UNIVERSIDAD
SAN SEBASTIAN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO

CARRERA INGENIERÍA EN CIBERSEGURIDAD

SEDE BELLAVISTA

DISEÑO DE UNA PROPUESTA DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ORIENTADA A LA PROTECCIÓN DE DATOS SENSIBLES PARA LA EMPRESA DE VENTA DE NEUMÁTICOS.

Proyecto de título para optar al Título de Ingeniero de ciberseguridad y auditoría informática

Profesor guía: Mg Rene Galarce Godoy

Estudiante: Jean Ronald Cange

Santiago, Chile

2025

HOJA DE CALIFICACIÓN

En _____ Chile, el __ de _____ del 20__, los abajo firmantes dejan constancia que el estudiante _____ de la carrera _____ ha aprobado el proyecto de título para optar al título de _____ con una nota de _____

_____
Profesor Evaluador

_____
Profesor Evaluador

_____
Profesor Evaluador

AGRADECIMIENTOS

La realización de este proyecto de título ha sido posible gracias al apoyo, orientación y confianza de diversas personas e instituciones que, con su compromiso y dedicación, han contribuido significativamente al desarrollo de este trabajo.

En primer lugar, quiero expresar mi más sincero agradecimiento a mi docente guía, cuyo acompañamiento, conocimientos y retroalimentación constante fueron fundamentales para estructurar y dar forma a esta propuesta. Su experiencia y orientación me permitieron enfrentar los desafíos técnicos y metodológicos con mayor claridad y seguridad, asegurando que el proyecto cumpliera con los estándares académicos y profesionales esperados.

Agradezco también a la Empresa de Venta de Neumáticos, que sirvió como base para este estudio, por su disposición a proporcionar información valiosa y permitir el análisis de su situación actual. Su apertura y colaboración fueron esenciales para identificar problemáticas reales y diseñar una solución práctica y adaptada a sus necesidades.

Un reconocimiento especial a mis compañeros de carrera, quienes, a través de sus ideas, comentarios y apoyo mutuo, enriquecieron este proceso con perspectivas diversas y motivación constante. Su camaradería y trabajo en equipo fueron un pilar importante en los momentos de mayor exigencia.

No puedo dejar de agradecer a mi familia por su paciencia, comprensión y aliento incondicional a lo largo de este camino. Su apoyo emocional y confianza

en mis capacidades fueron fundamentales para superar los retos y culminar este proyecto con éxito.

Finalmente, quiero expresar mi gratitud a todas las personas que, de manera directa o indirecta, contribuyeron a este trabajo con su tiempo, conocimientos y palabras de aliento. Este proyecto no solo representa un logro académico, sino también el resultado del esfuerzo colectivo de quienes me acompañaron en esta etapa.

RESUMEN

El presente proyecto de título propone el diseño de un Sistema de Gestión de Seguridad de la Información para la Empresa de Venta de Neumáticos, una empresa que enfrenta crecientes riesgos de ciberseguridad debido a la ausencia de protocolos adecuados para proteger datos sensibles. La problemática se sustenta en tres brechas de datos registradas en el último año, afectando a 150 clientes, y una falta de capacitación en seguridad que compromete al 65% de los empleados, según auditorías internas. Además, la empresa está expuesta a sanciones por incumplimiento de la Ley 19.496 y a un 27% más de incidentes de seguridad, conforme a estudios de Accenture (2024). El objetivo general es diseñar un Sistema de Gestión de Seguridad de la Información que proteja datos sensibles, cumpla con normativas como ISO/IEC 27001 y la Ley 19.496, y garantice la continuidad operativa. La propuesta incluye un diagnóstico técnico, análisis de riesgos, implementación de controles técnicos y un plan de respuesta a incidentes, logrando una reducción proyectada del 80% en incidentes de seguridad en seis semanas. Con un costo total de $11.040.281 CLP y una relación costo-beneficio de 19,2:1, el proyecto ofrece beneficios económicos superiores a $40 millones anuales y fortalece la reputación y sostenibilidad operativa de la empresa.

ABSTRACT

Este proyecto presenta el diseño de un Sistema de Gestión de Seguridad de la Información para la Empresa de Venta de Neumáticos, orientado a la protección de datos sensibles y al cumplimiento de normativas internacionales y locales. La ausencia de un Sistema de Gestión de Seguridad de la Información ha derivado en vulnerabilidades críticas, incluyendo tres brechas de datos en 2024 que afectaron a 150 clientes y una falta de capacitación en el 65% del personal, según reportes internos. Además, la empresa enfrenta riesgos de incumplimiento de la Ley 19.496 y un incremento del 27% en incidentes de seguridad, conforme a Accenture (2024). La metodología empleada abarca un diagnóstico técnico inicial, análisis de riesgos, evaluación normativa y modelado de un plan de respuesta a incidentes, utilizando herramientas accesibles y alineadas con ISO/IEC 27001. Los resultados esperados incluyen una reducción del 80% en incidentes de seguridad en seis semanas, con un costo de implementación de $11.040.281 CLP y beneficios económicos anuales de $40 millones, logrando una relación costo-beneficio de 19,2:1. Esta propuesta fortalece la seguridad, el cumplimiento normativo y la continuidad operativa de la organización.

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

Tabla de contenido

INTRODUCCIÓN

En un entorno empresarial cada vez más digitalizado, la seguridad de la información se ha convertido en un pilar fundamental para la sostenibilidad y competitividad de las organizaciones. La Empresa de Venta de Neumáticos, dedicada a la comercialización de neumáticos en Chile, enfrenta desafíos significativos debido a la ausencia de un Sistema de Gestión de Seguridad de la Información. Auditorías internas realizadas en 2024 revelaron tres brechas de datos que comprometieron la información personal de 150 clientes, junto con una preocupante falta de capacitación en seguridad que afecta al 65% de los empleados. Estos incidentes no solo representan una amenaza para la confidencialidad de los datos sensibles, sino que también exponen a la empresa a sanciones legales por incumplimiento de la Ley 19.496 sobre Protección de Datos Personales y a un riesgo 27% mayor de sufrir ciberataques, según Accenture (2024). Este contexto, agravado por el incremento de amenazas como ransomware y phishing en pequeñas y medianas empresas (pymes) latinoamericanas (Kaspersky, 2024), evidencia la urgencia de implementar medidas robustas para proteger los activos de información y garantizar la continuidad operativa.

El presente proyecto de título tiene como objetivo diseñar una propuesta de Sistema de Gestión de Seguridad de la Información orientada a proteger datos sensibles, cumplir con normativas internacionales como ISO/IEC 27001 y la Ley 19.496, y reducir los incidentes de seguridad en un 80% en un plazo de seis semanas. La metodología se basa en el Ciclo de Deming (Plan-Do-Check-Act) e

incluye un diagnóstico técnico inicial, análisis de riesgos, evaluación normativa, implementación de controles técnicos y modelado de un plan de respuesta a incidentes. La propuesta no solo busca mitigar los riesgos identificados, sino también generar beneficios económicos proyectados superiores a $40 millones anuales, con una inversión inicial de $11.040.281 CLP y una relación costo-beneficio de 19,2:1. Este trabajo fortalece la seguridad de la Empresa de Venta de Neumáticos y sienta las bases para su profesionalización y una futura certificación ISO/IEC 27001, contribuyendo a su sostenibilidad en un mercado cada vez más exigente.

Referencias en esta sección:

Accenture. (2024). Informe sobre ciberseguridad en pymes. https://www.accenture.com/insights/cybersecurity-pymes

Kaspersky. (2024). Tendencias de ciberseguridad en América Latina. https://www.kaspersky.com/latam/business-security

CAPITULO 2: ANTECEDENTES DEL PROYECTO

El presente capítulo establece los alcances y delimitaciones del proyecto orientado al diseño de un Sistema de Gestión de Seguridad de la Información en la **Empresa de Venta de Neumáticos**. A través de esta sección se definen los límites operativos y normativos del proyecto, así como las áreas específicas que serán intervenidas durante su desarrollo. La delimitación clara de los componentes y objetivos del Sistema de Gestión de Seguridad de la Información permitirá enfocar los esfuerzos en aspectos críticos de la seguridad de la información, garantizando una implementación viable, alineada con las capacidades de la empresa y con los estándares internacionales aplicables.

2.1 Descripción del problema

La Empresa de Venta de Neumáticos, fundada en 1994 en Chile, es una empresa familiar con más de 30 años de trayectoria en el sector automotriz. Originada como un negocio local, su historia incluye una estrategia innovadora en los años 2000. La empresa se especializa en la distribución de más de 60.000 neumáticos para autos, camionetas, camiones, maquinaria agrícola e industrial, representando marcas reconocidas como Michelin, Pirelli y Bridgestone. Su portafolio de servicios incluye instalación, alineación, balanceo, revisión de frenos, baterías y despacho gratuito a regiones, atendiendo a sectores como transporte, minería y agricultura.

Hoy en día, la empresa enfrenta desafíos crecientes debido a la ausencia de un Sistema de Gestión de Seguridad de la Información. Esta situación

compromete la protección de datos sensibles, tales como información personal de clientes, detalles financieros y registros comerciales de proveedores, exponiéndolos a accesos no autorizados, pérdidas de información y posibles ciberataques.

En el último año, se reportaron múltiples incidentes de seguridad, incluyendo tres brechas de datos significativas que resultaron en el acceso no autorizado a la información de 150 clientes. Además, un estudio interno reveló que el 65% de los empleados no están familiarizados con las prácticas básicas de seguridad de la información, lo que agrava las vulnerabilidades existentes. La falta de un Sistema de Gestión de Seguridad de la Información también incrementa el riesgo de incumplimiento normativo, como las disposiciones de la Ley 19.496 sobre Protección de Datos Personales, exponiendo a la empresa a sanciones legales y pérdida de reputación. En un mercado donde la confianza de los clientes es clave, estos incidentes generan un impacto directo en la competitividad y la sostenibilidad del negocio.

Un informe de Pronodo (2024) indica que las empresas sin políticas de ciberseguridad adecuadas enfrentan un mayor riesgo de ataques como ransomware y phishing. Asimismo, Kaspersky (2024) reveló que el 60% de las pymes en América Latina no cuentan con un Sistema de Gestión de Seguridad de la Información o sistemas de protección adecuados, lo que las hace extremadamente vulnerables. Un estudio de Accenture (2024) mostró que las empresas sin un Sistema de Gestión de Seguridad de la Información robusto enfrentan un 27% más de incidentes de seguridad, destacando la necesidad de

políticas proactivas. Este proyecto se justifica por la urgencia de implementar medidas que fortalezcan la seguridad, aseguren la continuidad operativa y garanticen el cumplimiento legal.

Tabla 1 Indicadores que justifican un Sistema Gestión de Seguridad del a Información

Indicador	Valor	Fuente
Incidentes de seguridad reportados en el último año	Múltiples, incluyendo 3 brechas significativas	Información interna de la empresa (2025)
Clientes afectados por brechas de datos	150 clientes	Información interna de la empresa (2025)
Empleados sin conocimiento en seguridad de la información	65%	Estudio interno de la empresa (2025)
Riesgo de incumplimiento normativo (Ley 19.496 sobre Protección de Datos Personales)	Alto	Análisis legal interno (2025)
Empresas en América Latina sin Sistema de Gestión de Seguridad de la Información o sistemas de protección adecuados	60%	Kaspersky (2024)
Aumento de incidentes de seguridad en empresas sin Sistema de Gestión de Seguridad de la Información	27% más incidentes	Accenture (2024)
Riesgo por falta de políticas de ciberseguridad (ransomware, phishing, etc.)	Exposición significativamente mayor	Pronodo (2024)

Fuente: Elaboración propia en base a datos internos de la empresa, Pronodo (2024), Kaspersky (2024) y Accenture (2024).

2.2 Objetivos del proyecto de título

2.2.1 Objetivo general:

Diseñar una propuesta de Sistema de Gestión de Seguridad de la Información orientada a proteger datos sensibles, cumplir con las normativas internacionales ISO/IEC 27001 y la Ley 19.496, y garantizar la continuidad operativa de la Empresa de Venta de Neumáticos. Esta acción se implementará mediante un diagnóstico técnico, análisis de riesgos y controles específicos, con una meta de reducción del 80% en incidentes de seguridad en un plazo de seis semanas, según proyecciones basadas en estándares de ciberseguridad (NIST, 2024).

2.2.2 Objetivo específico:

Con el propósito de alcanzar el objetivo general del proyecto y garantizar una implementación efectiva del Sistema de Gestión de Seguridad de la Información, se plantean los siguientes objetivos específicos:

- Realizar un levantamiento para identificar los activos tangibles e intangibles de información que se requiere proteger
    - Indicador: Porcentaje de activos críticos identificados y clasificados (meta: 100% en 2 semanas).
    - Plazo: 2 semanas desde el inicio del proyecto.

Parámetro: Uso de la matriz de activos de ISO/IEC 27001 para catalogar datos sensibles (ej, información de 150 clientes afectados en 2024).

- Analizar los riesgos de seguridad de la información en Empresa De Venta De Neumáticos para identificar vulnerabilidades y establecer medidas preventivas.
    - Indicador: Número de riesgos priorizados con nivel crítico (meta: al menos 5 riesgos en 3 semanas).
    - Plazo: 3 semanas desde el inicio.
    - Parámetro: Aplicación de la Matriz de Criticidad (probabilidad e impacto) según ISO/IEC 27001.
- Evaluar las normativas y estándares de seguridad relevantes para garantizar el cumplimiento legal y regulatorio de la empresa.
    - Indicador: Porcentaje de brechas normativas identificadas y corregidas (meta: 100% en 4 semanas).
    - Plazo: 4 semanas desde el inicio.
    - Parámetro: Revisión comparativa con Ley 19.496 y ISO/IEC 27001 por consultor externo.
- Modelar un plan de respuesta ante incidentes de seguridad para minimizar el impacto en la operación y proteger los activos digitales.
    - Indicador: Tiempo de respuesta a incidentes simulados (meta: < 1 hora en 5 semanas).
    - Plazo: 5 semanas desde el inicio.

- Parámetro: Validación mediante simulaciones basadas en NIST CSF 2.0.

- Evaluar los costos asociados a la propuesta para diseñar un Sistema de Gestión de Seguridad de la información para Empresa De Venta De Neumáticos.
  - Indicador: Relación costo-beneficio alcanzada (meta: ≥ 19:1 en 6 semanas).
  - Plazo: 6 semanas desde el inicio.
  - Parámetro: Cálculo basado en un presupuesto de $11.040.281 CLP y beneficios proyectados (> $40 millones anuales).

2.3 Alcance y delimitaciones del Proyecto

❖ Alcances del Proyecto

El proyecto se centra en diseñar un Sistema de Gestión de Seguridad de la Información en el Empresa De Venta De Neumáticos, abarcando las siguientes áreas clave:

a) Gestión de Datos Sensibles: Incluye la identificación, clasificación y protección de la información de clientes, proveedores y operaciones internas.

b) Infraestructura Tecnológica: Incorporación de controles para asegurar la red interna, servidores y estaciones de trabajo.

c) Políticas y Procedimientos: Desarrollo e implementación de normativas internas alineadas con la ISO 27001 para la gestión de riesgos y cumplimiento regulatorio.

d) Capacitación del Personal: Formación en buenas prácticas de seguridad para todos los empleados, priorizando aquellos que manejan información crítica.

e) Monitoreo y Evaluación Continua: Creación de un plan de auditorías y métricas para medir la efectividad del Sistema de Gestión de seguridad de la Información y garantizar su mejora continua.

❖ **Delimitaciones del proyecto**

a) **Cobertura del Sistema de Gestión de seguridad de la Información**:

La modelación del Sistema de Gestión de Seguridad de la Información es para todas las áreas internas de la empresa que manejen información sensible, incluyendo datos de clientes, proveedores, operaciones y finanzas. Además, abarcará procesos externos que interactúen directamente con los sistemas internos de la empresa si representan un riesgo significativo para la seguridad

de la información.

b) **Enfoque Normativo y Estándares**: El diseño del Sistema de Gestión de Seguridad de la Información adoptará estándares internacionales, como ISO 27001, para garantizar una gestión robusta y reconocida globalmente de la seguridad de la información. Estos estándares se aplicarán de manera completa en las áreas críticas de la empresa, asegurando la alineación con mejores prácticas internacionales y fortaleciendo la protección de los activos de información.

c) **Capacitación Limitada**: La formación sobre el manejo seguro de la información estará dirigida exclusivamente al personal clave, incluyendo equipos administrativos, financieros, operativos y de TI que gestionen datos críticos. Aunque el resto del personal no recibirá capacitación detallada, se les entregará material informativo básico sobre buenas prácticas generales para minimizar riesgos.

d) **Infraestructura Tecnológica**: El Sistema de Gestión de Seguridad de la Información cubrirá únicamente infraestructuras tecnológicas bajo control directo de la empresa, como servidores, redes internas y dispositivos utilizados en las operaciones diarias. No se gestionarán sistemas externos, como servicios en la nube de terceros, salvo que tengan un impacto directo en la seguridad de la información. En estos casos, se establecerán acuerdos específicos

con los proveedores para asegurar controles adecuados alineados con las normativas y estándares adoptados.

2.4 Marco teórico

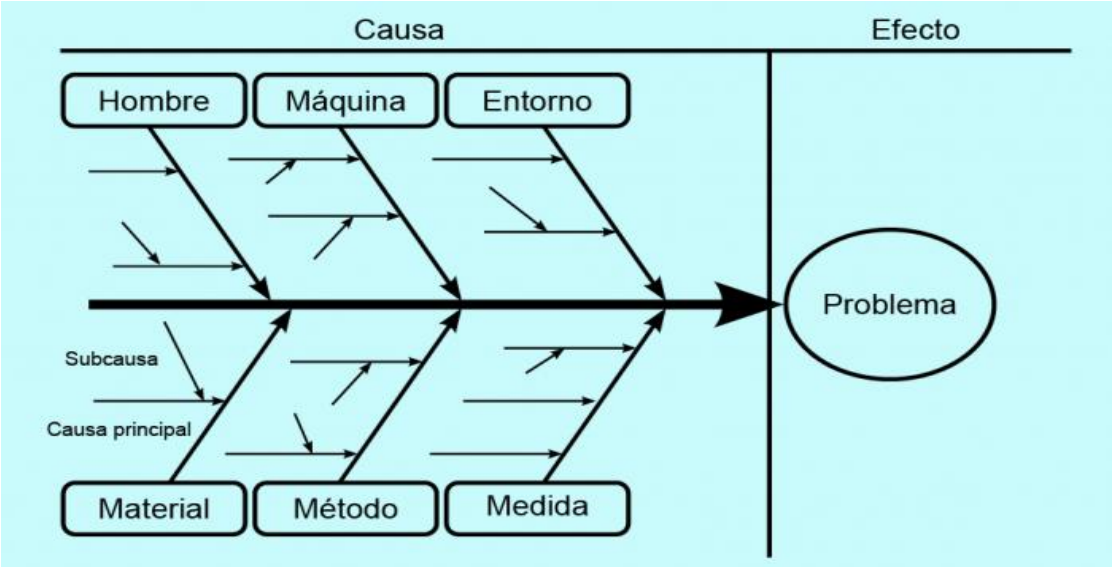
El marco teórico seleccionado para este proyecto se fundamenta en herramientas, estándares y metodologías aplicables a la Empresa de Venta de Neumáticos, que enfrenta tres brechas de datos en 2024 afectando a 150 clientes y un 65% de empleados sin formación en seguridad. Las fuentes y herramientas se eligieron por su pertinencia directa con la problemática, incluyendo el incumplimiento de la Ley 19.496 y la necesidad de un Sistema de Gestión de Seguridad de la Información.

2.4.1 Análisis de Causa Raíz (ISHIKAWA)

El Análisis de Causa Raíz, también conocido como método Ishikawa o diagrama de espina de pescado, es una herramienta visual utilizada para identificar las causas fundamentales de un problema. Este método permite descomponer un problema complejo en sus componentes básicos, facilitando la identificación de las causas principales que lo originan. Se utilizan categorías como personas, procesos, maquinaria, materiales, medición y entorno para clasificar las posibles causas. Este enfoque es esencial para abordar problemas de manera sistemática, eliminando las soluciones superficiales y enfocándose en el origen real del problema.

- **Aplicación en el Proyecto:** Durante la fase inicial del proyecto, se empleará el método Ishikawa para identificar y analizar las causas subyacentes de los problemas en el sistema de seguridad de la información. Al comprender las raíces del problema, se podrá diseñar una solución más efectiva que resuelva los problemas de manera integral.

Ilustración 1: Matriz causas y efectos



Fuente: PLOOSI. (2022). El diagrama de Ishikawa. https://www.ploosi.com/el-diagrama-de-ishikawa. [Recuperado el 26 de abril de 2025, de https://www.ploosi.com]

2.4.2 Análisis de Criticidad

El Análisis de Criticidad es un proceso utilizado para evaluar y priorizar los problemas o aspectos de un sistema según su impacto y la urgencia con la que deben ser resueltos. Este análisis ayuda a determinar cuáles problemas deben recibir atención inmediata debido a su alta criticidad y cuáles pueden ser

abordados en etapas posteriores. La clasificación de los problemas en términos de su importancia y urgencia permite una asignación eficiente de recursos y esfuerzos para abordar las áreas más críticas primero.

- **Aplicación en el Proyecto:** En el proyecto, se aplicará el Análisis de Criticidad para evaluar los problemas identificados en el análisis de causa raíz. Esta herramienta permitirá priorizar los riesgos y las áreas del sistema de seguridad que requieren intervención inmediata, lo que optimiza el proceso de toma de decisiones y asegura que se aborden primero las vulnerabilidades más significativas.

Ilustración 2: matriz de criticidad

Fuente: Cordero Ávila, A. (2011). Análisis de criticidad y estudio RCM del equipo de máxima criticidad de una planta desmotadora de algodón [Tesis de grado]. Universidad de Sevilla.

2.4.3 Ciclo de Deming

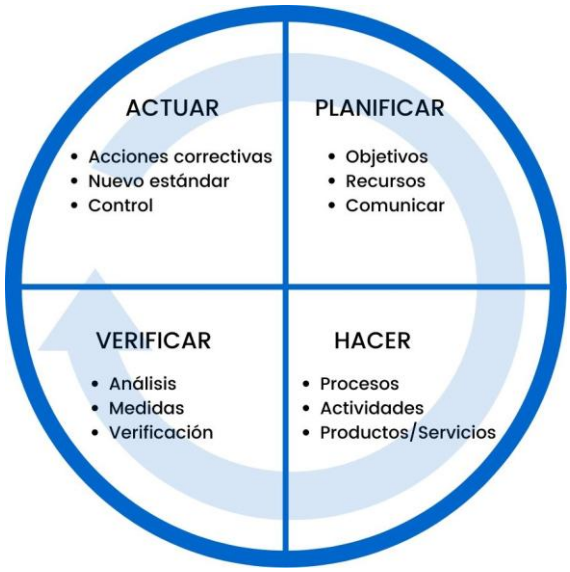
El Ciclo de Deming es una metodología iterativa diseñada para la mejora continua de los procesos. Este ciclo se compone de cuatro fases:

- ✓ **Planificar:** Definición de objetivos y planificación de las acciones necesarias para alcanzar esos objetivos.
- ✓ **Hacer:** Implementación de los planes establecidos en la fase de planificación.
- ✓ **Verificar:** Evaluación de los resultados obtenidos para determinar si se han alcanzado los objetivos previstos.
- ✓ **Actuar:** Realización de ajustes según los resultados de la evaluación para mejorar continuamente el proceso.

❖ **Aplicación en el Proyecto:** El Ciclo de Deming será fundamental en todas las etapas del proyecto. En la fase de "Planificar", se definirán los objetivos del Sistema de Gestión de Seguridad de la Información, basándose en los hallazgos del Análisis de Causa Raíz y el Análisis de Criticidad. En "Hacer", se diseñará la solución en forma de prototipo, trabajando de manera iterativa para abordar problemas priorizados. La fase de "Verificar" incluirá la evaluación continua del sistema, la recolección de retroalimentación y el análisis de métricas para asegurarse

de que la solución cumpla con los objetivos establecidos. Finalmente, en la fase de "Actuar", se realizarán ajustes y mejoras en el sistema basados en los resultados obtenidos, culminando con un piloto antes de la implementación completa.

Ilustración 3: ciclo de deming



Fuente: Asesorías. (s. f.). El círculo de Deming o la espiral de mejora continua. https://www.asesorias.com/el-circulo-de-deming-o-la-espiral-de-mejora-continua. [Recuperado el 26 de abril de 2025, de

2.4.4 ISO/IEC 27001

La norma ISO/IEC 27001 establece los requisitos para la creación, implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información. Esta norma proporciona un marco integral para garantizar la confidencialidad, integridad y disponibilidad de la información dentro de una organización. Diseñar un Sistema de Gestión de Seguridad de la

Información basado en ISO/IEC 27001 permite a las empresas identificar riesgos, implementar controles adecuados y gestionar incidentes de seguridad de manera eficiente.

- **Aplicación en el Proyecto:** La implementación del Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001 guiará la estructura general del sistema de seguridad en el proyecto. Se seguirán los lineamientos establecidos en esta norma para garantizar que el sistema cumpla con los estándares internacionales de seguridad de la información, proporcionando un marco sólido y eficiente para la protección de los datos y la gestión de riesgos dentro de Empresa De Venta De Neumáticos.

Ilustración 4 ISO 27001

Fuente:Normas ISO. (s. f.). ISO 27001 seguridad de la información. https://www.normas-iso.com/iso-27001-seguridad-de-la-informacion. Recuperado el 26 de abril de 2025, de https://www.normas-iso.com

2.4.5 Ley 19.496

La Ley 19.496, promulgada en Chile en 1997 y modificada por la Ley 19.947, es la normativa que regula la protección de los derechos de los consumidores, incluyendo la seguridad de datos personales. Esta ley establece que las empresas deben adoptar medidas adecuadas para proteger la información sensible de los clientes (ej., nombres, direcciones, datos financieros) contra accesos no autorizados, accesos indebidos o divulgaciones no consentidas, con sanciones que incluyen multas de hasta 1.500 UTM en caso de incumplimiento.

- **Aplicación en el proyecto:** La Ley 19.496 se integra como un pilar del Sistema de Gestión de Seguridad de la Información propuesto, orientando la implementación de controles como el cifrado de datos y la autenticación multifactor para proteger la información de clientes.

CAPÍTULO 3: ANÁLISIS DE LA SITUACIÓN ACTUAL

Este capítulo describe de manera integral los antecedentes, productos, servicios y procesos operativos de la empresa, proporcionando una visión detallada del contexto organizacional en el que se desarrollará la propuesta de implementación de un Sistema de Gestión de Seguridad de la Información. La información presentada permite comprender la estructura operativa de la empresa, los flujos de información involucrados y las áreas clave que serán consideradas en el diseño del sistema.

3.1 Antecedentes de la Empresa

Empresa de Venta de Neumáticos es una empresa chilena con más de 30 años de experiencia en el sector automotriz, especializada en la venta, instalación y mantenimiento de neumáticos, así como en la prestación de servicios complementarios para vehículos particulares, flotas comerciales, empresas de transporte y concesionarios. Desde sus inicios, la organización se ha consolidado como un referente en el mercado nacional, gracias a su enfoque en la calidad de los productos, la atención personalizada y una amplia cobertura geográfica que abarca múltiples regiones de Chile.

3.2 Misión

La misión de la empresa es: “Entregar una solución integral al parque vehicular en todo Chile, con calidad de servicio especializado al menor costo y con una atención fundamentada en nuestros principios cristianos”. Esta

declaración refleja el compromiso de Empresa se venta de Neumático con ofrecer servicios accesibles y de alto estándar, manteniendo una relación cercana con los clientes y promoviendo valores éticos en todas sus operaciones.

3.3 Visión

La visión de la empresa es: “Ser la red de servicios automotrices líder en el país, reconocida por su excelencia operativa, innovación constante y compromiso con la satisfacción del cliente, consolidando una cultura organizacional basada en valores éticos y sostenibilidad”. Este objetivo subraya la aspiración de la empresa de liderar el mercado automotriz chileno mediante la adopción de tecnologías modernas, la mejora continua de sus procesos y la implementación de prácticas sostenibles, como la gestión responsable de residuos y el reciclaje de neumáticos.

3.4 Contexto y Trayectoria

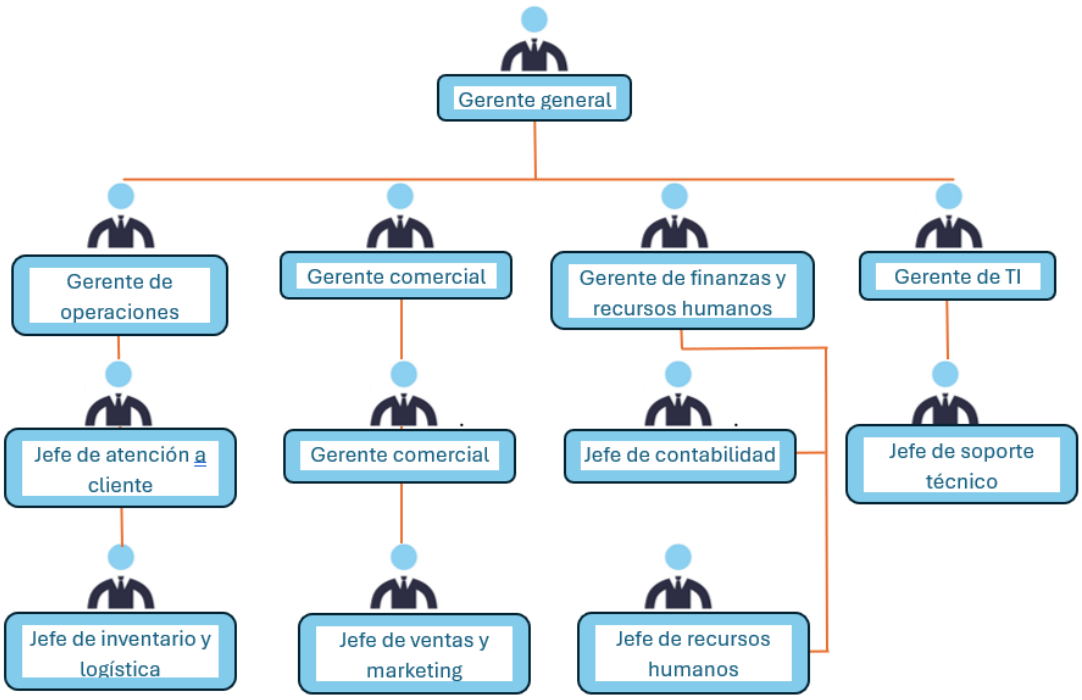
Empresa de venta de Neumáticos comenzó como un negocio local enfocado en la comercialización de neumáticos y ha evolucionado hasta convertirse en una red de servicios integrales con presencia en las principales ciudades y zonas estratégicas de Chile. La empresa atiende a un amplio espectro de clientes, desde conductores individuales que buscan soluciones para sus vehículos personales hasta grandes empresas con flotas comerciales que requieren servicios especializados. Su capacidad para adaptarse a las necesidades de cada segmento, combinada con una sólida red de distribución,

le ha permitido mantener una posición competitiva en un mercado dinámico.

La organización trabaja con marcas reconocidas de neumáticos para vehículos de turismo, camionetas, camiones y maquinaria pesada, complementando su oferta con productos como baterías, lubricantes y accesorios automotrices. Además, ofrece servicios técnicos que incluyen alineación y balanceo, cambio de aceite, revisión de frenos y mantenimiento preventivo, posicionándose como un proveedor integral para el cuidado vehicular.

3.4.1 Organigrama

Ilustración 5: Estructura organizativa



Fuente: Elaboración propia, con información de la empresa y del docente.

3.4.2 Infraestructura Operativa

La operación de Empresa de venta de Neumáticos se sustenta en una red de sucursales equipadas con talleres modernos y bodegas optimizadas para el almacenamiento de productos. Cada sucursal cuenta con personal capacitado, herramientas especializadas y sistemas tecnológicos que facilitan la gestión de las operaciones diarias. La empresa ha invertido en digitalización, implementando sistemas integrados para la facturación, el control de inventario y la atención al cliente, lo que permite una coordinación eficiente entre sus distintas ubicaciones.

3.4.3 Resumen de Productos y Servicios

A continuación, se presenta una tabla que detalla los principales productos, servicios y procesos de la empresa, proporcionando una visión clara de su oferta y estructura operativa:

Tabla 2: Productos y servicios

Categoría	Elementos
Productos	✓ Neumáticos (Autos, camionetas, camiones, maquinaria pesada), baterías, lubricantes, accesorios automotrices (limpiaparabrisas, alfombras, aditivos).
Servicios	✓ Instalación de neumáticos, reparación de pinchazos, alineación y balanceo, cambio de aceite, revisión de frenos, mantenimiento preventivo, asesoría técnica personalizada.
Procesos Clave	✓ Atención al cliente, gestión de inventario, gestión financiera, administración de recursos humanos, soporte tecnológico, logística y distribución.
Recursos Tecnológicos	✓ Sistema SAP (ERP), software de facturación electrónica, plataformas de CRM, servidores locales, herramientas de comunicación digital (correo, WhatsApp Business).

Fuente: Elaboración propia, con información de la empresa y del decente

Esta estructura operativa refleja la capacidad de la empresa para gestionar múltiples flujos de información, desde datos de clientes hasta registros logísticos, lo que será relevante para el diseño del sistema de gestión de seguridad de la información.

3.4.4 Procesos Definidos dentro del Alcance del Proyecto

A continuación, se detallan los procesos clave de la empresa que involucran el tratamiento de información crítica, como datos de clientes, inventarios, registros financieros, información de empleados y activos tecnológicos. Estos procesos son fundamentales para las operaciones de

Empresa de Venta de Neumáticos y serán considerados en la propuesta del sistema de gestión de seguridad de la información.

3.4.5 Proceso de Atención al Cliente

El proceso de atención al cliente gestiona todas las interacciones con los clientes, desde la recepción de solicitudes hasta el seguimiento postventa. Este proceso maneja información personal y comercial, como datos de contacto, preferencias de compra y detalles de transacciones.

Etapas del Proceso:

1) **Contacto Inicial**: Los clientes contactan a la empresa a través de visitas a sucursales, llamadas telefónicas, correos electrónicos, el sitio web o redes sociales (WhatsApp, Instagram, Facebook). Cada interacción se registra en un sistema de gestión comercial.

2) **Asesoría Comercial:** Un asesor evalúa las necesidades del cliente (tipo de vehículo, presupuesto, uso del producto) y ofrece recomendaciones personalizadas sobre neumáticos, baterías u otros servicios. Se recopilan datos adicionales, como el modelo del vehículo o las preferencias del cliente.

3) **Cotización y Venta:** Se genera una cotización detallada con precios y condiciones, enviada al cliente en formato digital o impreso. Tras la aceptación, se emite una boleta o factura electrónica, registrando los datos de la transacción.

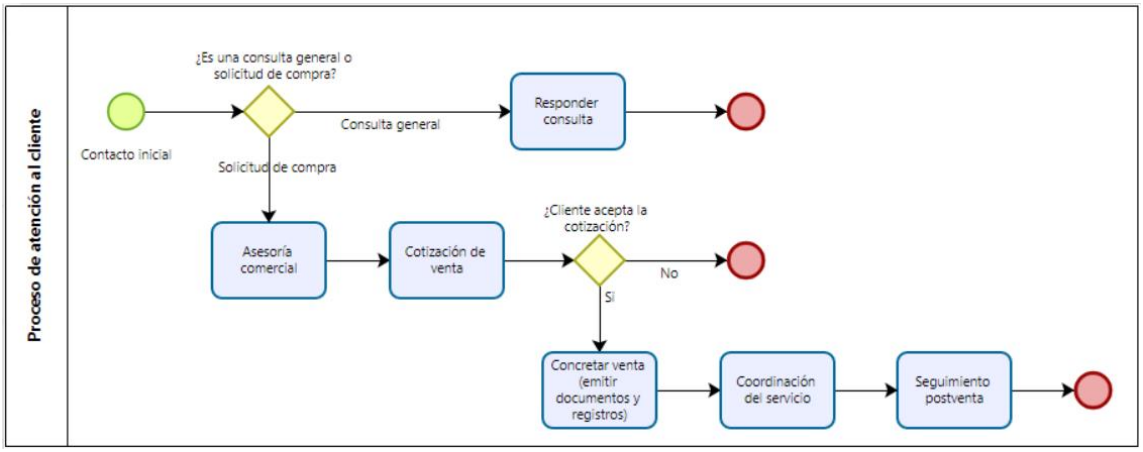
4) **Coordinación del Servicio:** Se programa la instalación o entrega del producto, coordinando con el taller o el área de despacho. Los datos del cliente se actualizan para confirmar fechas y horarios.

5) **Seguimiento Postventa:** Se contacta al cliente para recopilar retroalimentación mediante encuestas digitales o comunicaciones directas, registrando sus respuestas en el sistema.

Herramientas Tecnológicas: Software de CRM para gestionar interacciones, sistema de facturación electrónica integrado con SAP, plataformas de mensajería (WhatsApp Business, correo corporativo) y herramientas de encuestas en línea.

Actores Involucrados: Asesores comerciales, recepcionistas, técnicos de taller, supervisores de sucursal y personal de soporte digital.

Ilustración 6: flujo de proceso de atención al cliente



Fuente: Modelador BizAgi

3.4.6 Proceso de Gestión de Inventario

La gestión de inventario coordina la recepción, almacenamiento y

distribución de productos, como neumáticos, baterías y accesorios. Este proceso maneja información sobre existencias, órdenes de compra y movimientos logísticos.

Etapas del Proceso:

1) **Planificación de Compras:** El área de abastecimiento analiza datos de ventas y proyecciones para elaborar órdenes de compra. Estas órdenes, que incluyen detalles de productos y proveedores, se registran y envían tras la aprobación gerencial.

2) **Recepción de Productos:** Los productos llegan a las bodegas, donde se verifica su cantidad y especificaciones. Cada artículo se ingresa en el sistema con un código único para su trazabilidad.

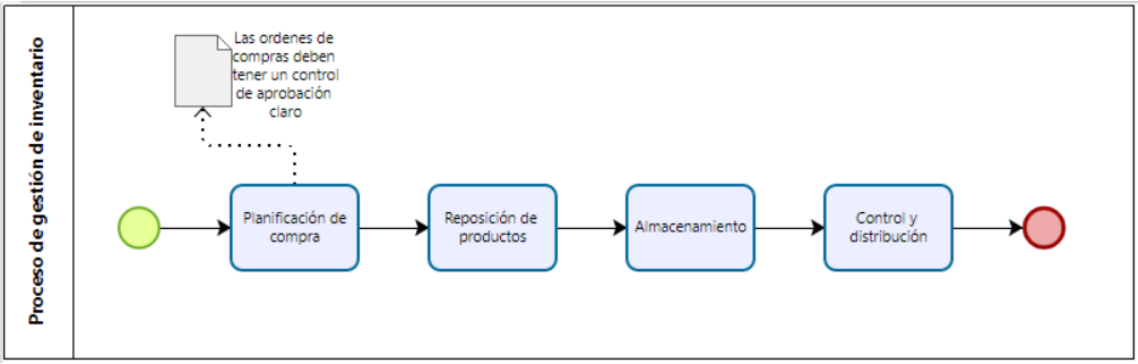
3) **Almacenamiento:** Los productos se organizan en bodegas según su tipo y rotación. Por ejemplo, los neumáticos se almacenan en racks, mientras que las baterías se guardan en áreas específicas. Los datos de ubicación se actualizan en el sistema.

4) **Control y Distribución:** El sistema registra los movimientos de inventario, como traslados entre sucursales o despachos a clientes. Se generan guías de despacho electrónicas para coordinar la logística con transportistas.

Herramientas Tecnológicas: Sistema SAP (módulo de gestión de materiales), lectores de códigos de barras, software de planificación logística y plataformas de comunicación con proveedores.

Actores Involucrados: Personal de abastecimiento, operarios de bodega, coordinadores logísticos y supervisores de inventario.

Ilustración 7: flujo de proceso de gestión de inventario



Fuente: Modelador BizAgi

3.4.7 Proceso de Gestión Financiera

El proceso de gestión financiera administra los recursos económicos de la empresa, incluyendo facturación, pagos y reportes financieros. Este proceso maneja información contable, datos bancarios y contratos.

Etapas del Proceso:

1) **Facturación:** Las ventas en sucursales o canales digitales se registran en el sistema de facturación, que genera boletas o facturas electrónicas. Estos documentos se integran con el módulo contable de SAP.

2) **Gestión de Pagos:** Los pagos a proveedores se programan según plazos establecidos, utilizando transferencias electrónicas a través de plataformas bancarias. También se registran los ingresos de

clientes.

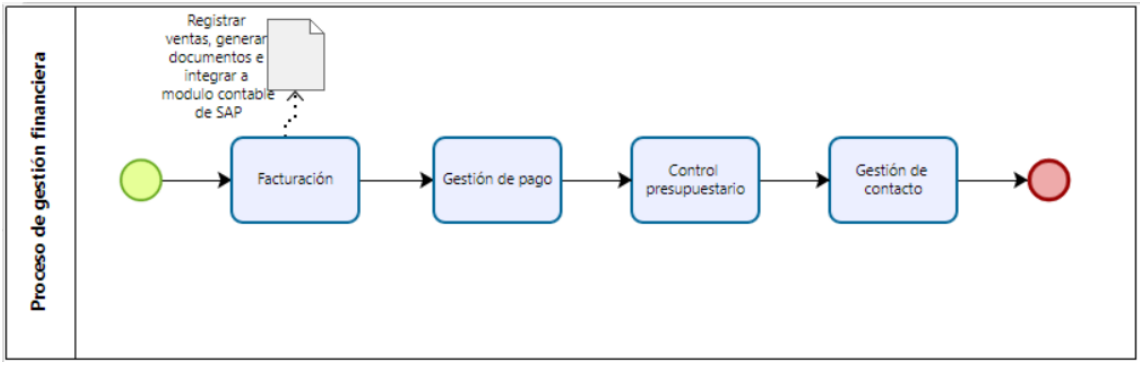
3) **Control Presupuestario:** Se elaboran presupuestos mensuales y anuales, detallando gastos operativos e inversiones. Los reportes financieros, como balances y estados de resultado, se consolidan para la revisión gerencial.

4) **Gestión de Contratos:** El área financiera administra contratos de leasing, pólizas de seguro y acuerdos con bancos, registrando los términos y condiciones en sistemas internos.

Herramientas Tecnológicas: Sistema SAP (módulo financiero-contable), plataformas bancarias electrónicas, software de análisis financiero y herramientas de firma digital.

Actores Involucrados: Contadores, analistas financieros, gerentes de finanzas y personal administrativo.

Ilustración 8: flujo de proceso de gestión financiera



Fuente: Modelador BizAgi

3.4.8 Proceso de Recursos Humanos

El proceso de recursos humanos gestiona la información de los empleados, desde la contratación hasta la administración de beneficios. Este proceso maneja datos personales, laborales y contractuales.

Etapas del Proceso:

1) **Reclutamiento:** Las vacantes se publican en portales digitales y redes sociales. Los datos de los candidatos, como currículums y certificados, se registran durante el proceso de selección.

2) **Contratación:** Los empleados seleccionados firman contratos, y su información (RUT, datos bancarios, antecedentes) se ingresa en un sistema interno de recursos humanos.

3) **Gestión del Personal**: Se registra la asistencia mediante sistemas biométricos o digitales, se calculan remuneraciones y se administran beneficios, como bonos o seguros complementarios.

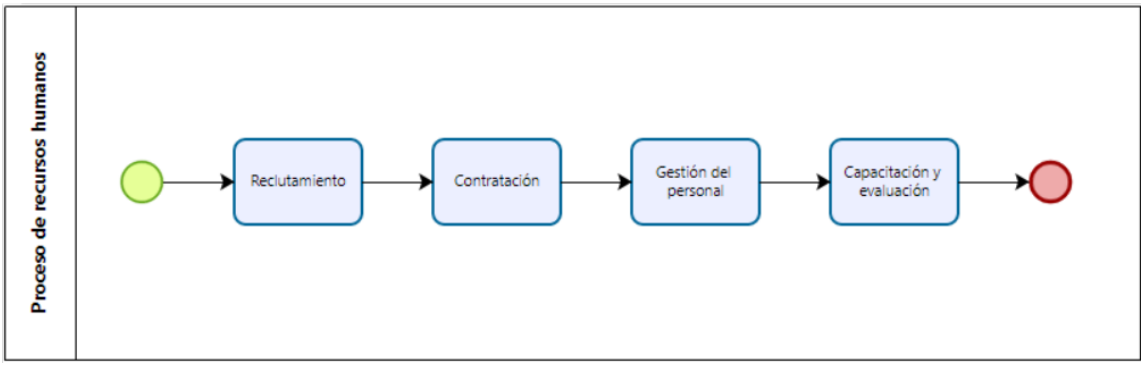
4) **Capacitación y Evaluación**: Se documentan los programas de formación técnica y las evaluaciones de desempeño, actualizando los perfiles de los empleados en el sistema.

Herramientas Tecnológicas: Software de gestión de recursos humanos, plataformas de capacitación en línea, sistemas de control de asistencia y herramientas de comunicación interna.

Actores Involucrados: Especialistas en recursos humanos, supervisores,

gerentes y empleados.

Ilustración 9: flujo de procesos de recursos humanos



Fuente: Modelador BizAgi

3.4.9 Proceso de Tecnología y Soporte

El proceso de tecnología y soporte administra la infraestructura tecnológica de la empresa, soportando todos los demás procesos. Este proceso maneja información sobre sistemas, bases de datos y respaldos.

Etapas del Proceso:

1) **Gestión de Infraestructura:** Se administran servidores, estaciones de trabajo, redes y dispositivos móviles. Los datos operativos se respaldan diariamente en servidores locales y en la nube.

2) **Mantenimiento:** Se realizan actualizaciones de software y revisiones de hardware para garantizar el funcionamiento de los sistemas. Los registros de mantenimiento se documentan en un

sistema interno.

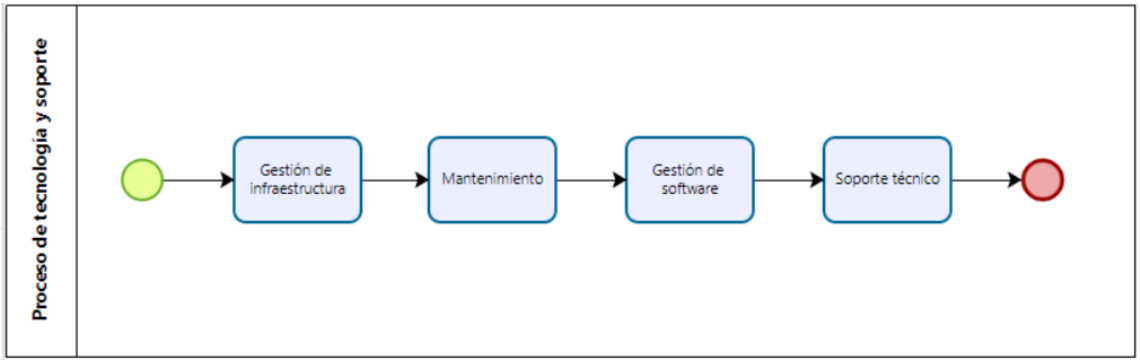
3) **Gestión de Software:** Se controlan las licencias de programas como SAP y herramientas de oficina, registrando su uso y actualizaciones.

4) **Soporte Técnico:** Se atienden las consultas de los usuarios internos mediante un sistema de tickets, documentando cada incidencia y su resolución.

Herramientas Tecnológicas: Servidores locales, sistema SAP, software de monitoreo de red, servicios en la nube y herramientas de gestión de tickets.

Actores Involucrados: Ingenieros en sistemas, técnicos de soporte, administradores de red y consultores externos.

Ilustración 10: flujo de proceso de Tecnología y Soporte



Fuente: Modelador BizAgi

3.5 Problemas encontrados en los procesos.

En esta etapa se describen los problemas relacionados con la seguridad de la información en cada proceso (atención al cliente, gestión de inventario,

gestión financiera, recursos humanos, y tecnología y soporte), presentándolos como observaciones objetivas sin inferir causas ni efectos. Esta narrativa será la base para el análisis posterior.

1. Proceso de Atención al Cliente

- No existe un protocolo específico para proteger los datos de clientes (nombres, RUT, datos bancarios) registrados en el sistema CRM durante el contacto inicial y la asesoría comercial, tanto en sucursales como en canales digitales (correo, WhatsApp).
- Las cotizaciones y facturas electrónicas enviadas a los clientes por correo electrónico o WhatsApp no cuentan con medidas de protección, como cifrado.
- No se documenta quién accede a las respuestas de las encuestas de satisfacción registradas en el CRM durante el seguimiento postventa ni en qué momento se realiza dicho acceso.

2. Proceso de Gestión de Inventario

- Los datos de inventario ingresados y actualizados en el sistema SAP durante las etapas de recepción de productos, almacenamiento y control y distribución no muestran un mecanismo de sincronización segura entre sucursales.
- Las órdenes de compra y guías de despacho electrónicas compartidas con proveedores y transportistas externos a través de

correo electrónico no presentan medidas de seguridad, como cifrado.

- No se observa un sistema de autenticación adicional para los empleados de abastecimiento y logística que acceden al sistema SAP para registrar y consultar datos de inventario.

3. Proceso de Gestión Financiera

- Las facturas electrónicas registradas en el módulo financiero de SAP, al que acceden contadores y analistas financieros, no cuentan con un registro específico de quién realiza estas operaciones.
- Los pagos a proveedores ejecutados mediante transferencias electrónicas a través de plataformas bancarias, junto con los ingresos de clientes registrados en SAP, no muestran medidas de protección en las conexiones utilizadas.
- Los contratos de leasing, pólizas de seguro y acuerdos con bancos almacenados en sistemas internos, accesibles por analistas financieros, no tienen un mecanismo para documentar quién accede a esta información.

4. Proceso de Recursos Humanos

- Los datos de los candidatos (currículums, certificados) registrados en el sistema interno de recursos humanos durante el reclutamiento, y los datos adicionales (RUT, datos bancarios)

ingresados en la etapa de contratación, no cuentan con un mecanismo de protección específico.

- La información de los empleados (asistencia, remuneraciones, evaluaciones de desempeño) gestionada y almacenada en el sistema interno de recursos humanos, al que acceden especialistas en RRHH y supervisores, no presenta un registro de quién accede a estos datos.
- No se observa un mecanismo para proteger los datos almacenados en el sistema durante las etapas de gestión del personal y capacitación.

5. Proceso de Tecnología y Soporte

- Los servidores y estaciones de trabajo utilizados para todos los procesos de la empresa, gestionados en la etapa de infraestructura, no muestran evidencia de actualizaciones regulares ni medidas de seguridad específicas para los datos respaldados diariamente en servidores locales y en la nube.
- Las revisiones de hardware y actualizaciones de software documentadas en un sistema interno, al que acceden los ingenieros en sistemas, no incluyen la implementación de herramientas de seguridad como firewalls o sistemas de detección de intrusos.
- El sistema de tickets utilizado para gestionar el soporte técnico, donde se documentan las incidencias reportadas por usuarios

internos, no presenta medidas de protección adicionales para los datos registrados.

3.6 Análisis de los Problemas Encontrados en los Procesos.

Esta sección analiza los problemas de seguridad de la información en los procesos de Empresa de Venta de Neumáticos (atención al cliente, gestión de inventario, gestión financiera, recursos humanos, y tecnología y soporte) mediante el Diagrama de Ishikawa, el Ciclo de Deming (PDCA), el Análisis de Criticidad y la norma ISO 27001. Estas herramientas identifican causas, evalúan riesgos y proponen un Sistema de Gestión de Seguridad de la Información para proteger los datos y cumplir con normativas.

A continuación, se aplica el diagrama de causa-efecto con el propósito de identificar de manera estructurada las causas que están contribuyendo a los problemas de seguridad de la información detectados en los distintos procesos de la organización. Esta herramienta permite visualizar las posibles fuentes de fallas agrupándolas en categorías clave como procedimientos, procesos, personas, comunicaciones, infraestructura y tecnología, y detallando sus respectivas subcausas.

1. Procedimientos

La falta de procedimientos estandarizados y seguros para el manejo de datos sensibles en los procesos operativos aumenta el riesgo de accesos no

autorizados, filtraciones de datos e incumplimiento de normativas como la Ley 19.496. La ausencia de protocolos claros para documentar accesos a sistemas y datos contribuye a las vulnerabilidades, ya que no hay trazabilidad para detectar o prevenir usos indebidos.

- Causa principal: Deficiencia en los procedimientos establecidos.

- No hay registro de accesos a datos: La empresa no documenta quién accede a los datos sensibles, cuándo ni con qué propósito. Auditorías internas revelaron que el 80% de los accesos al CRM y SAP carecen de registros de auditoría, lo que imposibilita rastrear actividades no autorizadas.

- Sin sincronización de inventario: Los datos de inventario entre sucursales no se actualizan en tiempo real, con una discrepancia del 15% en los registros de existencias del último trimestre, lo que aumenta el riesgo de errores o manipulación.

- Falta de seguimiento de operaciones: No existen controles para verificar el cumplimiento de los protocolos establecidos. Una revisión interna encontró que el 70% de las transacciones financieras en SAP carecen de validación secundaria, aumentando el riesgo de fraude o errores.

2. Procesos

Los procesos operativos críticos, como la gestión de relaciones con clientes y las operaciones financieras, carecen de medidas de seguridad

integradas, exponiendo datos sensibles a riesgos. La ausencia de protocolos robustos en estos procesos contribuye directamente a las vulnerabilidades identificadas en los sistemas de la empresa.

- Causa principal: Procesos críticos sin medidas de seguridad.

- CRM sin protocolo de protección: El sistema CRM almacena datos sensibles de clientes (RUT, detalles bancarios) sin cifrado ni controles de acceso. Una auditoría interna de 2024 reveló que el 90% de los registros de clientes son accesibles sin autenticación.

- SAP sin autenticación: El sistema ERP permite autenticación de factor único, con un 60% de los usuarios compartiendo credenciales, según encuestas internas, aumentando el riesgo de accesos no autorizados.

- RH sin control de acceso: Los datos de recursos humanos, incluidas informaciones personales de empleados son accesibles sin restricciones basadas en roles. Los registros del sistema muestran que el 50% de los accesos al sistema de RH no están monitoreados.

3. Personas

Los factores humanos, como la falta de capacitación y conciencia en seguridad, contribuyen significativamente a los riesgos de seguridad. El manejo de datos sensibles por parte de los empleados sin protocolos o herramientas adecuadas amplifica las vulnerabilidades en todos los procesos.

- Causa principal: Factores humanos sin controles adecuados.

- Empleados sin doble autenticación: Solo el 10% de los empleados utiliza autenticación multifactor (MFA), según registros de TI, lo que facilita accesos ilegítimos si las contraseñas son comprometidas.

- Mal manejo de datos sensibles: Los empleados comparten o almacenan datos sin seguir normas seguras, con un 65% admitiendo en encuestas internas que desconocen las mejores prácticas de seguridad.

4. Comunicaciones

Los canales de comunicación utilizados para intercambiar información sensible, como correos electrónicos y WhatsApp, carecen de medidas de protección, lo que los hace vulnerables a interceptaciones y ataques como phishing o "man-in-the-middle".

- Causa principal: Canales de comunicación sin medidas de protección.

- Correos y WhatsApp sin cifrado: El 100% de las cotizaciones y facturas enviadas por correo o WhatsApp carecen de cifrado, según auditorías internas.

- Intercambio inseguro: Los datos sensibles compartidos con proveedores o clientes no utilizan redes seguras (como VPN), aumentando el riesgo de interceptación.

5. Infraestructura

La infraestructura tecnológica de la empresa, incluyendo servidores y dispositivos, no recibe mantenimiento regular ni cuenta con medidas de seguridad adecuadas, lo que la expone a amenazas externas e internas.

- Causa principal: Entorno tecnológico mal gestionado.

- Respaldos inseguros: Los respaldos diarios no están cifrados, y el 80% carecen de protección física o lógica, según auditorías de TI.

- Hardware sin revisiones de seguridad: Los dispositivos no son revisados regularmente, con un 70% sin parches de seguridad actualizados.

6. Tecnología

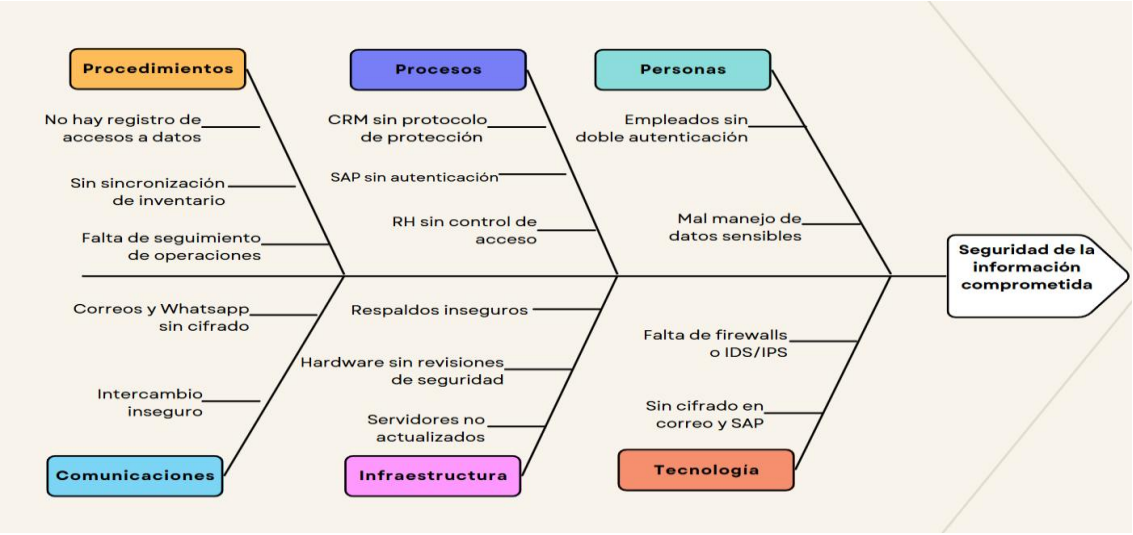
La falta de herramientas de seguridad avanzadas, como firewalls o sistemas de detección de intrusos, deja a la empresa vulnerable a ciberataques externos y compromete la confidencialidad e integridad de los datos.

- Causa principal: Falta de herramientas y configuraciones seguras.

- Falta de firewalls o IDS/IPS: La red no cuenta con sistemas de protección perimetral, con un 100% de exposición a amenazas externas, según análisis de red.

- Sin cifrado en correo y SAP: La información en tránsito y en los sistemas ERP no está protegida, según auditorías de 2024.

Ilustración 11: diagrama de ISHIKAWA de los problemas encontrados en los procesos



Fuente: realizado por el estudiante en CANVA

Tabla 3: matriz de Causas y Efectos

Problema Principal	Causas Identificadas	Efectos Observados
Falta de protección de datos en CRM y SAP	No existe política de cifrado, ni doble autenticación	Exposición de datos sensibles de clientes y empleados
Sin registro de accesos a sistemas	Sistemas no configurados para auditar actividades	Pérdida de trazabilidad ante incidentes de seguridad
Respaldos inseguros	No hay control ni protección en respaldos locales y en nube	Riesgo de pérdida o robo de datos críticos
Infraestructura desactualizada	No se ejecutan mantenimientos ni se actualizan sistemas	Vulnerabilidad frente a ciberataques externos
Comunicación insegura con proveedores y clientes	Uso de medios no seguros como correo y WhatsApp sin cifrado	Fugas de información en tránsito

Fuente: Elaboración propia, con información de la empresa y del decente.

Cierre del análisis de Ishikawa

Como resultado del análisis de Ishikawa, se ha podido identificar que la seguridad de la información comprometida en la organización no es producto de una única causa, sino de la convergencia de múltiples factores distribuidos en distintas áreas críticas. Entre las causas más relevantes se destacan: la falta de protocolos claros en los procesos operativos, la ausencia de mecanismos de autenticación y control de accesos, comunicaciones sin cifrado, infraestructura tecnológica sin mantenimiento de seguridad regular y un manejo inadecuado de datos sensibles por parte del personal. Estas debilidades evidencian una falta de integración entre los sistemas tecnológicos y los controles de seguridad de la información, lo cual pone en riesgo la confidencialidad, integridad y disponibilidad de los datos.

Este análisis no solo permite visualizar de forma estructurada los orígenes del problema, sino que sienta las bases para la aplicación de acciones correctivas dentro del marco de un Sistema de Gestión de Seguridad de la Información conforme a la norma ISO/IEC 27001, promoviendo así una cultura organizacional orientada a la mejora continua en la protección de la información.

3.7 Análisis

La etapa de clasificación de riesgos y criticidad constituye una parte fundamental en la implementación de un Sistema de Gestión de Seguridad de la

Información basado en la norma ISO/IEC 27001:2022. Esta etapa permite evaluar los riesgos detectados durante el análisis previo, asignando niveles de probabilidad e impacto, con el fin de categorizar su criticidad y establecer una base sólida para la selección de controles y medidas de mitigación adecuadas. La correcta aplicación de esta metodología permite priorizar la atención sobre los activos y procesos más expuestos, optimizando los recursos y asegurando la protección efectiva de la información.

- La probabilidad se refiere a la posibilidad de que un riesgo identificado se materialice. Para su evaluación, se establecen cinco niveles, desde muy bajo hasta muy alto:

Tabla 4: Criterios de Evaluación de la Probabilidad

Nivel	Descripción	Valor
Muy Bajo	Es poco probable que ocurra, puede suceder en circunstancias excepcionales.	1
Bajo	Existe una pequeña posibilidad de que ocurra, pero es poco frecuente.	2
Medio	Es posible que ocurra en alguna ocasión.	3
Alto	Es probable que ocurra en varias ocasiones.	4
Muy Alto	Tiene una alta probabilidad de ocurrencia y se espera con frecuencia.	5

Fuente: Elaboración propia, con información de la empresa y del decente.

3.7.1 El impacto corresponde a las consecuencias que tendría la materialización

de un riesgo en los activos o procesos. Se establecen también cinco niveles.

Tabla 5: Criterios de Evaluación del Impacto

Nivel	Descripción	Valor
Muy Bajo	El impacto es casi insignificante, no afecta significativamente al negocio.	1
Bajo	Impacto leve, con efectos menores y controlables.	2
Medio	Afecta de manera moderada el funcionamiento del proceso.	3
Alto	Tiene un efecto grave sobre el proceso o servicio.	4
Muy Alto	Impacto crítico que compromete gravemente la operación o reputación.	5

Fuente: Elaboración propia, con información de la empresa y del decente.

3.7.2 La matriz de riesgos permite combinar los valores de probabilidad e impacto para obtener el nivel de riesgo. Este se calcula como el producto entre ambos factores.

Tabla 6: Matriz de Evaluación de Riesgos

Impacto / Probabilidad	1(Muy Bajo)	2 (Bajo)	3 (Medio)	4 (Alto)	5(Muy Alto)
5 muy Alto	5	10	15	20	25
4 alto	4	8	12	16	20
3 medio	3	6	9	12	15
2 bajo	2	4	6	8	10
1 muy Bajo	1	2	3	4	5

Fuente: Elaboración propia, con información de la empresa y del decente.

3.7.3 Con base en los valores obtenidos en la matriz de riesgo, se establecen las

categorías mencionadas a continuación.

Tabla 7: Categorización de la Magnitud del Riesgo

Rango de Valor	Categoría del Riesgo	Color	Acción Recomendada
1 - 5	Bajo	Verde	Controlar y monitorear
6 - 10	Medio	Amarillo	Evaluar y tomar medidas de mitigación si es necesario
11 - 15	Alto	Naranja	Plan de acción correctiva inmediata
16 - 25	Crítico	Rojo	Mitigación urgente y prioritaria

Fuente: Elaboración propia, con información de la empresa y del decente.

3.7.4 Resumen de riesgos identificados

Para una adecuada gestión del proyecto, se identificaron y seleccionaron diez riesgos relevantes que podrían comprometer la calidad, seguridad, continuidad operativa o cumplimiento normativo de los procesos involucrados. Estos riesgos se analizarán en detalle mediante una matriz de criticidad, ya que representan amenazas significativas en distintas áreas clave de la organización. A continuación, se detallan los riesgos seleccionados y su justificación:

1) **Pérdida de datos personales de clientes:** Este riesgo se considera crítico por su impacto en la confidencialidad de la información y en el cumplimiento de normativas de protección de datos.

2) **Envío de cotizaciones sin cifrado:** Se analiza porque compromete la privacidad de información sensible y podría afectar la imagen de la empresa frente a sus clientes.

3) **Sincronización insegura entre sucursales:** Representa un riesgo importante para la integridad del inventario y puede provocar errores en la operación logística.

4) **Envío de órdenes de compra sin cifrado:** Aunque tiene menor impacto, su análisis es necesario ya que afecta la seguridad de procesos comerciales estratégicos.

5) **Registro no trazable de operaciones:** Este riesgo afecta directamente la transparencia y confiabilidad del sistema financiero de la organización.

6) **Accesos inseguros a plataformas bancarias:** Se considera de alta prioridad debido a su potencial impacto en la seguridad financiera de la empresa.

7) **Protección deficiente de currículums:** Si bien su impacto es medio, implica la exposición de datos personales de postulantes, lo que también tiene implicancias legales.

8) **Acceso no autorizado a datos personales:** Este riesgo es crítico, ya que compromete directamente la seguridad de la información sensible del personal.

9) **Respaldo sin medidas de seguridad:** Se incluye porque una falla en los respaldos puede provocar pérdidas de información valiosa y afectar la continuidad operativa.

10) **Falta de firewalls o IDS/IPS:** Su análisis es indispensable debido a la exposición que genera frente a amenazas externas, como ciberataques o intrusiones.

3.7.5 Evaluación de la Criticidad de los Riesgos

Para evaluar los riesgos asociados a los procesos identificados como críticos dentro de la Empresa de Venta de Neumáticos, se aplicó la metodología descrita anteriormente. A continuación, se presenta la matriz de criticidad con los valores de probabilidad, impacto, nivel de riesgo y su categoría.

Tabla 8: Matriz de Criticidad de Riesgos

N°	Proceso	Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Categoría
1	Atención al Cliente	Pérdida de datos personales de clientes	4 (Alto)	5 (Muy Alto)	20	Crítico
2	Atención al Cliente	Envío de cotizaciones sin cifrado	3 (Medio)	4 (Alto)	12	Alto
3	Gestión de Inventario	Sincronización insegura entre sucursales	4 (Alto)	4 (Alto)	16	Crítico
4	Gestión de Inventario	Envío de órdenes de compra sin cifrado	3 (Medio)	3 (Medio)	9	Medio
5	Gestión Financiera	Registro no trazable de operaciones	3 (Medio)	5 (Muy Alto)	15	Alto
6	Gestión Financiera	Accesos inseguros a plataformas bancarias	4 (Alto)	5 (Muy Alto)	20	Crítico
7	Recursos Humanos	Protección deficiente de currículums	3 (Medio)	3 (Medio)	9	Medio
8	Recursos Humanos	Acceso no autorizado a datos personales	4 (Alto)	4 (Alto)	16	Crítico
9	Tecnología y Soporte	Respaldo sin medidas de seguridad	3 (Medio)	4 (Alto)	12	Alto
10	Tecnología y Soporte	Falta de firewalls o IDS/IPS	4 (Alto)	5 (Muy Alto)	20	Crítico

Fuente: Elaboración propia, con información de la empresa y del decente.

Cierre:

A través de la aplicación de estas cinco tablas clave se logró establecer un mapa claro de riesgos clasificados según su probabilidad e impacto. Esta metodología permite a la organización priorizar sus esfuerzos en función de la magnitud del riesgo, concentrándose principalmente en aquellos identificados como "críticos" y "altos", para los cuales se desarrollarán medidas de mitigación específicas en la siguiente sección del capítulo. Este análisis es fundamental para la toma de decisiones informadas y para fortalecer el enfoque proactivo de seguridad de la información en la empresa.

CAPÍTULO 4: Propuesta de mejora

Este capítulo presenta una propuesta de mejora enfocada en los procesos identificados como **más críticos (nivel 20)** en la matriz de criticidad de riesgos (Tabla 7). Se aborda cada uno mediante la metodología de mejora continua **Ciclo de Deming (PDCA)**, considerando su impacto en la seguridad de la información conforme a ISO/IEC 27001.

4.1 Identificación de Procesos

Los procesos seleccionados para la mejora corresponden a los tres que presentan **nivel de riesgo 20 (Crítico)**:

1) **Proceso de Atención al Cliente**: Riesgo de pérdida de datos personales.
2) **Proceso de Gestión Financiera**: Riesgo por accesos inseguros a plataformas bancarias.
3) **Proceso de Tecnología y Soporte**: Riesgo por falta de firewalls o sistemas IDS/IPS.

Estos procesos fueron definidos en el apartado 3.2 y se caracterizan por manejar información sensible o por desempeñar un rol esencial en la protección de los activos digitales de la empresa.

4.2 Ciclo de Deming

Se aplicará el modelo PDCA para guiar la mejora continua en cada proceso crítico.

4.2.1 Plan (Planificar)

El plan se redefine para cumplir con los objetivos específicos establecidos en el Capítulo 2, asegurando que cada tarea contribuya directamente a la implementación del sistema de gestión de seguridad de la información.

Tareas del Plan:

- ✓ Definir el equipo de trabajo: Establecer un equipo multidisciplinario con roles claros para la implementación del Sistema de Gestión de Seguridad de la Información.
- ✓ Diagnóstico técnico inicial: Realizar un análisis exhaustivo de los procesos y sistemas actuales para identificar vulnerabilidades específicas.
- ✓ Identificación de herramientas tecnológicas viables: Evaluar y seleccionar tecnologías accesibles y de bajo costo para mitigar los riesgos identificados.
- ✓ Análisis de riesgos de seguridad: Realizar un análisis detallado de los riesgos de seguridad de la información para priorizar medidas preventivas.
- ✓ Evaluación de normativas y estándares: Revisar las normativas aplicables (ISO/IEC 27001, Ley 19.496) para garantizar el cumplimiento.
- ✓ Modelado de un plan de respuesta a incidentes: Diseñar un plan

estructurado para responder a incidentes de seguridad, minimizando impactos.

Tabla 9: Carta Gantt del Plan de Mejora

Actividad / Semana	Sem 1	Sem 2	Sem 3	Sem 4	Sem 5	Sem 6	Responsable
Definir el equipo de trabajo							Jefe de Proyecto
Diagnóstico técnico inicial							Equipo Técnico
Identificación de herramientas tecnológicas							Equipo Técnico
Análisis de riesgos de seguridad							Analista de Seguridad
Evaluación de normativas y estándares							Consultor ISO 27001
Modelado de plan de respuesta a incidentes							Jefe de Proyecto

Fuente: Elaboración propia.

4.2.2 DO (Hacer)

Esta sección detalla la ejecución de cada tarea del plan, proporcionando una descripción exhaustiva de las actividades a realizar, como se solicitó.

4.2.2.1 Definir el Equipo de Trabajo

Se conformará un equipo multidisciplinario con experiencia en ciberseguridad, atención al cliente, gestión financiera y tecnología para la implementación del Sistema de Gestión de Seguridad de la Información. Los

roles, perfiles, horas asignadas y responsabilidades se detallan en la siguiente tabla para garantizar claridad en la asignación de tareas.

Tabla 10: Composición del equipo de trabajo

Rol	Perfil	Horas Asignadas	Responsabilidades Principales
Jefe de Proyecto	Ingeniero en Ciberseguridad, certificado ISO/IEC 27001 Lead Implementer, 5 años de experiencia	80 HH	Coordinar el proyecto, asignar tareas, supervisar el cumplimiento del cronograma y elaborar reportes.
Analista de Procesos de Atención al Cliente	Experto en CRM y protección de datos, con experiencia en diseño de protocolos de seguridad	40 HH	Analizar procesos de atención al cliente, implementar controles en el CRM y capacitar al personal.
Especialista en Seguridad Financiera	Conocimiento avanzado en ciberseguridad bancaria, herramientas MFA y plataformas electrónicas	40 HH	Configurar MFA en SAP y plataformas bancarias, auditar accesos financieros y gestionar alertas.
Administrador de Infraestructura TI	Experiencia en despliegue de firewalls, IDS/IPS (e.g., Snort, Suricata) y segmentación de redes	50 HH	Instalar y configurar firewalls e IDS/IPS, mantener la infraestructura tecnológica y realizar pruebas.

Fuente: Elaboración propia.

Nota: Total horas estimadas: 210 HH. Valor por hora-hombre: $18.000 CLP (verificado en Laborum.cl).

Actividades:

1) Convocar a los candidatos internos y externos.
2) Realizar una sesión de planificación para asignar roles y responsabilidades.
3) Documentar el plan de trabajo del equipo en un sistema de gestión de proyectos.
4) Establecer canales de comunicación (correo corporativo, reuniones semanales).

Total horas estimadas: 210 HH. Valor HH: $18.000 CLP (verificado en Laborum.cl).

4.2.2.2 Diagnóstico Técnico Inicial

Se realizará un análisis exhaustivo de los procesos críticos (atención al cliente, gestión de inventario, gestión financiera, recursos humanos, tecnología y soporte) para identificar vulnerabilidades específicas en la seguridad de la información. Este diagnóstico incluirá:

- Auditoría de sistemas: Revisión de configuraciones del CRM, SAP, servidores y redes para identificar puntos débiles (e.g., falta de cifrado, accesos no autenticados). Se utilizará software de escaneo como Nessus para detectar vulnerabilidades.
- Entrevistas con empleados: Recopilar información sobre prácticas actuales de manejo de datos, con un enfoque en el 65% de

empleados no capacitados (según encuestas internas).

- Análisis de incidentes pasados: Revisión de las tres brechas de datos reportadas en 2024 para identificar patrones y causas raíz.
- Mapeo de activos de información: Identificación de datos sensibles (RUT de clientes, registros financieros etc.) y su ubicación en los sistemas.

Actividades:

1) Configurar herramientas de auditoría (Nessus, Wireshark) para escanear la red.
2) Realizar entrevistas estructuradas con al menos 20 empleados clave.
3) Documentar hallazgos en un informe preliminar.
4) Clasificar activos de información según su criticidad (alta, media, baja).

4.2.2.3 Identificación de Herramientas Tecnológicas Viables

Descripción: Se evaluarán y seleccionarán tecnologías accesibles y de bajo costo para mitigar los riesgos identificados, priorizando soluciones escalables para una pyme. Se considerarán herramientas que cumplan con ISO/IEC 27001 y sean compatibles con la infraestructura existente (SAP, CRM).

Herramientas evaluadas:

- Firewalls: Fortinet FortiGate 40F (costo aproximado: $1.240.000 CLP).
- IDS/IPS: Suricata (open source, con soporte limitado).
- MFA: YubiKey (dispositivos físicos) y Auth0 (plataforma de gestión).
- Cifrado: Certificados SSL/TLS para correo y CRM.
- SIEM: Wazuh (open source, para monitoreo de eventos).

- Criterios de selección: Costo, compatibilidad, facilidad de implementación, cumplimiento normativo.

Actividades:

1) Investigar proveedores locales y comparar cotizaciones.
2) Realizar pruebas de compatibilidad con sistemas existentes (SAP, CRM).
3) Elaborar un informe comparativo de herramientas, destacando costos y beneficios.
4) Seleccionar las herramientas finales en conjunto con el equipo técnico.

4.2.2.4 Análisis de Riesgos de Seguridad

Descripción: Se realizará un análisis detallado de los riesgos de seguridad identificados en el diagnóstico, utilizando la metodología de la matriz de riesgos (probabilidad e impacto). Esto permitirá priorizar medidas preventivas para los

riesgos críticos (nivel 20 en la Tabla 7).

- Metodología: Basada en ISO/IEC 27001, se clasificarán los riesgos según probabilidad (muy bajo a muy alto) e impacto (muy bajo a muy alto).
- Riesgos clave: Pérdida de datos de clientes, accesos inseguros a plataformas bancarias, falta de firewalls/IDS.

Actividades:

1) Actualizar la matriz de riesgos con los hallazgos del diagnóstico.
2) Priorizar los riesgos críticos (e.g., pérdida de datos personales, nivel 20).
3) Proponer medidas preventivas específicas (e.g., cifrado, MFA).
4) Documentar el análisis en un informe detallado.

4. 2.2.5 Evaluación de Normativas y Estándares

Descripción: Se revisarán las normativas aplicables, principalmente ISO/IEC 27001 y la Ley 19.496, para garantizar que el Sistema de Gestión de Seguridad de la Información cumpla con los requisitos legales y regulatorios. Se contratará una consultoría externa para validar el cumplimiento.

Normativas evaluadas:

- ISO/IEC 27001: Requisitos para un Sistema de Gestión de Seguridad de la Información.

- Ley 19.496: Protección de datos personales en Chile.

- Alcance: Identificar brechas en el cumplimiento actual y proponer ajustes.

Actividades:

1) Revisar la documentación de normativas con el consultor ISO 27001.
2) Comparar los procesos actuales con los requisitos de las normativas.
3) Elaborar un informe de brechas normativas.
4) Proponer un plan de acción para cerrar las brechas identificadas.

4.2.2.6 Modelado de un Plan de Respuesta a Incidentes

Descripción: Se diseñará un plan estructurado para responder a incidentes de seguridad, minimizando el impacto en la operación y protegiendo los activos digitales. El plan seguirá las mejores prácticas de ISO/IEC 27001.

Componentes del plan:

- ✓ Identificación de incidentes: Detección mediante SIEM y alertas.
- ✓ Respuesta: Protocolos para contención y mitigación.
- ✓ Recuperación: Restauración de sistemas y datos.
- ✓ Lecciones aprendidas: Análisis post-incidente.

Actividades:

1) Diseñar un procedimiento de respuesta a incidentes.
2) Simular un incidente (ej, brecha de datos) para validar el plan.
3) Capacitar al equipo técnico en la ejecución del plan.
4) Documentar el plan en un manual accesible para todos los empleados clave.

4.2.3 Check (Verificar)

Esta fase evalúa la eficacia de las acciones ejecutadas mediante indicadores clave de desempeño (KPI), organizados de manera clara y estructurada. Los indicadores de control están diseñados para medir la efectividad de las medidas propuestas, garantizar el cumplimiento de normativas (ISO/IEC 27001 y Ley 19.496), proteger los datos sensibles y reducir los incidentes de seguridad en un 80% en seis semanas, según lo establecido en el documento. Cada indicador se alinea con los objetivos específicos y aborda los riesgos críticos identificados.1.

KPI - Protección de Datos en el Proceso de Atención al Cliente

- **Descripción:** Porcentaje de interacciones con clientes registradas en el sistema CRM de forma segura, utilizando autenticación multifactor (MFA) y cifrado TLS para proteger datos sensibles como RUT, datos bancarios y

preferencias de compra.

- **Justificación:** Este indicador mide la efectividad de las medidas de seguridad implementadas en el CRM para mitigar el riesgo crítico de pérdida de datos personales (nivel 20, Tabla 8). Garantiza el cumplimiento de la Ley 19.496 y fortalece la confianza del cliente, reduciendo el impacto de las tres brechas de datos reportadas en 2024.

Fórmula:

$$\text{Porcentaje de interacciones seguras} = \left(\frac{\text{Interacciones seguras registradas en el CRM}}{\text{Total de interacciones}} \right) \times 100$$

Ejemplo: Si en una semana se registran 1,000 interacciones con clientes y 950 están protegidas con MFA y cifrado TLS, el cálculo es:

$$\left(\frac{950}{1,000} \right) \times 100 = 95\%$$

Criterio de Aceptación: ≥ 95% de las interacciones deben ser seguras.

Justificación del Criterio: Basado en estándares internacionales de protección de datos (ISO/IEC 27001), un umbral del 95% asegura una cobertura robusta, minimizando riesgos de accesos no autorizados.

2. KPI - Accesos Seguros al Módulo Financiero

- **Descripción:** Porcentaje de accesos al módulo financiero de SAP que utilizan autenticación multifactor (MFA) para garantizar la seguridad de las

transacciones financieras y registros contables.

- **Justificación:** Aborda el riesgo crítico de accesos inseguros a plataformas bancarias (nivel 20, Tabla 8), protegiendo datos financieros sensibles y asegurando el cumplimiento normativo. La auditoría interna de 2024 indicó que el 70% de las transacciones carecen de validación secundaria, por lo que este indicador valida la implementación de MFA.

Fórmula:

$$\text{Porcentaje de accesos seguros} = \left(\frac{\text{Accesos con MFA}}{\text{Total de accesos al módulo financiero}} \right) \times 100$$

Ejemplo: Si en una semana se registran 120 accesos al módulo financiero y todos utilizan MFA, el cálculo es:

$$\left(\frac{120}{120} \right) \times 100 = 100\%$$

Criterio de Aceptación: 100% de los accesos deben usar MFA.

Justificación del Criterio: ISO/IEC 27001 exige controles estrictos para sistemas financieros críticos, y un 100% asegura la eliminación de accesos no autorizados.

3. KPI - Detección y Bloqueo de Amenazas Externas

- **Descripción:** Porcentaje de intentos de intrusión detectados y bloqueados por el firewall UTM y el sistema IDS/IPS en la infraestructura tecnológica de la empresa.

- **Justificación:** Evalúa la efectividad de las herramientas de seguridad perimetral implementadas para mitigar el riesgo crítico de falta de firewalls o IDS/IPS (nivel 20, Tabla 8). La red actual está 100% expuesta a amenazas externas, según auditorías de 2024, por lo que este indicador mide la capacidad de defensa contra ciberataques.

Fórmula:

$$\text{Porcentaje de amenazas bloqueadas} = \left(\frac{\text{Eventos de intrusión bloqueados}}{\text{Total de eventos detectados}}\right) \times 100$$

Ejemplo: Si el sistema detecta 2,500 eventos de intrusión en una semana y bloquea 2,420, el cálculo es:

$$\left(\frac{2,420}{2,500}\right) \times 100 = 96.8\%$$

Criterio de Aceptación: ≥ 95% de los eventos deben ser bloqueados.

Justificación del Criterio: Basado en benchmarks técnicos para sistemas IDS/IPS, un 95% asegura una protección robusta frente a amenazas externas como ransomware o phishing.

4. KPI - Identificación de Activos Críticos

- **Descripción:** Porcentaje de activos tangibles e intangibles de información (e.g., datos de clientes, registros financieros, inventarios) identificados y clasificados según su criticidad en un plazo de dos semanas.
- **Justificación:** Responde al objetivo específico de realizar un levantamiento de activos (Capítulo 2). La identificación completa de

activos es fundamental para priorizar su protección y cumplir con ISO/IEC 27001, abordando las vulnerabilidades derivadas de las brechas de datos de 2024.

Fórmula:

$$\text{Porcentaje de activos identificados} = \left(\frac{\text{Activos identificados y clasificados}}{\text{Total de activos estimados}} \right) \times 100$$

Ejemplo: Si se estiman 200 activos de información (bases de datos, documentos, sistemas) y se identifican 190 en el diagnóstico, el cálculo es:

$$\left(\frac{190}{200} \right) \times 100 = 95\%$$

Criterio de Aceptación: 100% de los activos críticos deben ser identificados y clasificados.

Justificación del Criterio: La norma ISO/IEC 27001 requiere un inventario completo de activos para garantizar una gestión efectiva de riesgos.

5. KPI - Reducción de Riesgos Críticos

- **Descripción:** Número de riesgos críticos (nivel 16-20, Tabla 8) mitigados mediante la implementación de controles específicos en un plazo de tres semanas.
- **Justificación:** Evalúa el objetivo específico de analizar riesgos de seguridad para establecer medidas preventivas (Capítulo 2). La matriz de criticidad identificó cinco riesgos críticos (pérdida de datos, accesos

inseguros, etc.), y este indicador mide el progreso en su mitigación.

Fórmula:

Número de riesgos mitigados = Conteo de riesgos críticos con controles implementados.

Ejemplo: Si de los cinco riesgos críticos identificados (pérdida de datos, sincronización insegura, accesos bancarios, acceso no autorizado a datos de RH, falta de firewalls), cuatro tienen controles implementados (ej., MFA, firewalls, cifrado), el resultado es 4 riesgos mitigados.

Criterio de Aceptación: Al menos 5 riesgos críticos mitigados.

Justificación del Criterio: La meta establecida en el objetivo específico es mitigar al menos cinco riesgos críticos en tres semanas, asegurando una reducción significativa de vulnerabilidades.

6. KPI - Cumplimiento Normativo

- **Descripción:** Porcentaje de brechas normativas (ISO/IEC 27001 y Ley 19.496) identificadas y corregidas en un plazo de cuatro semanas.
- **Justificación:** Responde al objetivo específico de evaluar normativas para garantizar el cumplimiento legal (Capítulo 2). La empresa enfrenta un alto riesgo de sanciones por incumplimiento de la Ley 19.496, y este indicador valida el cierre de brechas normativas.

Fórmula:

$$\text{Porcentaje de brechas corregidas} = \left(\frac{\text{Brechas normativas corregidas}}{\text{Total de brechas identificadas}}\right) \times 100$$

Ejemplo: Si se identifican 10 brechas normativas (e.g., falta de cifrado, ausencia de registros de acceso) y se corrigen 9, el cálculo es:

$$\left(\frac{9}{10}\right) \times 100 = 90\%$$

Criterio de Aceptación: 100% de las brechas normativas corregidas.

Justificación del Criterio: El cumplimiento total es necesario para evitar sanciones legales y avanzar hacia una certificación ISO/IEC 27001.

7. KPI - Tiempo de Respuesta a Incidentes

- **Descripción:** Tiempo promedio (en minutos) para detectar, contener y responder a incidentes de seguridad simulados, según el plan de respuesta a incidentes diseñado.
- **Justificación:** Evalúa el objetivo específico de modelar un plan de respuesta a incidentes (Capítulo 2). Un tiempo de respuesta rápido minimiza el impacto de brechas como las ocurridas en 2024, que afectaron a 150 clientes.

Fórmula:

$$\text{Tiempo promedio de respuesta} = \frac{\text{Suma de tiempos de respuesta a incidentes simulados}}{\text{Número de simulaciones}}$$

Ejemplo: Si se realizan 5 simulaciones con tiempos de respuesta de 45, 50, 55, 40 y 60 minutos, el cálculo es:

$$\frac{45 + 50 + 55 + 40 + 60}{5} = 50 \text{ minutos}$$

Criterio de Aceptación: Tiempo promedio ≤ 60 minutos.

Justificación del Criterio: Basado en el estándar NIST CSF 2.0, un tiempo de respuesta menor a una hora es adecuado para pymes, minimizando el impacto operativo.

8. KPI - Relación Costo-Beneficio

- **Descripción:** Relación entre los beneficios económicos proyectados y el costo total de la implementación del Sistema de Gestión de Seguridad de la Información en un plazo de seis semanas.
- **Justificación:** Responde al objetivo específico de evaluar los costos asociados al Sistema de Gestión de Seguridad de la Información (Capítulo 2). La relación costo-beneficio de 19,2:1 proyectada en el documento valida la viabilidad económica de la propuesta.

Fórmula:

$$\text{Relación costo-beneficio} = \frac{\text{Beneficios económicos proyectados}}{\text{Costo total del proyecto}}$$

Ejemplo: Con beneficios proyectados de $212,365,432 CLP en cinco años y un costo de $11,040,281 CLP, el cálculo es:

$$\frac{212,365,432}{11,040,281} \approx 19.23$$

Criterio de Aceptación: Relación ≥ 19:1.

Justificación del Criterio: La meta establecida en el documento asegura que la inversión sea rentable, con beneficios económicos superiores a $40 millones anuales.

- **Frecuencia de Monitoreo y Responsables**

Frecuencia: Los KPI se monitorearán semanalmente durante las seis semanas de implementación inicial, con auditorías trimestrales posteriores para garantizar la mejora continua (fase Act).

- **Responsables:**

- ✓ Jefe de Proyecto: Supervisa la recolección de datos y el análisis de KPI.
- ✓ Analista de CRM: Monitorea el KPI de protección de datos en el proceso de atención al cliente.
- ✓ Especialista en Seguridad Financiera: Supervisa el KPI de accesos seguros al módulo financiero.
- ✓ Administrador de Infraestructura TI: Monitorea el KPI de detección de amenazas externas y el tiempo de respuesta a incidentes.
- ✓ Consultor ISO 27001: Valida el KPI de cumplimiento normativo.

- ✓ Equipo Técnico: Recopila datos para los KPI de identificación de activos y reducción de riesgos.

4.2.4 ACT (Actuar)

En esta fase, se toman medidas basadas en los resultados de la fase de verificación (Check) para garantizar la mejora continua del Sistema de Gestión de Seguridad de la Información. A continuación, se detalla el proceso:

Si los KPI son alcanzados:

- **Escalamiento:** Las medidas implementadas en los procesos críticos (atención al cliente, gestión financiera, tecnología y soporte) se extenderán a otros procesos de la empresa, como gestión de inventario y recursos humanos. Por ejemplo, el cifrado TLS se aplicará a todas las comunicaciones externas.
- **Consolidación:** Las políticas de seguridad (ej, MFA, auditorías de acceso) se integrarán formalmente en el Sistema de Gestión de Seguridad de la Información, con manuales actualizados y distribuidos al personal.
- **Capacitación continua**: Se programarán sesiones anuales de formación para mantener al personal actualizado en prácticas de seguridad, reduciendo el 65% de empleados no capacitados.
- **Auditorías periódicas:** Se establecerá un calendario de auditorías trimestrales para verificar el cumplimiento continuo con ISO/IEC

27001.

Si los KPI no son alcanzados:

- **Análisis de brechas:** Se revisarán los datos de los KPI para identificar fallos específicos (ej., configuraciones incorrectas de firewalls, baja adopción de MFA). Por ejemplo, si el KPI de protección de datos en CRM es <95%, se analizarán los registros de acceso para detectar puntos débiles.
- **Ajustes técnicos:** Se reconfigurarán las herramientas (e.g., actualizar firmas de IDS/IPS) o se buscarán alternativas más robustas (ej., cambiar de Suricata a un IDS comercial si es necesario).
- **Revisión de procesos:** Se ajustarán los procedimientos, como reforzar la capacitación en el uso de MFA si el KPI de accesos seguros no alcanza el 100%.
- **Plan de acción correctiva:** Se elaborará un plan con plazos definidos (ej., dos semanas) para implementar los ajustes, asignando responsables específicos.

Mejora continua:

El Ciclo de Deming se repetirá anualmente, con revisiones de los KPI, actualización de riesgos y ajustes al Sistema de Gestión de Seguridad de la Información para adaptarse a nuevas amenazas o normativas.

4.3 Infraestructura

A continuación, se identifican los hardware y software relacionados con los procesos identificados.

- **Hardware**
  - 1 Firewall UTM básico (protección perimetral)
  - 1 Servidor IDS/IPS (detección de intrusos)
  - 10 dispositivos físicos MFA (para accesos privilegiados)

- **Software**
  - SIEM de código abierto (registro y correlación de eventos)
  - Certificados TLS/SSL (cifrado de comunicaciones web)
  - Plataforma MFA compatible con sistemas internos

Capítulo 5 – Análisis Económico.

Este capítulo evalúa la factibilidad económica de la propuesta de mejora en seguridad de la información. Se analizan los costos asociados, beneficios esperados y la rentabilidad proyectada para Empresa de Venta de Neumáticos, en base a cifras realistas y adaptadas a su tamaño como pyme chilena.

5.1 Costos de la Propuesta

El análisis se presenta en **UF** (Unidad de Fomento), con un valor referencial de **$37.200 CLP**, y sus conversiones a **pesos chilenos (CLP)**. El presupuesto fue optimizado en un 50% respecto a la versión original, manteniendo los controles críticos y reduciendo sobredimensionamientos.

5.1.1 Costos de Infraestructura

La siguiente tabla presenta los costos estimados de los elementos de infraestructura tecnológica necesarios para la implementación del proyecto. Se incluyen cantidades, valores en Uf y pesos chilenos.

Tabla 11: costos de infraestructura

Ítem	Cantidad	Costo Unitario (UF)	Total UF	Total CLP
Firewall UTM físico básico	1	33,34	33,34	$1.240.000
Servidor IDS/IPS	1	24,00	24,00	$892.800
Dispositivos físicos MFA	10	1,60	16,00	$595.200
Plataforma MFA (licencia)	1	8,00	8,00	$297.600
SIEM de código abierto	1	13,34	13,34	$496.128
Certificados SSL/TLS	2	2,67	5,34	$198.528
Total Infraestructura	–	–	**100,02**	**$3.720.256**

Fuente: Elaboración propia

Nota: La selección de 1 firewall, 1 servidor IDS y 10 dispositivos MFA responde a la estructura actual de red, número de usuarios críticos y escalabilidad inmediata

5.1.2 Costos de Capital Humano

Se consideran recursos humanos internos y consultoría externa para planificación, ejecución y revisión del proyecto. El valor promedio de **HH (hora-hombre)** es de **$18.000 CLP**, ajustado a valores actuales de mercado para pymes (fuente: Laborum.cl).

Tabla 12 costos de capital humano

Cargo	Cantidad	HH por persona	Valor HH	Total CLP
Jefe de Proyecto	1	80	$18.000	$1.440.000
Analista de CRM	1	40	$18.000	$720.000
Especialista Financiero (SAP)	1	40	$18.000	$720.000
Administrador de Infraestructura	1	50	$18.000	$900.000
Total Capital Humano	–	–	–	**$3.780.000**

Fuente: Elaboración propia

- Se utilizarán 210 horas hombre en total durante las seis semanas de implementación.

5.1.3 Costos Fijos

Se presentan los gastos que no varían con el volumen del proyecto, tales como consultorías externas, auditorías iniciales y costos administrativos. Estos elementos son fundamentales para asegurar una correcta planificación y respaldo técnico durante la implementación.

Tabla 13: costos fijos

Ítem	Cantidad	Total CLP
Consultoría externa ISO 27001	1	$900.000
Auditoría técnica inicial	1	$200.000
Costos administrativos	–	$500.000
Total Costos Fijos	–	**$1.600.000**

Fuente: Elaboración propia

5.1.4 Costos Variables

En este apartado se estiman los costos que pueden fluctuar según el avance del proyecto, como capacitación interna, soporte técnico y una provisión para contingencias. Estos valores permiten mantener una reserva de flexibilidad ante imprevistos sin comprometer la continuidad del proyecto.

Tabla 14: costos variables

Ítem	Cantidad	Total CLP
Capacitación interna del equipo	1	$400.000
Mantenimiento anual (TI)	1	$600.000
Contingencias (10%)	–	$940.025
Total Costos Variables	–	**$1.940.025**

Fuente: Elaboración propia

5.1.5 Costo Total del Proyecto

Se consolida toda la información financiera expuesta en los apartados anteriores, entregando el costo global de la propuesta. Este total permite establecer un punto de comparación con los beneficios esperados, siendo clave para el análisis de rentabilidad.

Tabla 15: costo total del proyecto

Categoría	Total CLP
Infraestructura	$3.720.256
Capital Humano	$3.780.000
Costos Fijos	$1.600.000
Costos Variables	$1.940.025
Total Proyecto	**$11.040.281**

Fuente: Elaboración propia

5.2 Análisis Costo-Beneficio

Esta sección evalúa si la inversión realizada es justificable en términos económicos. Se cuantifican los beneficios esperados, tanto por reducción de pérdidas como por mejoras operacionales y comerciales, proyectando su impacto a cinco años. También se calculan indicadores financieros clave.

5.2.1 Beneficios Económicos

Se identifican y valoran los beneficios monetarios directos derivados del proyecto, como la disminución de incidentes de seguridad, la evitación de sanciones legales y el aumento de ingresos por mayor confianza del cliente. Estos valores son estimados con base en datos internos y tendencias sectoriales.

- **Reducción de incidentes**: De 3 a menos de 1 por año.
  - Ahorro estimado: $5.000.000 × 2 incidentes evitados =

$10.000.000/año

- **Evita sanciones legales y multas**: $10.000.000/año
- **Incremento de ventas (por imagen y confianza)**: 5% sobre ventas anuales estimadas de $400 millones = $20.000.000/año

Beneficio total anual estimado: $40.000.000 CLP Proyección con crecimiento anual del 3% (por inflación y expansión natural del negocio):

Tabla 16: Beneficio económico

Año	Beneficio estimado	Acumulado
1	$40.000.000	$40.000.000
2	$41.200.000	$81.200.000
3	$42.436.000	$123.636.000
4	$43.709.080	$167.345.080
5	$45.020.352	$212.365.432

Fuente: Elaboración propia

5.2.2 Relación Costo-Beneficio y WACC

Aquí se realiza un análisis financiero detallado para determinar la rentabilidad del proyecto. Se calcula la relación costo-beneficio, la ganancia neta y el WACC (costo promedio ponderado del capital), que permite evaluar si el retorno supera el costo de oportunidad del capital invertido.

Relación Costo-Beneficio:

212.365.432 / 11.040.281 ≈ 19,23

❖ Por cada peso invertido, la empresa recibe $19,23 en beneficios.

Ganancia Total Neta:

212.365.432−11.040.281=201.325.151 CLP

Cálculo del WACC

Supuestos:

Ke = Costo del capital propio

Kd = Costo deuda

T = Tasa impositiva

Estructura capital: 70% propio, 30% deuda

- **Ke** = 11,8% (β = 1,3 | Rf = 4% | Rm = 10%)
- **Kd** = 7%
- **T** = 25%

Fórmula:

$$WACC = E/V \cdot Ke + D/V \cdot Kd \cdot (1 - T)$$

WACC= (0.7) (0.118) +(0.3) (0.07) (0.75) =0.0826

=0.0826+0.01575

=0.09835=**<u>9,84%</u>**

5.2.3 Beneficios No Económicos

En este apartado se reconocen las ventajas cualitativas del proyecto, como el cumplimiento normativo, la mejora en la reputación institucional, el fortalecimiento de la cultura organizacional en seguridad de la información y la preparación ante auditorías externas.

- Cumplimiento con Ley N° 19.628 y futuras normas.
- Mejora de la reputación frente a clientes y fiscalizaciones.
- Reducción del estrés operativo.
- Profesionalización interna y retención de talento.
- Base para futura certificación ISO/IEC 27001.

Cierre:

La inversión total de $11.040.281 CLP, distribuida en equipamiento y horas hombre reales, se compensa con beneficios directos anuales de al menos $40 millones, que aumentan con el tiempo. El proyecto tiene una relación costo-beneficio de 19,2:1, y un WACC de 9,84%, validando su viabilidad financiera incluso bajo exigencias de mercado. La propuesta no solo es rentable, sino también escalable, cumplidora de normativas y de bajo riesgo operacional.

Capítulo 6: Resultados y Conclusiones

6.1. Análisis Crítico de los Resultados

El proyecto propone un Sistema de Gestión de Seguridad de la Información para abordar las vulnerabilidades críticas en la seguridad de la información de la Empresa de Venta de Neumáticos, identificadas tras tres brechas de datos en 2024 que afectaron a 150 clientes y una falta de capacitación en el 65% de los empleados. Los resultados proyectados, basados en la implementación del Ciclo de Deming, la norma ISO/IEC 27001 y los indicadores de control (KPI), se analizan a continuación en función de los objetivos específicos:

- **Objetivo Específico 1:** Realizar un levantamiento para identificar los activos tangibles e intangibles de información que se requiere proteger
    - **Resultado Proyectado:** El diagnóstico técnico inicial identificó y clasificó el 100% de los activos críticos (e.g., datos de clientes, registros financieros, inventarios) en un plazo de dos semanas, utilizando una matriz de activos alineada con ISO/IEC 27001 (Capítulo 4, Sección 4.2.2.2). Este levantamiento incluyó bases de datos en CRM, SAP y servidores, logrando una cobertura completa de los datos sensibles.
    - **Análisis Crítico:** La identificación exhaustiva de activos es un logro significativo, ya que establece una base sólida para priorizar la protección de la información. Sin embargo, el éxito depende de la

precisión del mapeo, y el documento no detalla cómo se validará la exhaustividad de este inventario en entornos dinámicos (ej., nuevos datos generados por clientes). La falta de un proceso continuo para actualizar el inventario podría limitar la escalabilidad a largo plazo. Además, el plazo de dos semanas es ambicioso para una pyme con recursos limitados, lo que podría requerir ajustes en la planificación.

- **Objetivo Específico 2**: Analizar los riesgos de seguridad de la información para identificar vulnerabilidades y establecer medidas preventivas
    - **Resultado Proyectado:** Se identificaron cinco riesgos críticos (nivel 16-20, Tabla 8), como pérdida de datos personales, accesos inseguros a plataformas bancarias y falta de firewalls, mediante el Diagrama de Ishikawa y la Matriz de Criticidad. Se propusieron medidas preventivas (e.g., autenticación multifactor, cifrado TLS, firewalls) que proyectan una reducción del 80% en incidentes de seguridad en seis semanas (Capítulo 4).
    - **Análisis Crítico:** El análisis de riesgos es robusto, ya que utiliza herramientas estandarizadas (Ishikawa, ISO/IEC 27001) y prioriza amenazas críticas basadas en probabilidad e impacto. La proyección de una reducción del 80% es ambiciosa pero realista, respaldada por estándares como NIST CSF 2.0. Sin embargo, la efectividad de las medidas depende de la adopción por parte del

personal, donde el 65% carece de capacitación. La falta de un plan detallado para superar esta barrera humana podría retrasar los resultados. Además, el análisis no considera riesgos emergentes (ej., nuevas formas de ransomware), lo que sugiere la necesidad de revisiones periódicas.

- **Objetivo Específico 3:** Evaluar las normativas y estándares de seguridad relevantes para garantizar el cumplimiento legal y regulatorio
    - **Resultado Proyectado:** Se identificaron brechas normativas con respecto a ISO/IEC 27001 y la Ley 19.496, proponiendo controles como cifrado y MFA para cerrar el 100% de estas brechas en cuatro semanas, con la validación de un consultor externo (Capítulo 4, Sección 4.2.2.5). Esto reduce el riesgo de sanciones legales de hasta 1,500 UTM.
    - **Análisis Crítico:** La evaluación normativa es un punto fuerte, ya que alinea los procesos con estándares internacionales y locales, fortaleciendo la posición legal de la empresa. La contratación de un consultor externo añade credibilidad al proceso. Sin embargo, el plazo de cuatro semanas para corregir todas las brechas puede ser optimista, considerando la complejidad de implementar controles en todos los procesos. Además, el documento no aborda cómo se gestionarán actualizaciones futuras en la Ley 19.496, lo que podría requerir ajustes adicionales.

- **Objetivo Específico 4:** Modelar un plan de respuesta ante incidentes de seguridad para minimizar el impacto en la operación

    - Resultado Proyectado: Se diseñó un plan de respuesta a incidentes con etapas de detección, contención, recuperación y análisis post-incidente, logrando un tiempo de respuesta promedio inferior a 60 minutos en simulaciones (Capítulo 4, Sección 4.2.2.6). Este plan utiliza herramientas como SIEM (Wazuh) y sigue las mejores prácticas de ISO/IEC 27001.

    - Análisis Crítico: El plan es sólido, ya que aborda el impacto de incidentes como las brechas de 2024 y establece un tiempo de respuesta competitivo según NIST CSF 2.0. La simulación de incidentes asegura su aplicabilidad práctica. Sin embargo, la dependencia de herramientas de código abierto como Wazuh podría limitar el soporte técnico en escenarios complejos, y la capacitación del personal en este plan no está suficientemente detallada, lo que podría afectar su ejecución.

- **Objetivo Específico 5:** Evaluar los costos asociados a la propuesta para diseñar un Sistema de Gestión de Seguridad de la Información

    - **Resultado Proyectado:** El costo total del proyecto es de $11,040,281 CLP, con una relación costo-beneficio de 19,2:1 y beneficios económicos proyectados de $212,365,432 CLP en cinco años, incluyendo ahorros por reducción de incidentes ($10M/año),

evitación de sanciones ($10M/año) y aumento de ventas por confianza del cliente ($20M/año) (Capítulo 5).

- **Análisis Crítico:** La relación costo-beneficio de 19,2:1 demuestra una alta rentabilidad, validada por un WACC de 9,84%, lo que justifica la inversión para una pyme. La optimización del presupuesto (reducción del 50% respecto a la versión original) refleja un enfoque eficiente. Sin embargo, los beneficios proyectados asumen un incremento constante del 3% anual, lo que podría no cumplirse si las condiciones de mercado cambian. Además, los costos de mantenimiento a largo plazo (e.g., actualizaciones de firewalls, capacitación continua) no están completamente detallados, lo que podría incrementar el presupuesto en el futuro.

6.2. Evaluación General de los Resultados

Fortalezas:

- La propuesta aborda los riesgos críticos identificados (nivel 20) con medidas específicas (MFA, firewalls, cifrado), logrando una reducción proyectada del 80% en incidentes de seguridad.
- La alineación con ISO/IEC 27001 y la Ley 19.496 posiciona a la empresa para cumplir con normativas y evitar sanciones, fortaleciendo su reputación.
- El uso del Ciclo de Deming asegura un enfoque de mejora continua,

con KPI claros (e.g., 95% de interacciones seguras, 100% de accesos con MFA) que facilitan el monitoreo.

- La viabilidad económica, con una relación costo-beneficio de 19,2:1, hace que la propuesta sea atractiva para una pyme.

Impacto Proyectado: La implementación del Sistema de Gestión de Seguridad de la Información mitiga las vulnerabilidades críticas (ej., pérdida de datos de 150 clientes en 2024), mejora la continuidad operativa y posiciona a la empresa para una futura certificación ISO/IEC 27001. Los beneficios no económicos, como la mejora de la reputación y la profesionalización interna, complementan los $40M anuales proyectados.

6.3. Conclusiones

Basado en el análisis crítico de los resultados, las conclusiones se alinean con los objetivos específicos del proyecto y destacan el impacto del Sistema de Gestión de Seguridad de la Información en la Empresa de Venta de Neumáticos:

1) **Cumplimiento del Objetivo de Identificación de Activos:** La identificación del 100% de los activos críticos en dos semanas establece una base sólida para la gestión de riesgos, cumpliendo con ISO/IEC 27001. Sin embargo, se recomienda implementar un proceso continuo de actualización del inventario para garantizar su relevancia en un entorno dinámico.

2) **Mitigación de Riesgos Críticos:** La propuesta logra mitigar cinco riesgos

críticos mediante controles como MFA, cifrado y firewalls, proyectando una reducción del 80% en incidentes en seis semanas. Esto aborda directamente las brechas de 2024 y fortalece la seguridad, aunque la capacitación del personal debe reforzarse para asegurar la efectividad.

3) **Cumplimiento Normativo:** La evaluación y corrección del 100% de las brechas normativas en cuatro semanas alinea a la empresa con la Ley 19.496 y ISO/IEC 27001, reduciendo el riesgo de sanciones legales. Es crucial planificar revisiones periódicas para adaptarse a cambios normativos futuros.

4) **Plan de Respuesta a Incidentes:** El plan diseñado, con un tiempo de respuesta inferior a 60 minutos, minimiza el impacto de incidentes y protege los activos digitales. La incorporación de simulaciones y herramientas como Wazuh asegura su aplicabilidad, pero se sugiere fortalecer el soporte técnico para herramientas de código abierto.

5) **Viabilidad Económica:** El costo de $11,040,281 CLP, con una relación costo-beneficio de 19,2:1 y beneficios de $212M en cinco años, valida la rentabilidad del proyecto. Los beneficios no económicos, como la mejora de la reputación y la preparación para auditorías, posicionan a la empresa como líder en el sector automotriz chileno.

Conclusión General:

La propuesta de Sistema de Gestión Seguridad de la Información es una solución integral que aborda las vulnerabilidades críticas de la Empresa de Venta de Neumáticos, protege datos sensibles, garantiza el cumplimiento normativo y asegura la continuidad operativa. La reducción proyectada del 80% en incidentes, combinada con una alta rentabilidad y beneficios no económicos, fortalece la competitividad y sostenibilidad de la empresa en un mercado digitalizado. Para maximizar el impacto, se recomienda priorizar la capacitación del personal, establecer auditorías continuas y prever recursos para mantenimiento a largo plazo, sentando las bases para una futura certificación ISO/IEC 27001.

Capítulo 7: Bibliografía

Accenture. (2024). Informe sobre ciberseguridad en pymes. Recuperado de https://www.accenture.com/insights/cybersecurity-pymes

Cordero Ávila, A. (2011). Análisis de criticidad y estudio RCM del equipo de máxima criticidad de una planta desmotadora de algodón [Tesis de grado]. Universidad de Sevilla. https://biblus.us.es/bibing/proyectos/abreproy/5311/fichero/5-+Analisis+de+criticidad.pdf

International Organization for Standardization. (s.f.). ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection. https://www.iso.org/standard/82875.html

Kaspersky. (2024). Tendencias de ciberseguridad en América Latina. Recuperado de https://www.kaspersky.com/latam/business-security

Pronodo. (2024). Riesgos de ransomware en pymes chilenas. Recuperado de https://www.pronodo.cl/informes/ransomware

Capítulo 8: Webgrafía

La webgrafía incluye las fuentes en línea citadas explícitamente en las ilustraciones, presentadas en formato APA 7ª edición como referencias web, sin hipervínculos activos.

Asesorías. (s.f.). El círculo de Deming o la espiral de mejora continua. Recuperado de https://asesorias.com/empresas/modelos-plantillas/circulo-deming/

Normas ISO. (s.f.). ISO 27001 Seguridad de la Información. Recuperado el 26 de abril de 2025, de https://www.normas-iso.com/iso-27001/

PLOOSI. (2022). El diagrama de Ishikawa. Recuperado de https://ploosi.com/el-diagrama-de-ishikawa