.

Tabla 31. Matriz hoja de ruta operacional

Aspecto	Procesos
Mejora Continua del SGSI	La política de SISLOCAR en relación con la mejora continua del SGSI incluye: Mejorar continuamente la efectividad del SGSI, alineándolo con las buenas prácticas definidas dentro de ISO/IEC 27001:2022 y las normas relacionadas. Mantener y mejorar la certificación de ISO/IEC 27001:2022 en un ciclo constante, asegurando una gestión proactiva de la seguridad de la información que refleje positivamente en la percepción de los interesados. Aumentar la proactividad en seguridad de la información para proporcionar una base sólida para decisiones informadas, haciendo los procesos y controles de seguridad de la información más medibles. Revisar anualmente las métricas relevantes para evaluar si es apropiado modificarlas, basándose en datos históricos y su eficacia. Fomentar la obtención de ideas para la mejora a través de reuniones regulares y otras formas de comunicación con las partes interesadas. Evaluar y revisar las ideas de mejora en las reuniones de gestión para priorizarlas y evaluar los beneficios y plazos. Estas pueden surgir de diferentes tipos de fuentes involucrados en el proceso empresarial, tanto en el contexto interno como el externo.
Áreas de Políticas de Seguridad de la Información	La empresa establece directrices específicas en diversas áreas vinculadas a la seguridad de la información. Estas se desarrollan en un conjunto articulado de documentos que complementan y fortalecen el marco normativo general en esta materia. Estas políticas incluyen: Política de Uso Aceptable de Internet, Política de Computación en la Nube, Política de Dispositivos Móviles, Política de Teletrabajo, Política de Uso Aceptable, Política de Prevención de Software Malicioso, Política de Criptografía, Política de Respaldo, Política de Seguridad de la Información para relaciones con proveedores.
Aplicación de la Política de Seguridad de la Información	La Política de Seguridad de la Información, es aplicable a todos los empleados, contratistas y terceros asociados. Es responsabilidad de cada uno adherirse a esta política y estar informado sobre sus obligaciones y responsabilidades en materia de seguridad de la información. Se proporciona formación regular para asegurar el conocimiento y la comprensión de la política por parte de todos los involucrados.

Fuente: Elaboración propia.

Política de Seguridad de la Información para Relaciones con Proveedores

El entorno de la empresa SISLOCAR Caldera S.A, se encuentra inmerso en el mundo de los negocios, contando como activo principal sus clientes, proveedores y talento humano. De acuerdo con exposiciones teóricas fundamentadas, los proveedores pueden convertirse en un riesgo latente, si existen brechas de seguridad de la información. La Comisión Federal de Comercio del Gobierno de los Estados Unidos (2019) recomienda, "Establezca controles en las bases de datos que contengan información delicada. Limite el acceso según lo que sea necesario que sepa cada proveedor, y sólo por la cantidad de tiempo que el proveedor lo necesite para hacer un trabajo" (párr. 5).

De acuerdo con la teoría expuesta en la cita anterior, es primordial que la empresa, elabore una política comprensiva y clara, para el manejo de la información con respecto a sus proveedores. Esta debe establecer las expectativas y requisitos de la organización en cuanto al gestión de la seguridad informática. Todas estas normativas, deben documentarse, socializarse, para obtener el compromiso de los usuarios, para el mantenimiento de controles efectivos. En la tabla 32, se presenta la matriz correspondiente a la instauración de estos procesos.

Tabla 31. Matriz hoja de ruta operacional

Objetivo: Establecer los lineamientos y requisitos mínimos que regulen la protección de los activos de información institucional en toda relación contractual con proveedores y terceros, dentro del entorno operativo y estratégico de SISLOCAR Caldera S.A.
Responsables: responsable del SGSI y área legal.

Aspecto	**Procesos**
Disposiciones Generales	Con el propósito de garantizar la protección de los activos de información durante la gestión con terceros, SISLOCAR Caldera S.A. establece esta política para regular los requisitos mínimos de seguridad aplicables en las relaciones contractuales con proveedores. El alcance incluye cualquier parte externa que, en el marco de un servicio prestado, acceda, procese, almacene o gestione información clasificada bajo criterios institucionales. La implementación de esta política considera los siguientes elementos estructurales: Los requisitos y controles de seguridad de la información deben documentarse formalmente en un acuerdo contractual que puede ser parte de, o un anexo al, contrato comercial principal. Es necesario garantizar que todos los acuerdos con proveedores incluyan cláusulas específicas de seguridad de la información, estableciendo responsabilidades y expectativas claras. Se deben utilizar Acuerdos de No Divulgación separados cuando se requiera un nivel más específico de control sobre la confidencialidad. Se debe ejercer la debida diligencia apropiada en la selección y aprobación de nuevos proveedores antes de acordar los contratos. Las disposiciones de seguridad de la información en los proveedores existentes (donde no se realizó la debida diligencia como parte de la selección inicial) deben ser claramente entendidas y mejoradas cuando sea necesario. El acceso remoto por parte de los proveedores debe ser a través de métodos aprobados que cumplan con las políticas de seguridad de la información de la organización. El acceso a la información de SISLOCAR Caldera S.A debe limitarse, cuando sea posible, según la necesidad clara del negocio. Se deben aplicar principios básicos de seguridad de la información como el mínimo privilegio, la separación de funciones y la defensa en profundidad. Se espera que el proveedor ejerza un control adecuado sobre las políticas y procedimientos de seguridad de la información utilizados

	dentro de los subcontratistas que participan en la cadena de suministro de entrega de bienes o servicios a SISLOCAR Caldera S.A SISLOCAR Caldera S.A tendrá el derecho de auditar las prácticas de seguridad de la información del proveedor y, cuando sea apropiado, de los subcontratistas. Se deben establecer arreglos de gestión de incidentes y contingencias basados en los resultados de una evaluación de riesgos. Se debe implementar un proceso regular de revisión y evaluación del desempeño de los proveedores en términos de seguridad de la información, incluyendo auditorías periódicas y evaluaciones de cumplimiento. Se deben establecer procedimientos para manejar cualquier cambio en los servicios proporcionados por los proveedores, asegurando que cualquier modificación no comprometa la seguridad de la información. La capacitación en concienciación será llevada a cabo por ambas partes del acuerdo, basada en los procesos y procedimientos definidos. La selección de controles requeridos debe basarse en una evaluación de riesgos integral teniendo en cuenta los requisitos de seguridad de la información, acorde con lo establecido en la norma ISO/IEC 27001:2022 y sus controles correlativos en ISO/IEC 27002, particularmente en materia de control de accesos (A.9), protección de activos (A.5.11–A.5.16) y gestión de vulnerabilidades (A.8.9) con el objetivo de evaluar, el producto o servicio a suministrar, su criticidad para la organización y las capacidades del proveedor para el cumplimiento de estas políticas.

Fuente: Elaboración propia.

Política de Seguridad de la Información Referente al Talento Humano

Esta política tiene como finalidad norma el uso de internet en el campo de acción de los colaboradores, para garantizar el uso adecuado de este servicio, provistos por SISLOCAR, en el marco de sus funciones profesionales. Es importante que cada persona usuaria de la red conozca sus responsabilidades y tenga claridad sobre los comportamientos aceptables y aquellos que deben

evitarse, con el fin de proteger la seguridad de la información y garantizar un entorno digital responsable.

La infraestructura de Internet está disponible para apoyar las actividades comerciales y operativas de la empresa. Se reconoce que puede existir cierto uso personal ocasional, siempre que sea razonable, respetuoso y no afecte el desempeño ni la integridad de los sistemas. Esta política aplica a todos los canales de conectividad facilitados por SISLOCAR, incluyendo redes internas, acceso remoto y dispositivos móviles autorizados. El cumplimiento de estas directrices contribuye a mantener un entorno seguro y alineado con los valores de la organización. En la tabla 27, se muestra la matriz de ruta operacional.

Tabla 32. Matriz hoja de ruta operacional

Objetivo: Establecer las directrices que aseguren el comportamiento responsable, ético y seguro del talento humano en todas las etapas de su relación laboral con SISLOCAR Caldera S.A., promoviendo la protección de los activos de información institucional. **Responsables:** Alta gerencia, encargado del SGSI y Departamento de Recursos Humanos.	
Aspecto	**Procesos**
Uso de Negocio del Servicio de Internet	El acceso a Internet por parte de los empleados está destinado exclusivamente a actividades laborales que contribuyan al cumplimiento de los objetivos de la organización. Entre los usos permitidos se incluyen: • Consultar información relevante que respalde el desarrollo de sus funciones y responsabilidades. • Actualizar o gestionar los sitios web que pertenecen o son administrados por la organización. • Realizar transacciones electrónicas necesarias para la operación de la organización. • Acceso a información relevante para cumplir con las obligaciones de negocio de la organización. • Capacidad para actualizar sitios web propiedad o mantenidos por la organización. • Facilidad de comercio electrónico (por ejemplo, comprar equipo para la organización). • Llevar a cabo investigaciones que fortalezcan la toma de decisiones o la mejora de procesos internos.

Uso Personal del Servicio de Internet	El acceso a Internet que proporciona la organización debe ser utilizado de manera responsable y siempre en función del cumplimiento de los objetivos institucionales. Aunque su uso es exclusivo para fines laborales, se reconocen ciertas acciones personales como aceptables siempre que no interfieran con las funciones propias del cargo ni comprometan la seguridad o reputación de la entidad. Los usos permitidos incluyen: • Consultar información relevante que apoye el desempeño profesional dentro del marco de las responsabilidades asignadas. • Realizar compras electrónicas exclusivamente relacionadas con las necesidades personales. La organización no se responsabiliza por las transacciones personales de los empleados, incluyendo la calidad, entrega o pérdida de artículos ordenados. Los bienes y servicios personales comprados deben ser entregados en el hogar o en otra dirección personal, no en la propiedad de la organización. • Si los colaboradores, compran bienes o servicios personales a través del servicio de Internet, deben asegurarse de que la información proporcionada muestre que la transacción se realiza personalmente y no en nombre de la organización. • Acceder a fuentes de información para realizar investigaciones que aporten valor a los procesos internos o a la mejora continua. Cualquier otro uso personal deberá ser evaluado bajo principios de transparencia, racionalidad y respeto por los recursos institucionales.
Gestión de Cuentas de Internet, Seguridad y Monitoreo	Este apartado de la politica aplicada a la gestión de cuentas de internet, bajo la gestión de seguridad de la información, va dirigida a establecer lineamientos claros para la asignación uso y protección de las credenciales de acceso a Internet por parte del personal de la organización, en conformidad con los controles de seguridad de la información definidos por la norma ISO/IEC 27001. El contexto de la aplicación abarca a todo el personal que disponga de credenciales institucionales para acceder a Internet dentro del entorno organizacional. • Cada colaborador recibirá credenciales únicas (usuario y contraseña) para acceder a Internet, configuradas bajo protocolos seguros. • La administración técnica de estas credenciales estará bajo la responsabilidad del Proveedor de Servicios de TI, quien aplicará controles de autenticación robustos (por ejemplo, MFA) y políticas de renovación periódica.

	• Los usuarios son responsables de proteger la confidencialidad de sus credenciales y de garantizar que no sean divulgadas ni utilizadas por terceros. • Está estrictamente prohibido el uso compartido o la suplantación de identidad digital mediante el uso de credenciales ajenas. • Todo acceso será auditado y trazado mediante registros automáticos, con revisión periódica por parte del Comité de Seguridad de la Información.
Politica de Uso Restringido de Acceso a Internet	Esta politica propone garantizar el uso responsable y seguro del acceso a Internet proporcionado por la organización, evitando conductas que comprometan la integridad institucional, la seguridad de la información o los principios éticos del entorno laboral. Su aplicación alcanza a todos los usuarios de cuentas institucionales de Internet dentro de la organización, incluyendo personal permanente, temporal y consultores. El uso de la cuenta de Internet estará sujeto a las siguientes restricciones. No está permitido: • Acceder a sitios web que contengan material pornográfico, violento, discriminatorio o cualquier otro contenido considerado inapropiado o ilegal. • Utilizar redes peer-to-peer (P2P), instalar software de compartición de archivos o participar en actividades que comprometan la red. • Usar salas de chat en tiempo real o aplicaciones de mensajería externa no autorizadas. • Entrar a sitios de apuestas, juegos en línea o similares. • Suscribirse a plataformas de tipo “ganar dinero” o utilizar programas asociados a actividades de lucro personal. • Operar un negocio privado, comercializar productos o servicios desde la infraestructura institucional. • Descargar software que no esté aprobado por la política de software de la organización o que ponga en riesgo los sistemas. La organización aplicará filtros automáticos que bloquearán el acceso a categorías de sitios web considerados ilegales, pornográficos, violentos, ofensivos, discriminatorios, relacionados con armas, hacking, apuestas, citas, juegos, estaciones de radio, chats web y medios de transmisión no autorizados. En caso de que, de manera inadvertida, se acceda a uno de estos sitios, el incidente deberá reportarse de inmediato al encargado de Servicios de TI para su análisis y trazabilidad. Se realizarán auditorías periódicas sobre el tráfico de red y los registros de navegación.

	El monitoreo se realizará en cumplimiento con los principios de proporcionalidad y protección de la privacidad institucional. Todo hallazgo será evaluado bajo el marco del ciclo PDCA para fortalecer los controles. El incumplimiento de esta política será considerado una falta grave y podrá dar lugar a sanciones conforme a la normativa interna vigente.

Fuente: Elaboración propia.

Política de Computación en la Nube de SISLOCAR Caldera S.A

La propuesta en este apartado reconoce que la computación en la nube es una herramienta poderosa para impulsar la eficiencia operativa, la escalabilidad de los servicios y la continuidad del negocio. Toma como punto de partido para la implementación, la concientización sobre responsabilidades críticas en cuanto a seguridad, trazabilidad y protección de la información.

Esta política nace del compromiso de la empresa por garantizar que el uso de servicios en la nube se alinee con las mejores prácticas internacionales de seguridad de la información, en particular con los controles establecidos en las normas ISO/IEC 27001 e ISO/IEC 27002. Más allá del cumplimiento técnico, se busca fortalecer la confianza de los colaboradores, socios y comunidad, protegiendo los activos informáticos con criterios claros, verificables y adaptados al entorno operativo.

Aplica a todo el personal, departamentos y proveedores que interactúen con servicios en la nube utilizados por SISLOCAR, incluyendo almacenamiento de información, aplicaciones, plataformas y servicios de infraestructura. Abarca desde la evaluación inicial de los servicios hasta

su implementación, monitoreo, auditoría y eventual desactivación, en función del ciclo de vida de la información y del riesgo asociado. En la tabla 28, se presenta la matriz hoja de ruta operacional para la implementación de esta política.

Tabla 33. Matriz hoja de ruta operacional

Objetivo: Establecer los lineamientos que regulen el uso seguro, eficiente y legal de servicios de computación en la nube por parte de SISLOCAR Caldera S.A., garantizando la protección de los activos de información en entornos externos. **Responsables:** Alta gerencia, encargado de SGSI área de TI.	
Aspecto	**Procesos**
Disposiciones Generales	En SISLOCAR Caldera S.A., se requiere un manejo particularmente cuidadoso a los datos que gestiona la empresa, dado su carácter estratégico y sensible. Por ello, se establece que, estos datos solo podrán almacenarse en servicios de computación en la nube con la autorización previa y explícita del director de TI. Antes de contratar o continuar el uso de cualquier servicio en la nube, se deberá realizar una evaluación de riesgos detallada, que incluya una comprensión clara y verificable de los controles de seguridad implementados por el proveedor del servicio (Cloud Service Provider, CSP). Esta evaluación no será un trámite administrativo, sino una herramienta clave para garantizar que los activos digitales se mantengan íntegros, confidenciales y disponibles. La empresa llevará a cabo una debida diligencia proactiva para asegurarse de que el CSP haya establecido controles robustos y eficaces que se alineen con los estándares internacionales. Se dará prioridad a aquellos proveedores que cuenten con certificación conforme a ISO/IEC 27001:2022, y que además demuestren conformidad con los códigos de buenas prácticas para servicios en la nube establecidos en ISO/IEC 27001 y 27002 Ningún servicio en la nube será utilizado sin que los acuerdos de nivel de servicio (S LA) y los contratos sean previamente revisados, comprendidos y aceptados por las partes responsables dentro de la organización. Esta revisión será compartida y registrada como evidencia de cumplimiento, integrando criterios de trazabilidad y mejora continua.
Roles de Responsabilidad	En SISLOCAR Caldera S.A, se reconoce que una gestión responsable de los servicios en la nube no solo exige tecnología confiable, sino también claridad en las acciones humanas que la respaldan. Por ello, los roles y responsabilidades para actividades clave como copias de seguridad, aplicación de parches, gestión de registros, protección contra malware y atención de incidentes deben estar claramente definidos y documentados antes del inicio de

	cualquier servicio en la nube**.** Esto garantiza trazabilidad, transparencia y control operativo desde el primer momento. En aquellas operaciones que impliquen acciones irreversibles, como la eliminación de servidores virtuales, la finalización de servicios o la restauración de datos, se deben establecer procedimientos formales que incluyan la supervisión de una segunda persona debidamente calificada, reforzando la responsabilidad compartida y reduciendo riesgos operativos. Como parte del compromiso con la seguridad, la autenticación de dos factores (MFA) deberá implementarse en todos los servicios en la nube donde esté disponible, asegurando que el acceso a los entornos digitales esté protegido por múltiples capas de verificación. La confianza en el uso de la nube se respalda también con evidencia: deben existir registros de auditoría suficientes y accesibles para que SISLOCAR pueda entender cómo se acceden sus datos y detectar cualquier actividad no autorizada**.** La visibilidad es clave en cualquier sistema seguro. En cuanto a la protección de la información confidencial, esta debe estar encriptada tanto en reposo como en tránsito utilizando técnicas aceptadas internacionalmente, priorizando en la medida de lo posible el uso de claves de cifrado gestionadas directamente por SISLOCAR, y no por el proveedor. Además, las políticas internas de SISLOCAR, relacionadas con la creación, administración y eliminación de cuentas de usuario deberán aplicarse de forma íntegra dentro del entorno en la nube**,** manteniendo la coherencia con los sistemas locales y reforzando los controles de acceso. Respecto a la conservación de la información, todos los datos almacenados en la nube deben contar con mecanismos de respaldo, ya sea gestionados directamente por SISLOCAR o definidos contractualmente con el proveedor**.** Esto asegura la disponibilidad de la información incluso frente a eventos no planificados. Finalmente, al cerrar cualquier contrato relacionado con servicios en la nube**,** todos los datos de SISLOCAR, deberán ser eliminados en su totalidad, sin permanencias innecesarias en el entorno digital. El tratamiento de la información estará orientado por el principio de minimización y por el ciclo real de uso en los procesos del negocio.

Fuente: Elaboración propia.

Política de Uso de Dispositivos Móviles

En un mundo interconectado virtualmente, se reconoce que el uso de dispositivos móviles, estructuran una herramienta versátil, para la gestión de negocios e intercambios de información que se convierten en una oportunidad para aumentar la productividad y la flexibilidad de los equipos, pero también implica riesgos importantes relacionados con la seguridad de la información.

Esta política establece los criterios que rigen el acceso, manejo y protección de los activos digitales desde dispositivos móviles, sean corporativos o personales autorizados, asegurando que su uso se mantenga dentro de los parámetros definidos por las normas ISO/IEC 27001:2022 y los controles aplicables como A. 6.2.1, A .6.2.2 y A. 9.1.2. La política busca promover una cultura de responsabilidad compartida, en la que la movilidad no comprometa la integridad, confidencialidad ni trazabilidad de los datos críticos para la operación y la continuidad del negocio.

Dispositivos Proporcionados por SISLOCAR Caldera S.A

En esta actualidad se comprende que los dispositivos móviles son herramientas clave para facilitar la comunicación, la movilidad y la continuidad de las operaciones. No obstante, su uso conlleva riesgos importantes en cuanto al acceso, manipulación y protección de la información clasificada. Por eso, establecemos que únicamente se podrán utilizar dispositivos móviles corporativos proporcionados por SISLOCAR, para procesar información clasificada, salvo autorización expresa por parte de la dirección responsable.

Estos dispositivos serán configurados conforme a las políticas internas de seguridad y estarán respaldados técnicamente por el área de TI. Es responsabilidad del usuario transportar el

dispositivo en un estuche protector, evitar dejarlo sin supervisión en espacios públicos, y abstenerse de realizar cambios en su configuración sin la aprobación previa del equipo de soporte.

El dispositivo entregado por la organización está destinado exclusivamente a fines laborales. No debe compartirse ni utilizarse para actividades personales. SISLOCAR podrá requerir su devolución en cualquier momento para fines de auditoría o inspección, en consonancia con las buenas prácticas establecidas en los controles A.6.2.1, A.9.2.1 y A.13.2.3 de la norma ISO/IEC 27001:2022.

Uso de Dispositivos Móviles Personales (BOYD)

Muchos colaboradores muestran interés en utilizar sus dispositivos personales para tareas laborales. Este modelo, conocido como Bring Your Own Device (BYOD), ofrece flexibilidad, pero también introduce riesgos de seguridad y control, como el acceso por parte de terceros, el almacenamiento en plataformas externas, la exposición en contextos sociales y la posible instalación de aplicaciones maliciosas.

Por tanto, la decisión de utilizar un dispositivo personal con fines laborales será acordada entre el colaborador y SISLOCAR, tras una evaluación individual y aprobación formal. Todos los controles definidos en esta política se deberán cumplir rigurosamente, sin excepción. Queda prohibido el procesamiento de información corporativa desde dispositivos personales que no hayan sido autorizados.

El nivel de control que ejercerá SISLOCAR sobre los dispositivos BYOD será proporcional a la sensibilidad de los datos tratados. Aun respetando la privacidad y la legislación vigente, la organización se reserva el derecho de supervisar el cumplimiento normativo, auditar el entorno del

dispositivo y aplicar medidas de protección como el borrado remoto en caso de pérdida, robo o desvinculación laboral. Estos dispositivos BYOD deberán ser auditados y depurados de todo contenido empresarial al finalizar la relación laboral, garantizando que la información corporativa no permanezca en entornos personales más allá del ciclo operativo permitido.

Política de Teletrabajo

El teletrabajo es una modalidad valiosa para promover la flexibilidad, continuidad operativa y bienestar de nuestro personal en la empresa SISLOCAR. Sin embargo, su implementación exige medidas concretas para garantizar que la seguridad de la información no se vea comprometida fuera de los entornos tradicionales de oficina.

Esta política establece las directrices bajo las cuales los colaboradores pueden desempeñar sus funciones de forma remota, en pleno cumplimiento con los requisitos establecidos por la norma ISO/IEC 27001:2022. A través de controles técnicos, organizativos y conductuales, se busca asegurar la confidencialidad, integridad y trazabilidad de los datos, fomentando una cultura de responsabilidad compartida y resiliencia digital.

Acuerdos de Teletrabajo

Desde el punto de vista de la seguridad de la información, se deben considerar varios aspectos en cada acuerdo de teletrabajo, y la política de la organización en estas áreas se detalla en los siguientes puntos:

- Antes de comenzar un acuerdo de teletrabajo, se realizará una evaluación inicial de riesgos del entorno propuesto y la naturaleza del trabajo a realizar.

- La evaluación de riesgos considera el tipo de actividades a realizar, incluyendo la clasificación de la información que se almacenará y procesará, el método de acceso a la información, la necesidad de imprimir información clasificada localmente y la criticidad del rol.
- La evaluación también considera la seguridad física del lugar de trabajo propuesto, incluyendo el espacio para el equipo, el área separada para el trabajo, la seguridad de la zona de trabajo, el acceso de otras personas al área, la visibilidad del equipo desde el exterior y la seguridad de documentos en papel.
- Se investigará el impacto del teletrabajo en el seguro del hogar del individuo para asegurar que las pólizas actuales sigan siendo válidas. Puede ser necesario un seguro adicional.

Instalaciones Proporcionadas

Solo se debe usar el equipo proporcionado por SISLOCAR para acceder a las redes de la empresa. Esto puede incluir un portátil, PC, una impresora, escritorio y silla, almacenamiento seguro y otros artículos necesarios para el rol.

Se proporcionará una conexión de comunicaciones físicamente separada de la banda ancha doméstica para garantizar el rendimiento de la red y la seguridad. Se utilizará una Red Privada Virtual (VPN) para cifrar el tráfico de red.

Se evitará almacenar datos en la máquina cliente y se proporcionará protección contra virus que se actualizará automáticamente.

Terminación del Acuerdo

En caso de terminación del acuerdo de teletrabajo, todo el equipo suministrado debe ser devuelto al área de TI lo antes posible.

Política de Compromiso de SISLOCAR con la Seguridad de la Información

SISLOCAR Caldera S.A., como parte de su compromiso ético y operativo, asume la responsabilidad de proteger rigurosamente toda la información que administra en beneficio de la organización y sus partes interesadas. En coherencia con los principios establecidos por las normas internacionales ISO/IEC 27001 y 27002:2022, esta política promueve una cultura institucional basada en la confidencialidad, integridad y disponibilidad de los activos digitales.

Se espera que cada colaborador comprenda y respete las políticas de seguridad de la información vigentes, actuando de forma proactiva ante cualquier situación que pudiera comprometerlas. Este documento resume los lineamientos esenciales del marco normativo, y requiere la firma de los empleados como constancia de lectura y entendimiento.

El incumplimiento de estas disposiciones puede derivar en medidas disciplinarias, y en casos de infracción legal, se facilitarán las acciones correspondientes ante las autoridades competentes. SISLOCAR reafirma así su compromiso con la protección responsable de la información en todos sus niveles. Conducta Esperada en la Gestión de la Seguridad de la Información:

- Los empleados reconocen que su uso de los sistemas informáticos y de comunicaciones de SISLOCAR puede ser monitoreado y/o grabado con fines legales.
- Aceptan la responsabilidad por el uso y protección de las credenciales de usuario que se les proporcionen (cuenta de usuario y contraseña, token de acceso u otros elementos).

- No utilizarán la cuenta de usuario y contraseña de otra persona para acceder a los sistemas de la empresa.
- No intentarán acceder a ningún sistema informático al que no se les haya dado acceso.
- Protegerán cualquier material clasificado enviado, recibido, almacenado o procesado de acuerdo con el nivel de clasificación asignado, incluyendo copias electrónicas y en papel.
- Asegurarán etiquetar adecuadamente cualquier material clasificado que creen, siguiendo las pautas publicadas para su adecuada protección.
- No enviarán información clasificada por Internet a través de correo electrónico u otros métodos a menos que se utilicen métodos apropiados (por ejemplo, cifrado) para protegerla de accesos no autorizados.
- Siempre se asegurarán de ingresar correctamente las direcciones de correo electrónico de los destinatarios para no comprometer la información clasificada.
- Se asegurarán de no ser observados por personas no autorizadas mientras trabajan y tomarán cuidado al imprimir información clasificada.
- Almacenarán de forma segura el material impreso clasificado y asegurarán su correcta destrucción cuando ya no sea necesario.
- No dejarán su computadora desatendida de manera que se pueda acceder a información a través de su cuenta cuando estén ausentes.
- Se familiarizarán con las políticas y procedimientos de seguridad de la organización y cualquier instrucción especial relacionada con su trabajo.
- Informarán inmediatamente a su gerente si detectan, sospechan o son testigos de un incidente que pueda ser una violación de seguridad o si observan debilidades de seguridad de la información sospechosas en sistemas o servicios.

- No intentarán eludir o subvertir los controles de seguridad del sistema ni usarlos para un propósito distinto al previsto.
- No retirarán equipo o información de las instalaciones de la organización sin la aprobación apropiada.
- Tomarán precauciones para proteger todos los medios informáticos y dispositivos móviles cuando los lleven fuera de las instalaciones de la organización.
- No introducirán virus u otro malware en el sistema o la red.
- No intentarán desactivar la protección antivirus proporcionada en su computadora.
- Cumplirán con las obligaciones legales, estatutarias o contractuales que la organización les informe son relevantes para su rol.

Al dejar la organización, informarán a su gerente antes de su partida sobre cualquier información importante en su cuenta.

Política de Prevención de Software Malicioso

SISLOCAR Caldera S.A. comprende que, en un entorno digital interconectado, la amenaza de software malicioso, como virus, spyware, ransomware o cualquier código diseñado para alterar, dañar o robar información, representa un riesgo constante para la integridad de sus operaciones, sistemas y datos. Esta política establece las directrices necesarias para prevenir, detectar y gestionar la exposición a este tipo de amenazas, garantizando que las medidas implementadas sean consistentes con los controles técnicos y organizativos definidos por las normas ISO/IEC 27001 y 27002:2022.

Desde el compromiso ético, SISLOCAR en esta materia, implica la actualización constante de mecanismos de protección, la concientización del personal sobre prácticas seguras, y la

adopción de procedimientos de respuesta eficaces ante incidentes relacionados con software malicioso. Desde controles automatizados de escaneo hasta configuraciones seguras de dispositivos, esta política refuerza el enfoque institucional hacia una seguridad proactiva, resiliente y colaborativa, donde todos los miembros de la organización comparten la responsabilidad de preservar los activos digitales. En la tabla 35, se muestra la matriz hoja de ruta operacional.

Tabla 34. Matriz hoja de ruta operacional

Aspecto	**Procesos**
Prevención de Software Malicioso	Esta política se basa en el principio de defensa en profundidad, reconociendo que ninguna medida por sí sola ofrece protección suficiente frente al creciente espectro de riesgos digitales. En lugar de optar por controles individuales, la organización adopta una combinación estratégica de mecanismos técnicos, administrativos y conductuales que funcionan de manera complementaria y escalonada. Cada uno de estos controles es considerado esencial, y su implementación se promueve de forma integral, conforme a las mejores prácticas recomendadas por las normas ISO/IEC 27001 y 27002:2022. La prevención de infecciones digitales se convierte así en una responsabilidad compartida entre personas, procesos y tecnología, con el objetivo de reducir al mínimo la exposición ante ataques y garantizar un entorno operativo seguro y resiliente.
Firewall	Para proteger la infraestructura de SISLOCAR frente a accesos no autorizados y amenazas provenientes de redes externas, los firewalls deberán cumplir con las siguientes características mínimas, según los niveles de exposición y criticidad del entorno: • Filtrado de paquetes por dirección IP, puerto y protocolo, permitiendo configurar reglas granulares de entrada y salida. • Capacidad de inspección profunda de paquetes (DPI) para detectar y bloquear contenido malicioso oculto en tráfico legítimo. • Gestión centralizada que permita configurar, monitorear y aplicar políticas desde una consola administrativa unificada. • Soporte para VPN seguras, con control del tráfico cifrado y autenticación reforzada.

- Actualizaciones automáticas de firmas y reglas de seguridad, asegurando respuesta ante nuevas amenazas emergentes.
- Registro de eventos y generación de logs auditables, necesarios para trazabilidad y cumplimiento normativo.
- Seguridad a nivel de usuario, incluyendo autenticación, segmentación de tráfico y restricciones por rol.
- Protección contra denegación de servicio (DoS/DDoS) mediante umbrales de tráfico y mecanismos de bloqueo preventivo.
- Interfaz segura para administración, con acceso restringido y autenticación de múltiples factores para configuraciones.
- Restricción de privilegios locales, impidiendo que usuarios finales puedan desactivar o modificar el firewall sin autorización.
- Integración con software antivirus y sistemas de detección de intrusos (IDS/IPS**)** como parte de un enfoque de defensa en profundidad.

Antivirus

Esta política establece la instalación y mantenimiento de una plataforma de antivirus comercial y con soporte institucional**,** desplegada en puntos críticos como firewalls, servidores de correo electrónico, servidores proxy, equipos de usuario y dispositivos móviles, incluyendo portátiles y tabletas cuando sea posible.

El sistema antivirus se configura para operar de forma automatizada y resiliente: las actualizaciones de firmas se gestionan regularmente desde el proveedor o desde un servidor central, asegurando la vigencia de la protección. El escaneo en acceso estará habilitado por defecto para brindar protección en tiempo real, complementado con escaneos completos semanales que permitan detectar amenazas latentes.

En línea con las prácticas establecidas por ISO/IEC 27001 y 27002, se restringirá la capacidad de los usuarios para desactivar estas configuraciones, garantizando que la defensa contra software malicioso se mantenga activa, consistente y alineada con los objetivos del SGSI.

Características del Antivirus Idóneo para SISLOCAR

- Protección en Tiempo Real (Escaneo en Acceso) Detecta y bloquea amenazas al momento de ejecutarse o al acceder a archivos, aplicaciones o sitios web, evitando la propagación inmediata.
- Actualización Automática de Firmas Capacidad para descargar de forma regular y automática las últimas definiciones de virus, tanto desde el proveedor como desde un servidor interno centralizado.
- Escaneo Programado Completo: Permite ejecutar análisis periódicos (mínimo semanal) para detectar amenazas latentes en áreas que no se activan por uso directo.
- Gestión Centralizada: Incluye una consola de administración que permita monitorear el estado de los dispositivos, aplicar políticas, generar reportes y responder a incidentes desde un único punto.
- Compatibilidad Multiplataforma Funciona eficazmente en entornos Windows, Linux, Android e iOS, cubriendo servidores, computadoras de escritorio, portátiles, tabletas y teléfonos.
- Cifrado y Protección de Archivos Sensibles Integra herramientas de protección de información, como cifrado de archivos o sandboxing para archivos sospechosos.
- Control Antispyware y Antiransomware Detecta comportamientos propios de amenazas persistentes avanzadas y bloquea mecanismos de secuestro o espionaje digital.
- Mínimo Impacto en el Rendimiento Opera con eficiencia sin ralentizar la ejecución de procesos críticos, especialmente en servidores y estaciones de trabajo exigentes.
- Restricción de Desactivación por Usuarios Evita que los colaboradores desactiven o modifiquen las

	configuraciones, protegiendo la integridad de las políticas definidas por TI. • Integración con Firewalls y IDS/IPS Compatible con otras medidas de seguridad como firewalls, sistemas de detección de intrusos y herramientas de cuarentena. • Capacidad de Reporte y Auditoría: Genera logs detallados y trazables, compatibles con las exigencias de auditoría interna y externa del SGSI.
Filtro de Correo Electrónico (Antispam y Antimalware)	Instalación de un sistema robusto para detectar, bloquear y eliminar correos electrónicos no solicitados o potencialmente dañinos antes de que lleguen al usuario. Se impedirá la entrega de adjuntos comunes en campañas de malware, como archivos ejecutables, documentos con macros sospechosas y formatos comprimidos inseguros. Este sistema se alinea con controles como A.13.2.1 y A.12.2.1 de la normativa ISO/IEC 27001:2022.
Instalación y Escaneo de Software	Los usuarios no deben tener acceso administrativo suficiente a su computadora para permitirles instalar software en ella. Solo se permitirá software aprobado y este debe ser instalado por el área de TI tras una solicitud autorizada. Se debe realizar escaneo de forma regular, por lo menos uno semanalmente, de las computadoras de los usuarios, para detectar software no autorizados.
Gestión de Vulnerabilidad	Se recopilará información sobre vulnerabilidades de software de proveedores y fuentes de terceros y se aplicarán actualizaciones donde estén disponibles. Si es posible y si lo permite la política de gestión de cambios organizacional, las actualizaciones se aplicarán automáticamente tan pronto como se liberen. Se debe realizar escaneos de vulnerabilidad regularmente, particularmente en servidores y redes críticas para el negocio.

	Para las nuevas vulnerabilidades identificadas por empleados de SISLOCAR, se aplicará una política de divulgación coordinada.
Concientización del Usuario	Los usuarios deben estar informados cuando comiencen con la organización sobre la política de seguridad de la información y ser capacitados en formas de evitar ser víctimas de ataques como el phishing. Esta capacitación en conciencia debe repetirse regularmente a todos los empleados que utilicen equipos informáticos
Monitoreo de Amenazas	SISLOCAR Caldera S.A. se compromete a obtener información actualizada sobre amenazas emergentes desde fuentes confiables, tales como plataformas de inteligencia de ciberseguridad, portales de alertas gubernamentales (como INCIBE o CSIRT), proveedores tecnológicos y canales oficiales de fabricantes. Esta información será utilizada para alertar proactivamente a los usuarios sobre ataques potenciales, proporcionando el mayor nivel de detalle posible que facilite su identificación y respuesta oportuna. Además, todas las amenazas detectadas y las alertas emitidas deberán ser registradas en un repositorio interno**, ya sea una** base documental centralizada, software de gestión de incidentes o plataforma SIEM (Security Information and Event Management)**.** Esta práctica permitirá el análisis histórico, la trazabilidad y la mejora continua del SGSI. Dado que la organización deberá investigar e implementar múltiples controles descritos en sus políticas, como decidir qué tipo de antivirus adquirir, qué firewall implementar o qué servicios en la nube utilizar, se recomienda iniciar una fase exploratoria técnica que incluya evaluación de proveedores, pruebas piloto y análisis comparativo. El área de TI, junto con el responsable del SGSI, tendrá a cargo definir los criterios de selección, considerando certificaciones de

	seguridad, compatibilidad operativa, facilidad de monitoreo y alineación con los estándares ISO/IEC 27001:2022.
Revisiones Técnicas	Se realizarán revisiones regulares (al menos una vez al mes) de servidores y redes críticos para el negocio para identificar cualquier malware que se haya instalado desde la última revisión. Esto incluirá la toma de una instantánea de la configuración para fines de comparación posterior.
Detección de Malware y Activación del Protocolo de Incidentes	Cuando SISLOCAR Caldera S.A. detecte la presencia de software malicioso en alguno de sus componentes tecnológicos, ya sea un servidor, equipo cliente, red interna o sistema móvil, se pondrá en marcha de inmediato el proceso de gestión de incidentes de seguridad de la información. Este procedimiento no solo consiste en aislar el evento, sino en activar una serie de acciones planificadas que incluyen análisis forense, contención del daño, notificación a los responsables y actualización de controles preventivos. Para asegurar una respuesta eficaz y trazable, la empresa debe implementar una plataforma especializada en gestión de incidentes y amenazas**,** preferiblemente con capacidades de correlación automatizada, alertas en tiempo real y almacenamiento estructurado de evidencias. Algunas soluciones recomendadas incluyen SIEM (Security Information and Event Management) como Microsoft Sentinel, Splunk o AlienVault, que permiten centralizar logs, identificar patrones sospechosos y documentar cada fase del incidente. El área de TI y el responsable del SGSI deberán liderar la selección y adquisición de dicho software**,** considerando criterios como integración con sistemas existentes, facilidad de uso, compatibilidad con normas ISO/IEC, y posibilidad de escalar según la criticidad de los activos afectados.

Fuente: Elaboración propia.

Política de Criptografía

En SISLOCAR Caldera S.A., salvaguardar la información clasificada exige una combinación de procedimientos organizativos, medidas operativas y controles técnicos robustos, capaces de enfrentar los desafíos actuales de la seguridad digital. Dentro de este enfoque integral, la criptografía se posiciona como un mecanismo esencial para mantener la confidencialidad, integridad y legitimidad de los datos estratégicos. El uso de técnicas criptográficas permite alcanzar varios objetivos clave:

- **Confidencialidad**: Impide que personas no autorizadas accedan o interpreten la información.
- **Integridad**: Garantiza que los datos no han sido manipulados ni alterados en tránsito o almacenamiento.
- **Autenticación**: Verifica la identidad de quien accede o solicita información.
- **No repudio**: Permite demostrar la ocurrencia de una acción o mensaje, y su autoría, evitando denegaciones posteriores.

La decisión de aplicar controles criptográficos dependerá de los resultados de la evaluación de riesgos institucional, especialmente en el entorno SISLOCAR, o cualquier sistema donde se gestionen activos digitales sensibles. Si el nivel de riesgo lo amerita, su implementación será obligatoria y se deberá ejecutar según los procedimientos técnicos definidos por el SGSI, en concordancia con las buenas prácticas internacionales.

Escenarios Críticos de Aplicación Criptográfica

El cifrado deberá considerarse especialmente en:

- Dispositivos móviles: portátiles, tabletas y smartphones utilizados en labores institucionales.
- Medios extraíbles autorizados: como memorias USB o discos externos.
- Transmisiones de datos clasificados a través de canales externos, como el Internet o redes públicas.
- Uso de servicios en la nube, sin distinción del tipo de modelo (IaaS, PaaS o SaaS).

Selección y Adquisición de Técnicas

Una vez validada la necesidad, se deberá determinar qué técnicas criptográficas específicas se utilizarán, incluyendo la posible adquisición de herramientas o licencias de software, dispositivos de cifrado o módulos criptográficos integrados (HSM). También puede considerarse el uso de funcionalidades ofrecidas por los proveedores de servicios en la nube (CSP), asegurando que cumplan con las normas ISO/IEC 27017 y 27018. En estos casos, las opciones disponibles podrían estar limitadas por el catálogo aprobado por el CSP, por lo que se recomienda validar esta compatibilidad antes del despliegue.

Despliegue Seguro

La implementación de criptografía debe gestionarse cuidadosamente, procurando que más de un miembro del personal calificado participe en el proceso, para evitar puntos únicos de fallo y facilitar la segregación de funciones, lo que refuerza la trazabilidad y responsabilidad institucional.

Pruebas y Revisión Continua

Una vez activadas las funciones de cifrado, es crucial someterlas a pruebas técnicas realistas, que permitan detectar vulnerabilidades antes de que se conviertan en incidentes. Las pruebas deben abordar:

- Intentos de acceso mediante software común diseñado para romper cifrados.
- Escenarios de ingeniería social que simulen intentos de obtención de claves.
- Pruebas de interceptación de datos cifrados durante la transmisión por múltiples puntos.

Los resultados deberán ser documentados formalmente, las lecciones aprendidas incorporadas al SGSI y compartidas entre las áreas que también utilicen técnicas criptográficas. En el caso de proveedores en la nube, es posible que se requiera autorización previa del CSP para ejecutar algunas de estas pruebas, por lo que se recomienda establecer ese canal desde el inicio.

Fase III. Evaluación y Validación del SGSI de SISLOCAR

Durante esta fase, la organización consolidará Respecto a la madurez en seguridad de la información, SISLOCAR Caldera S.A. se presenta la tercera fase del proyecto, cuyo propósito es fortalecer los mecanismos de evaluación, validación y mejora continua del sistema. Esta etapa responde al objetivo de garantizar que el SGSI no solo cumpla con los requisitos normativos y expectativas de clientes, sino que se mantenga alineado con las mejores prácticas de la industria y los estándares internacionales ISO/IEC 27001 y 27002:2022**.**

un conjunto de herramientas y procesos técnicos y operativos que permitan monitorear, analizar y perfeccionar de forma continua el sistema, asegurando su capacidad de adaptación a nuevos riesgos y a las necesidades cambiantes del negocio.

Mecanismos de Evaluación Institucional

- **Auditorías Internas:** Se establecerá un calendario de revisiones sistemáticas que abarque controles, políticas, procedimientos y evidencias de conformidad. Estas auditorías se documentarán y retroalimentarán el ciclo PDCA**.**
- **Evaluaciones de Riesgo Periódicas:** El área SGSI definirá una metodología para identificar amenazas emergentes, vulnerabilidades latentes y brechas operativas, asegurando que las decisiones de tratamiento de riesgos sean oportunas y adecuadas.
- **Indicadores de Desempeño (KPI):** Se diseñarán indicadores SMART vinculados a los objetivos del SGSI, como porcentaje de cumplimiento de controles, tiempo de respuesta ante incidentes o nivel de participación en capacitaciones.
- **Revisión por la Dirección:** Se realizarán sesiones formales para garantizar que el SGSI permanezca en sintonía con las metas estratégicas de la empresa, los requerimientos de los clientes y el entorno regulatorio.
- **Pruebas Técnicas de Controles:** SISLOCAR adoptará prácticas como pruebas de penetración, simulacros de respuesta a incidentes y validación de configuración segura, documentando los resultados en informes trazables.
- **Gestión de No Conformidades**: Se establecerá un método sistemático para atender hallazgos críticos mediante acciones correctivas, preventivas y oportunidades de mejora, conforme a lo establecido en ISO/IEC 27001 (A.10.1.1, A.17.2.1).

- **Feedback del Cliente y Partes Interesadas:** Se incorporará una línea de retroalimentación que permita recoger la percepción de los usuarios sobre la seguridad de la información, convirtiendo sus aportes en acciones de mejora tangibles.

Áreas Monitoreadas del SGSI de SISLOCAR

Se hace necesario, establecer mecanismos para la supervisión efectiva para lograr una mejora continua del SGSI de SISLOCAR. Para esto se establecen áreas específicas de monitoreo, en las que existen indicadores claros y definidos. Para esta gestión, se propone un enfoque multidimensional, alineado con el ciclo PDCA (Planificar, Hacer, Verificar, Actuar) y los controles de las normas ISO/IEC 27001:2022 **y** 27002:2022**.**

1. **Enfoque Basado en Riesgos**

- Evalúa y prioriza áreas críticas según el impacto potencial de las amenazas.
- Se alinea con los resultados de la evaluación de riesgos de activos como SISLOCAR.
- Fortalece la trazabilidad de decisiones frente a auditorías.

2. **Enfoque por Controles ISO**

- Cada área monitoreada se vincula con los controles específicos del Anexo A.
- Facilita la auditoría cruzada entre controles implementados, aplicabilidad y eficacia.
- Ejemplo: A.12.4.1 para registro de eventos, A.9.4.1 para acceso lógico.

3. **Enfoque Funcional-Operativo**

- Divide el SGSI en funciones clave: acceso, cifrado, continuidad, autenticación, etc.

- Asigna responsables por cada función monitoreada.
- Permite construir visuales como radar charts para evaluar desempeño por función.

4. **Enfoque por Ciclo de Vida del Dato**

- Monitorea desde la creación del dato hasta su destrucción segura.
- Permite mapear controles como A.8.1.1 (inventario), A.8.3.2 (eliminación segura).

5. **Enfoque Integrado con Indicadores SMART**

- Cada área monitoreada incorpora KPIs específicos de desempeño.
- Se registra evolución y cumplimiento a través de paneles, heatmaps o dashboards.
- Ejemplo: porcentaje de cumplimiento de backup semanal, tiempo de respuesta a incidentes.

Tabla 35. Matriz de Áreas Monitoreadas del SGSI – SISLOCAR

Área Monitoreada	**Métrica**	**Método de Recolección**	**Frecuencia de Recolección**	**Responsable**
Objetivos de Seguridad de la Información	Cumplimiento de los objetivos establecidos	Revisión de objetivos	Anualmente	Encargado del SGSI
Riesgos de Seguridad de la Información	Número de riesgos identificados	Análisis de riesgos	Semestralmente	Encargado del SGSI
Controles de Seguridad de la Información	Eficacia de los controles implementados	Revisión de controles	Trimestralmente	Encargado del SGSI
Incidentes de Seguridad de la Información	Número de incidentes reportados	Registro de incidentes	Diariamente	Encargado del SGSI
Auditoría y Respuestas a Auditorías	Número de hallazgos y recomendaciones	Informe de auditorías	Anualmente	Encargado del SGSI
Gestión de Cambios Tecnológicos	Cambios realizados sin aprobación	Sistema de gestión de cambios	Semanalmente	Encargado del SGSI
Capacitación en Seguridad	Porcentaje de personal capacitado	Registro de capacitaciones	Anualmente	Encargado del SGSI

Fuente: Elaboración propia.

Esta tabla resume de forma clara las dimensiones clave del monitoreo del SGSI de SISLOCAR, permitiendo visualizar cómo se mide, con qué frecuencia y quién tiene la responsabilidad operativa de cada componente.

- **Objetivos de Seguridad**: Se revisan anualmente, lo que es adecuado para validar alineación estratégica con ISO/IEC 27001:2022. Refleja si los compromisos en seguridad están siendo alcanzados.
- **Riesgos**: Evaluados semestralmente, lo cual garantiza que el entorno de amenazas sea monitoreado sin perder relevancia. Permite ajustar controles si surgen vulnerabilidades nuevas.
- **Controles Implementados**: Se revisan cada trimestre, lo que da buena cadencia para confirmar eficacia técnica y funcional de las medidas aplicadas.
- **Incidentes**: Su registro diario denota alta madurez operativa. Además de permitir una respuesta rápida, genera trazabilidad para análisis mensual o anual.
- **Auditorías y Respuestas**: La revisión anual captura la gestión correctiva y preventiva derivada de hallazgos, y se conecta con el ciclo PDCA del SGSI.
- **Gestión de Cambios Tecnológicos**: El monitoreo semanal es crucial para detectar modificaciones no autorizadas que podrían introducir riesgos, especialmente en infraestructura crítica.
- **Capacitación en Seguridad**: Medir anualmente el porcentaje de personal capacitado permite validar el alcance de la concientización y soporte cultural del SGSI.

En conjunto, esta matriz establece un sistema de monitoreo equilibrado y recurrente que cubre tanto el plano técnico como organizacional, alineado con los requisitos de mejora continúa definidos en la norma ISO/IEC 27001:2022.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES DEL PROYECTO

Esta sección final del proyecto de graduación está compuesta por dos partes claramente definidas: las conclusiones **y** las recomendaciones. Su propósito principal es ofrecer una síntesis reflexiva y estructurada de los resultados obtenidos, los desafíos enfrentados y los aprendizajes adquiridos durante la ejecución del trabajo.

Las conclusiones que se presentan a continuación se distinguen por su claridad, precisión y capacidad de síntesis, abordando tanto el grado de cumplimiento como las dificultades relacionadas con los objetivos del proyecto. Se inicia con una valoración global, derivada del Objetivo General, y posteriormente se desglosan las conclusiones específicas relacionadas con cada uno de los objetivos particulares. También se integran reflexiones que permiten comprender cómo distintos componentes del proyecto se articulan y fortalecen entre sí.

Por otro lado, las recomendaciones recogen aspectos que, aunque no fueron incluidos directamente en el alcance del proyecto, se consideran relevantes para el fortalecimiento del SGSI de SISLOCAR Caldera S.A. Estas sugerencias apuntan a consolidar buenas prácticas, abordar oportunidades de mejora y aportar valor futuro a la gestión de la seguridad de la información en la organización.

Conclusión del Objetivo General del Proyecto

La concurrencia de la teoría con la práctica otorga una relevancia fundamental al proyecto de Desarrollo de una Propuesta de Implementación de Mejoras en Seguridad de la Información Alineada a ISO 27001:27002 para la Mitigación de Riesgos en la Empresa SISLOCAR Caldera. Trasciende de mera aplicación técnica de controles para consolidarse como un pilar de la estrategia empresarial y la resiliencia operativa de la organización. Todo el proceso de investigación y diseño permite la implementación de mejoras concretas, basadas en los estándares ISO/IEC 27001 y 27002:2022 como marco técnico y organizativo. En una empresa con este tipo de logística aduanera, establecer controles asociados a los activos digitales facilita la mejora continua de aspectos esenciales como la trazabilidad operativa, permitiendo procesos formales que responden de forma oportuna y eficaz ante incidentes emergentes.

En este contexto, se evidenció que la gestión del riesgo constituye un eje transversal y estratégico para consolidar la seguridad informática en la empresa. La aplicación de herramientas clave como la Matriz de Riesgo, el Análisis de Brechas y la evaluación del entorno tecnológico permitió diagnosticar vulnerabilidades reales, priorizar acciones de tratamiento y fundamentar decisiones técnicas en criterios objetivos. Al incorporar la gestión del riesgo como parte estructural del SGSI, SISLOCAR no solo logra reducir su exposición ante amenazas cibernéticas, sino que también establece las bases para una mejora continua, adaptable al crecimiento operativo y a la evolución constante del panorama tecnológico.

El valor esencial del proyecto radica en la transformación del enfoque y la comprensión del concepto de seguridad de la información, pasando de una óptica reactiva a una habilitación estratégica del plan real de gestión del riesgo. Esto es crucial en una empresa como SISLOCAR

Caldera, cuyo negocio principal es la logística aduanera, fundamentada en el manejo de información sensible. En este sector, la confianza es fundamental; por ello, la adopción de un SGSI de estas características no solo mitiga el riesgo, sino que ofrece una garantía sólida en la transferencia y custodia de datos. El proyecto, por sí mismo, otorga una ventaja competitiva a la organización, fortaleciendo la continuidad operativa y la resiliencia mediante la implementación de los controles idóneos que aseguran la trazabilidad operativa.

Es imprescindible considerar el enfoque pertinente para la identificación de los riesgos cibernéticos más relevantes a fin de obtener un diagnóstico seguro que permita la toma de decisiones oportunas para la aplicación de controles, tales como el cifrado de datos, la protección contra amenazas oportunistas, la gestión de accesos y el uso seguro de dispositivos móviles y servicios en la nube. Todo esto tiene como finalidad mantener un SGSI estructurado y robusto que pueda sostenerse y escalar con el tiempo.

Más allá de los resultados técnicos, el proceso completo permite comprender cómo se traduce la teoría en prácticas reales dentro de una organización, mediante la observación de los indicadores, las auditorías, los protocolos y las decisiones del SGSI, y su impacto directo en la operativa diaria de la empresa. Esto se convierte en un aporte teórico-práctico de gran valor para el área de la informática. Todas las acciones sugeridas permiten a la empresa SISLOCAR estar mejor preparada para afrontar amenazas digitales y demostrar conformidad con normativas internacionales. Con el proyecto, el SGSI no solo estará operativo, sino que se sostendrá como parte de la cultura institucional y continuará evolucionando en función del negocio y su entorno.

En resumen, la propuesta de mejoras del proyecto eleva la gobernanza de la seguridad en la gestión de la información digital de la empresa SISLOCAR Caldera, generando la oportunidad

de tomar decisiones que garanticen el manejo sigiloso de los datos sensibles. Todas las acciones propuestas se alinean bajo el estándar ISO 27001/27002, dotando a la empresa de la madurez, la resiliencia y la credibilidad necesarias para operar de manera segura en un entorno digital de alta amenaza, garantizando que el SGSI estará operativo, sostenible y plenamente integrado a la cultura institucional a partir de agosto de 2025.

Conclusiones de los Objetivos Específicos

De acuerdo con los objetivos específicos planteados y su desarrollo mediante el diagnóstico y la propuesta de soluciones, se presentan conclusiones puntuales que refuerzan el aporte teórico y práctico ante situaciones de riesgo en la seguridad de la información que enfrenta la empresa SISLOCAR Caldera S.A. El análisis realizado en SISLOCAR Caldera establece que la implementación de mejoras en seguridad, conforme a los estándares ISO/IEC 27001 y 27002, resulta fundamental y estratégicamente orientada a corregir las deficiencias detectadas en tres ejes clave: técnico, organizacional y cultural. Se concluye que únicamente un enfoque integral de SGSI puede transformar el estado reactivo actual de la empresa en un modelo proactivo, resiliente y sostenible.

Objetivo 1. Identificar los principales riesgos de seguridad de la información que enfrenta la empresa SISLOCAR Caldera S.A, mediante la evaluación de sus procesos operativos y del manejo de información confidencial, con el propósito de establecer un diagnóstico que sirva

de base para la implementación de controles alineados con los estándares ISO/IEC 27001 y 27002.

La evaluación, centrada en los procesos operativos y el manejo de información confidencial, permitió identificar un conjunto de riesgos relevantes que inciden directamente en la seguridad de la información permite identificar riesgos estructurales, tecnológicos y humanos, que ponen en peligro, la seguridad de los datos que trasiegan en la empresa. Mediante el diagnostico aplicado, se logra detectar brechas importantes que comprometen la integridad, disponibilidad y confidencialidad de los activos informacionales. Por tanto, se hace necesario, alinear estos procesos a los establecido por ISO/IEC 27001 y 27002, para las coexistencias de procesos tecnológicos, que puedan detectar las vulnerabilidades y enfrentar de forma asertiva, las amenazas evolutivas.

Asimismo, se destaca la necesidad de una arquitectura de protección homogénea, que evite la fragmentación tecnológica, aplicando controles integrales y sistémicos, en la que el uso de antivirus y firewalls evidencie esfuerzos por fortalecer la seguridad, sin que persistan riesgos derivados de una gestión dividida. Las políticas establecidas para la gestion del riesgo de la seguridad cibernética, debe responder a una lógica que transverse todas las acciones del ejercicio empresarial. Se requiere que los sistemas operativos ampliamente utilizados (Windows Server 2022, Windows 11 Pro), que requieren configuraciones seguras, actualizaciones constantes y monitoreo activo, dada su alta visibilidad en el mercado y su vulnerabilidad frente a amenazas persistentes avanzadas (APT), acaparen el accionar del departamento TI.

También se deben fortalecer las debilidades en los mecanismos de controles de accesos, que se traduce en una trazabilidad limitada, una gestión asistemática de privilegios y una escasa capacidad de respuesta ante accesos indebidos o incidentes internos. No se puede facilitar la falta

de formalización en los procesos de inducción y capacitación, lo que impide una apropiación efectiva del conocimiento en seguridad por parte del personal y limitar la generación de hábitos organizacionales orientados a la protección de activos críticos. Todos estos riesgos configuran un entorno operativo que, sin una intervención estratégica, puede comprometer la sostenibilidad institucional. Se enfatiza en la necesidad de adoptar un enfoque integral de SGSI, que articule medidas técnicas, acciones formativas y una gobernanza fortalecida, alineadas con los estándares ISO/IEC 27001 y 27002 e implementar controles amparados a la realidad existente de la empresa, evitando soluciones genéricas y promoviendo prácticas adaptativas.

Este proyecto, genera una visión generalizada sobre la seguridad de la información, no como un requerimiento técnico aislado, sino como, un valor organizacional compartido, que permee todas las áreas y funciones de la empresa. La cultura institucional en ciberseguridad debe considerarse en la base operativa de una empresa que maneje información sensible. Por tanto, la gobernanza debe evolucionar hacia una estructura robusta y trazable, con roles claramente definidos, supervisión activa y mecanismos de rendición de cuentas que fortalezcan la capacidad de anticipación y respuesta ante incidentes.

Objetivo 2. Analizar las debilidades en los mecanismos actuales de control de accesos y protección de datos sensibles, mediante la revisión de políticas internas, tecnologías empleadas y prácticas vigentes en la empresa, con el fin de orientar mejoras que reduzcan la exposición a riesgos cibernéticos.

En el análisis de los mecanismos actuales de control de accesos y protección de datos sensibles en SISLOCAR Caldera S.A., realizado a partir de la revisión de políticas internas, tecnologías empleadas y prácticas vigentes, permitió identificar debilidades estructurales,

operativas y culturales que incrementan la exposición de la organización a riesgos cibernéticos. Estas debilidades no solo comprometen la seguridad de los activos informacionales, sino que también evidencian una disociación entre los lineamientos normativos y su aplicación efectiva en el entorno operativo.

Las políticas de control deben convertirse en la ruta de prevención que formalice las acciones aplicadas para la protección de datos, desde una visión actualizada, tomando en cuenta, todos aquellos factores que comprometan el resguardo de la información. Todos los procesos deben encaminarse hacia la trazabilidad de las acciones y el favorecimiento de respuesta oportuna a eventos fortuitos que aprovechen las vulnerabilidades en tal gestion y se puedan convertir en amenazas oportunistas. El conjunto de estrategias y herramientas de protección, deben alinearse hacia una meta clara, para evitar el riesgo de suplantación de identidades y accesos no autorizados, así como a la protección de datos sensibles. La falta de segmentación lógica en los entornos digitales, la escasa articulación entre las tecnológicas y protección de datos, las políticas internas débiles y la escaza observancia mediante monitoreos periódicos, impiden la implementación de políticas seguras que establezcan un entorno seguro.

Por tanto, es fundamental consolidar una cultura organizacional de seguridad, mediante procesos formativos continuos, simulacros de incidentes y campañas de concientización que promuevan el comportamiento informado y responsable de todos los colaboradores. SISLOCAR Caldera, debe avanzar hacia un modelo de gobernanza digital proactiva, donde la seguridad de los datos sensibles no dependa exclusivamente de la tecnología, sino de la interacción armónica entre políticas, procesos, personas y sistemas.

Objetivo 3. Diseñar una propuesta de mejora del sistema de gestión de seguridad de la información, basada en los lineamientos de las normas ISO/IEC 27001 y 27002, que incluya controles específicos para el acceso y la protección de datos, y que permita mitigar los riesgos de accesos no autorizados y la vulneración de información crítica.

La propuesta de mejora del Sistema de Gestión de Seguridad de la Información (SGSI) para SISLOCAR Caldera S.A., diseñada conforme a los lineamientos de las normas ISO/IEC 27001 y 27002, constituye un paso decisivo hacia la consolidación de un modelo de gobernanza digital resiliente, ético y sostenible. No solo se fundamenta en aspectos teóricos, sino que sensibiliza su contenido al entorno empresarial, respondiendo de forma directa, a las vulnerabilidades detectadas en el contexto actual. No pretende convertirse en una receta con pasos a seguir, sino como una vivencia real de la interiorización del recurso humano, sobre la necesidad de contar con mecanismo actualizados, que establezcan rutas de protección de los datos informáticos, desde una visión integral y vinculada con las tecnologías de punta y la esencia social de la organización,

Además, la propuesta considera aspectos esenciales sobre controles que deben establecerse para la reducción significativa del riesgo y la aplicación constante de la trazabilidad en la gestion de los datos. Los encargados de las acciones para la protección cibernética deben entender la necesidad preponderante de establecer protocolos que se conviertan en barreras robustas para la prevención, detección y mitigación de los ataques informáticos, que evolucionan de forma constante El departamento TI, debe convertirse en un escudo potente, que vele por la privacidad, la seguridad y el resguardo de los efectivos documentales, que se gestionan en la empresa.

Se debe tomar en cuenta que, en un mundo divergente, donde las estrategias de los ciberdelitos fluctúan constantemente y se perfeccionan infatigablemente, una propuesta efectiva

para la mitigación del riesgo debe alinearse a las normas estándares en ISO/IEC 27001 y 27002, proponiendo mejoras en las estructuras del SGSI, de forma que admita la gestion y la auditoria constante. Son muchos los elementos que inciden en una práctica sana y protectora, estos deben ser tomados en cuenta, para realmente establecer rutas de mejoras que sean protectoras. Por tanto, la integración de acciones formativas y de sensibilización, orientadas a fortalecer la apropiación del conocimiento por parte del personal, fomentar hábitos seguros y consolidar una cultura organizacional que valore la seguridad como un principio transversal es fundamental en la aplicación de la propuesta de mejoras.

Se concluye que esta propuesta de mejora no debe entenderse como un conjunto de medidas técnicas aisladas, sino como una estrategia institucional articulada, capaz de transformar el enfoque reactivo actual en un modelo proactivo, preventivo y culturalmente consolidado. La seguridad de la información deja de ser una función periférica para convertirse en un eje estructural de la sostenibilidad organizacional. Asimismo, se reconoce que la implementación efectiva de esta propuesta requiere: Un compromiso directivo claro y sostenido, que respalde la asignación de recursos, la supervisión estratégica y la transversalización de los principios de seguridad en todos los niveles de la organización. Una gobernanza fortalecida, que articule los tres ejes fundamentales: políticas claras, cultura organizacional y arquitectura tecnológica segura.

Otro aspecto esencial consiste, en la aplicación de un enfoque adaptativo que permita contextualizar los controles según las particularidades operativas de SISLOCAR Caldera S.A., evitando soluciones genéricas y promoviendo prácticas situadas. En suma, la propuesta diseñada no solo mitiga los riesgos de accesos no autorizados y la vulneración de información crítica, sino que establece las bases para una transformación profunda del SGSI, orientada a la dignificación

del entorno digital, la protección de los activos informacionales y la consolidación de una cultura institucional resiliente frente a los desafíos del ciberespacio.

Recomendaciones

Las recomendaciones ofrecidas se fundamentan en los vacíos que deja la aplicación del proyecto, de acuerdo con su alcance. Se ofrecen como aporte para la consideración de la organización en la toma de decisiones. Se explicitan tomando como sujeto destinatario, la empresa SISLOCAR Caldera S.A.

Recomendaciones para SISLOCAR Caldera S.A.

1. Unificar el sistema para la conservación, trazabilidad y consulta de evidencias que respalden las acciones del SGSI.
2. Implementar una plataforma de gestión documental con controles de acceso, firma digital y versión controlada para evidencias de cumplimiento, auditorías y decisiones técnicas del SGSI.
3. Diseñar un conjunto de indicadores SMART alineados con la mejora continua y los objetivos de ISO/IEC 27001. Estos deben reflejar avances en trazabilidad, detección de incidentes, tiempos de respuesta y concienciación organizacional.
4. Diseñar un programa anual de concienciación que incluya simulacros de phishing, campañas de comunicación positiva, formación diferenciada por rol, y reconocimientos a buenas prácticas en ciberseguridad.

5. Crear escenarios de simulación que integren crecimiento operacional, incorporación de nuevos activos digitales y migraciones tecnológicas, con base en matrices de impacto y probabilidad.
6. Consolidar un plan de interoperabilidad técnica que armonice herramientas de seguridad (MFA, antivirus, GPOs, cifrado de discos, firewalls) mediante políticas de configuración estandarizadas.
7. Desarrollar mecanismos de articulación entre el SGSI y los distintos departamentos operativos. Esto puede lograrse mediante flujos de trabajo compartidos, responsables coordinadores por área y sesiones de alineación interdepartamental.
8. Se sugiere implementar canales formales para recopilar información desde el entorno interno, como encuestas, buzones de hallazgos o mesas de revisión técnica, que alimenten la mejora del SGSI de forma dinámica. Esto permitirá ajustar controles y procedimientos con base en evidencia contextual.
9. Es recomendable realizar un diagnóstico de capacidades técnicas en ciberseguridad por rol, que sirva como base para un programa de formación especializado. Esto garantizará la apropiación efectiva del SGSI por parte del personal operativo, técnico y administrativo.
10. Para fortalecer la capacidad de anticipación ante nuevas amenazas, se propone establecer una rutina de análisis del entorno regulatorio, tecnológico y competitivo del sector logístico, incorporando informes trimestrales sobre riesgos emergentes, tendencias de ciberataques y cambios normativos.
11. Se recomienda desarrollar un plan de interoperabilidad que estandarice la configuración de herramientas de seguridad (como antivirus, firewalls, MFA y cifrado), evitando conflictos entre sistemas y asegurando una arquitectura de protección coherente.

REFERENCIAS BIBLIOGRÁFICAS

Balestrini, M. (2006). Cómo se elabora el proyecto de investigación. Venezuela: BL Consultores Asociados. https://luisdoubrontg.school.blog/wp-content/uploads/2023/12/balestrini_como_se_elabora_un_proyecto_de_inve.pdf

Cascade Strategy. (2022, octubre 24). *Análisis GAP: Qué es y cómo realizarlo* Cascade Strategy. https://www.cascade.app/blog/es-gap-analysis

Centro Nacional de Seguridad Digital (CNSD) (2024) *Gestión del Riesgo de la Seguridad de la Información.* Presidencia del ministro. Perú. https://cdn.www.gob.pe/uploads/document/file/7756679/6554792-guia-de-gestion-de-riesgos.pdf

Comisión Federal de Comercio (2019) *Seguridad de los proveedores*. Gobierno de Estados Unidos de América. https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/seguridad-proveedores

David, W y Monsalve, S (2023) *Ciberseguridad, reto empresarial para afrontar la Era de la digitalización actual*. (Tesis de grado) Universidad Pontificia Bolivariana. Bolivia. file:///D:/2025/tesis%20NACHO/antecedentes/Ciberseguridad,%20reto%20empresarial%20para%20afrontar%20la%20era%20de%20la%20digitalizaci%C3%B3n%20actual.pdf

Espinoza, O (2020) Principios de seguridad informática. Universidad San Marcos. https://repositorio.usam.ac.cr/xmlui/bitstream/handle/11506/2069/LEC%20ING%20SIST%200033%202020.pdf?sequence=1&isAllowed=y

Garantía de Calidad de Red (NQA), (2024) *ISO 27001:2022 guía de implementación de sistemas de gestión de seguridad de la información*. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Gómez, A (2025) *Qué es la gobernanza de la ciberseguridad y porqué es importante*. https://www.ollusa.edu/blog/what-is-cybersecurity-governance.html#:~:text=en%20acci%C3%B3n%20controlada.-,Monitoreo%20continuo,de%20sus%20grupos%20de%20inter%C3%A9s.

Instituto Nacional de Ciberseguridad (2019) *Guía de acceso seguro a los dispositivos de campo*. España: incibe. https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe-cert_guia_acceso_seguro_dispositivos_campo.pdf

Internacional Standard (ISO), (2022) *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. ISO. https://www.iso.org/es/contents/data/standard/07/56/75652.html#:~:text=Mientras%20que%20ISO/IEC%2027001,y%20la%20respuesta%20ante%20incidentes.

Jaén, L (2019) Fuentes de Información para la investigacion en Archivística y bibliotecología. San José, Costa Rica: UCR. file:///C:/Users/vvive/Downloads/MUESTRA_fuentes_informacion.pdf

Marín, J. Bautista, y García, J (2014) Etapas en la evolución de la mejora continua: Estudio multicaso. *Intangible Capital*, vol. 10. https://www.redalyc.org/pdf/549/54932488008.pdf

Palo Alto Networks (s.f) *¿Qué es el principio del mínimo privilegio?,* https://www.paloaltonetworks.es/cyberpedia/what-is-the-principle-of-least-privilege#:~:text=El%20principio%20del%20m%C3%ADnimo%20privilegio%20(PoLP)%20es%20un%20concepto%20relacionado,a%20cabo%20una%20determinada%20tarea

Romero, C (2005) La categorización un aspecto crucial en la investigación cualitativa. *Cesmag* Vol. 11. https://proyectos.javerianacali.edu.co/cursos_virtuales/posgrado/maestria_asesoria_familiar/Investigacion%20I/Material/37_Romero_Categorizaci%C3%B3n_Inv_cualitativa.pdf

Rozo, J y Suarez, O (2016) *GESTION DE SEGURIDAD DE LA INFORMACIÓN EN LA INSTITUCIÓN EDUCATIVA LEÓN XIII DEL MUNICIPIO DE SOACHA*. (Tesis de grado) Universidad Politécnica GRANCOLOMBIANO. Colombia. https://alejandria.poligran.edu.co/bitstream/handle/10823/659/Rozo%20Suarez%20Proyecto%20trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

Sánchez, H (2018) *Identificación de vulnerabilidades y riesgos en los activos de Ti de ENERGITEL.* (Tesis de grado) Universidad Nacional Abierta a Distancia (UNAD). Colombia. https://repository.unad.edu.co/jspui/bitstream/10596/28221/1/93405573.pdf

Stallings, W. y Brown, L. (2018). *Computer Security: Principles and Practice* (4th ed.). Pearson.

Tarazona, C (2009) *Amenazas informáticas y seguridad de la información*. file:///C:/Users/vvive/Downloads/Dialnet-AmenazasInformaticasYSeguridadDeLaInformacion-3311853.pdf

Torres, A y Monroy, J (2019) El problema de la definición del Problema de Investigación. *Boletín Científico de la Escuela Superior Atotonilco de Tula*. Vol. 13. file:///C:/Users/vvive/Downloads/webmaster,+5265-Manuscrito-24645-3-10-20191122.pdf

Vega, E (2021) Seguridad en la información. *3 ciencias.* Vol. 1. https://3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIO%CC%81N.pdf

Wright, T (2022) Analisis GAP Qué es y cómo aplicarlo. *CASCADE Blog*. Análisis GAP: Qué es y cómo realizarlo + plantillas gratuitas

ANEXOS

Anexo 1. Entrevista Estructurada

ENTREVISTA ESTRUCTURADA

Datos generales del entrevistado:

- Nombre (opcional): _____
- Cargo: _____
- Años de experiencia en el puesto: _____
- Departamento/Área: _____

Sección 1: Riesgos cibernéticos (preguntas para los tres perfiles)

1.1 Preguntas cerradas
(Responder con una "X")

1. ¿Ha experimentado la organización algún incidente de seguridad informática en los últimos 12 meses?
   ☐ Sí ☐ No ☐ No sabe / No responde
2. ¿Considera que los riesgos de ciberseguridad están debidamente identificados y gestionados en la empresa?
   ☐ Totalmente de acuerdo ☐ De acuerdo ☐ En desacuerdo ☐ Totalmente en desacuerdo
3. ¿Se realizan auditorías o evaluaciones periódicas de los sistemas de información?
   ☐ Sí, trimestralmente ☐ Sí, anualmente ☐ No se realizan ☐ No sabe / No responde

1.2 Preguntas abiertas

4. Desde su experiencia, ¿cuáles considera que son los principales riesgos cibernéticos que enfrenta la empresa?
5. ¿Qué tipo de amenazas informáticas cree que podrían tener mayor impacto sobre los sistemas críticos de SISLOCAR?

Sección 2: Políticas de seguridad y cultura organizacional

2.1 Preguntas cerradas

6. ¿Está familiarizado(a) con las políticas internas de seguridad de la información de SISLOCAR?
   ☐ Sí ☐ Parcialmente ☐ No
7. ¿Ha recibido capacitación formal sobre ciberseguridad en el último año?
   ☐ Sí ☐ No
8. ¿Considera que la empresa cuenta con una cultura organizacional sólida en materia de protección de la información?
   ☐ Totalmente de acuerdo ☐ De acuerdo ☐ En desacuerdo ☐ Totalmente en desacuerdo
9. ¿Usted reportaría un incidente de seguridad si lo detecta?
   ☐ Sí ☐ No ☐ No sabe / No está seguro

2.2 Preguntas abiertas

10. ¿Cómo describe la cultura de seguridad de la información dentro de la empresa?
11. ¿Qué aspectos considera que deben mejorar en cuanto a políticas, prácticas o formación en ciberseguridad?
12. ¿Qué sugerencias haría para fortalecer la protección de la información sensible en su área de trabajo?

¡Gracias ¡

Anexo 2. Matriz de Brechas para el SGSI de SISLOCAR

Área de Competencia	Estado Actual	Estado Deseado (ISO/IEC)	Brecha Identificada	Acción Recomendada
Conocimiento de ISO/IEC 27001	Parcial y sin certificación	Dominio certificado y aplicado en el entorno laboral	Baja especialización técnica	Capacitación formal, certificaciones
Gestión de controles de seguridad	Implementación básica o reactiva	Gestión proactiva, sistematizada y alineada a SGSI	Déficit en mantenimiento de controles normativos	Formación y consultoría especializada
Documentación y trazabilidad	Registros informales, no estandarizados	Procedimientos, indicadores y reportes integrados	Falta de evidencia operativa	Definición de indicadores y procedimientos
Análisis de riesgos	Sin metodología definida	Aplicación continua del análisis de riesgos	Ausencia de enfoque estructurado	Adopción de metodología y formación técnica
Soporte externo especializado	Eventual y sin estrategia	Mecanismos definidos: outsourcing, alianzas, consultores	Ausencia de planificación colaborativa	Diseño de plan de soporte técnico externo

Anexo 3. Instrumento de Análisis de Brechas (Gap Analysis)

Control de Seguridad	Estado Actual	Requisito ISO/IEC	Brecha Detectada	Acción Correctiva	Nivel de Prioridad
Gestión de accesos	Parcialmente implementado	Control 9.1 (ISO 27002)	Deficiencia en monitoreo de accesos	Mejorar auditoría de accesos	Alta
Protección de activos	Implementado	Control 8.2 (ISO 27002)	Sin inventario actualizado	Realizar auditoría de activos	Media
Gestión de incidentes	No implementado	Control 16.1 (ISO 27002)	Falta procedimiento formal	Desarrollar política de respuesta a incidentes	Alta

Anexo 4. Evaluación de Vulnerabilidades

Activo Evaluado	Vulnerabilidad Detectada	Impacto Potencial	Probabilidad de Explotación	Recomendación
Servidor web	Inyección SQL	Alto	Alta	Implementar validación de entradas
Red corporativa	Configuración débil de firewall	Medio	Alta	Reconfigurar reglas de acceso
Aplicación interna	Uso de credenciales por defecto	Alto	Media	Implementar autenticación robusta