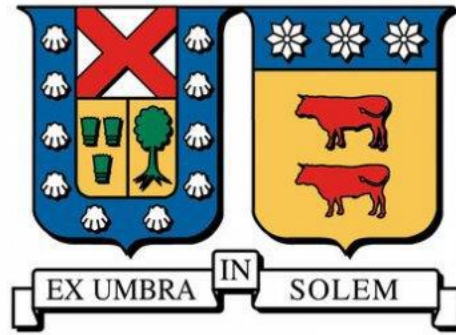




UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA

DEPARTAMENTO DE INDUSTRIAS

DISEÑO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

PARA TERMINAL PORTUARIO EN CHILE

MEMORIA PARA OPTAR AL TÍTULO DE INGENIERO CIVIL INDUSTRIAL

AUTOR

ALDO BRUNO QUINTEROS CORREA

PROFESORA GUÍA

MÓNICA LÓPEZ C.

PROFESOR CORREFERENTE

SIMÓN GÓMEZ M.

JUNIO 2025



CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☒ Memoria o trabajo de título; ☐ Tesis de Postgrado;

Título del trabajo: DISEÑO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA TERMINAL PORTUARIO EN CHILE

Nombre del candidato(a): Aldo Bruno Quinteros Correa

Carrera / Grado: Ingeniería Civil Industrial

Campus: Casa Central Valparaíso ; **Departamento:** Industrias

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Mónica López Campos, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL

☐ El trabajo **NO contiene información que amerite confidencialidad** y puede ser publicado de inmediato en repositorio con acceso abierto.

☒ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (embargo) por:

☐ 6 meses; ☒ 12 meses; ☐ 2 años; ☐ 3 años; ☐ 5 años; ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

Describe la situación de la empresa en cuanto a sus riesgos informáticos, el plan y estado de la implementación de controles de seguridad para mitigar estos riesgos. Se describen costos de servicios relacionados contratados por la empresa. Los planes y metodologías aplicadas podrían constituir una ventaja competitiva de la empresa.

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 21-08-2025

; Firma:

Estudiante o Candidato(a):

Fecha: 20-08-2025

; Firma:

Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.

Resumen Ejecutivo

La presente memoria propone el diseño y la estrategia de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para una empresa portuaria chilena, en respuesta al creciente riesgo de ciberataques que afecta al sector logístico nacional. Considerando el rol estratégico de los puertos en el comercio exterior del país y su operación continua, se plantea un enfoque integral que combine estándares internacionales como ISO/IEC 27001, ISO/IEC 27005, ISO 22301 y los controles CIS v7.1, con metodologías de mejora continua como el ciclo PDCA, Lean y Six Sigma. El objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información crítica, fortaleciendo la resiliencia operativa frente a amenazas emergentes.

El diseño del SGSI se fundamenta en un análisis de la industria portuaria chilena, la infraestructura tecnológica de la empresa, y los procesos críticos que dependen de sistemas informáticos como el Terminal Operation System (TOS), sistemas financieros, y plataformas de gestión de recursos humanos. Se identifican activos de información, áreas operativas clave, y se evalúan riesgos mediante una matriz que clasifica amenazas según su probabilidad e impacto. A partir de esta evaluación, se seleccionan controles técnicos, organizativos y físicos, priorizando aquellos que abordan los riesgos intolerables y críticos.

La estrategia de implementación se estructura en fases, comenzando con la formalización de políticas y procedimientos basados en controles ISO y CIS, seguida por la capacitación del personal y la integración de los controles en los procesos existentes. Se establece un cronograma de un año para la implementación inicial, con participación del área de informática y apoyo de asesores externos. La planificación contempla la asignación de recursos humanos especializados y la adquisición de herramientas tecnológicas.

Finalmente, se propone un sistema de monitoreo y mejora continua que incluye auditorías internas, revisión periódica de documentos, y actualización de controles conforme a la evolución de amenazas. Este enfoque escalonado permite una implementación ordenada y sostenible del SGSI, alineando la seguridad de la información con los objetivos estratégicos de la empresa y las exigencias legales del marco normativo chileno. El resultado es una propuesta robusta, adaptable y orientada a fortalecer la cultura de seguridad en una industria clave para el desarrollo económico del país.

Índice de contenidos

Capítulo I: Introducción	5
1. Problema de investigación	5
Capítulo II: Objetivos	9
1. Objetivo General	9
2. Objetivos Específicos	9
Capítulo III: Metodología	10
1. Análisis de la industria Portuaria en Chile	10
2. Investigación de estándares internacionales y metodologías de mejora continua	10
a. Normas y Estándares Internacionales	11
b. Metodologías de Mejora Continua	11
3. Diseño de un sistema de gestión de seguridad de la información para una empresa portuaria de Chile	11
c. Definición del alcance	12
d. Identificación de riesgos específicos	12
e. Selección de Controles de Seguridad	12
f. Desarrollo de políticas y procedimientos	13
4. Diseño de la estrategia de implementación de un sistema de gestión de seguridad de la información para una empresa portuaria de Chile	13
a. Planificación de la implementación	13
b. Capacitación y Concientización	14
c. Integración de Procesos existentes	14
d. Monitoreo y Mejora continua	14
Capítulo IV: Marco Teórico	15
1. Industria portuaria chilena	15
a. Infraestructura portuaria chilena	16
b. Volumen y tipo de carga en puertos chilenos	17
c. Actores principales	18
2. Estándares internacionales de seguridad de la información	19
a. ISO/IEC 27001	19
b. ISO/IEC 27005	21
c. ISO 22301	22
d. Controles CIS	23
3. Metodologías de Mejora Continua	24

a. Six Sigma	24
b. Lean	25
c. Ciclo PDCA	26
d. Integración de Ciclo PDCA con Estándares Internacionales.....	28
Capítulo V: Desarrollo.....	29
2. Diseño del Sistema de Gestión de Seguridad de la Información para una empresa portuaria de Chile	29
a. Identificación de Activos de Información	29
b. Identificación de áreas y procesos de la organización	31
c. Clasificación de riesgos	34
d. Selección de controles de seguridad	39
e. Desarrollo de políticas y procedimientos	45
Capítulo VI: Implementación	56
1. Planificación de la implementación.....	56
2. Cronograma de la implementación.....	58
3. Recursos para la implementación	64
Capítulo VII: Conclusiones	67
Referencias Bibliográficas	70

Índice de tablas

Tabla 1 Tipos de activos de información.....	31
Tabla 2 Áreas, procesos y sistemas críticos.....	33
Tabla 3 Criticidad de activos de información.....	35
Tabla 4 Probabilidad e impacto de amenazas.....	38
Tabla 5 Matriz de riesgos.....	38
Tabla 6 Nivel de riesgo y mitigación de riesgos evaluados.....	39
Tabla 7 Selección de controles ISO.....	41
Tabla 8 Selección de controles CIS.....	45
Tabla 9 Implementación de Controles CIS en Políticas y Procedimientos.....	59
Tabla 10 Actividades y participantes implementación controles.....	63
Tabla 11 Cronograma Implementación Controles.....	64

Índice de figuras

Ilustración 1 Comercio exterior (% del PIB) de Chile últimos 20 años.....	15
Ilustración 2 Ciclo PDCA aplicado a ISO 27001.....	28
Ilustración 3 Diagrama de flujo ejemplo procedimiento.....	54

Capítulo I: Introducción

1. Problema de investigación

El avance de la era digital ha traído consigo una serie de cambios significativos en la forma en que las empresas operan, sin embargo, este cambio también ha llevado a un aumento en la cantidad y sofisticación de ciberataques. En la actualidad se han multiplicado exponencialmente los incidentes de este tipo, convirtiéndose en una amenaza constante para empresas, gobiernos y ciudadanos. Una muestra de esto es que en América Latina los ciberataques han aumentado considerablemente, con más de 1.1 billones de ataques de malware bloqueados entre junio de 2023 y julio de 2024, lo que equivale a aproximadamente 2.2 millones de ataques por minuto (Kaspersky, 2024). El Panorama de Amenazas de Kaspersky de 2024 destaca que la amenaza "UFO:Blocked.Adware" se posicionó como el riesgo más significativo, representando el 44.45% de las detecciones. En varios países de la región se han registrado incrementos en la cantidad de ataques en comparación con el año anterior: Argentina un 15 %, Bolivia un 10 %, Chile un 11.2 %, Costa Rica un 6.4 %, Panamá un 4.9 %, Paraguay un 1.7 %, Perú un 2.9 %, República Dominicana un 25 % y Uruguay un 16 %. La sofisticación de los ataques, la expansión de la superficie de ataque y la creciente interconexión de dispositivos han dado lugar a una urgente necesidad de proteger la información sensible de las organizaciones.

Fortinet, por su parte, reportó que América Latina y el Caribe sufrieron más de 289 mil millones de intentos de ciberataques en 2021, lo que representa un aumento del 600% con respecto a 2020 (FortiGuard Labs, 2022). México fue el país que más intentos de ataques recibió (156 mil millones), seguido de Brasil (88,5 mil millones), Perú (11,5 mil millones) y Colombia (11,2 mil millones). Check Point también informó que los ciberataques registrados en Latinoamérica se incrementaron un 38% en 2021 (Valades, 2022).

Estos datos entregados por distintas organizaciones especializadas en ciberseguridad reflejan el panorama actual de amenazas cibernéticas en constante evolución y que es imperativo para las empresas adoptar medidas proactivas para proteger su información crítica. Un Sistema de Gestión de Seguridad de la Información (SGSI) se presenta como una solución integral, diseñada para asegurar la confidencialidad, integridad y

disponibilidad de los datos. Basándose en estándares internacionales como el ISO/IEC 27001, un SGSI ayuda a las organizaciones a establecer un marco robusto que no solo previene incidentes de seguridad, sino que también proporciona un enfoque estructurado para responder a ellos de manera efectiva. Implementar un SGSI no es una tarea única, sino un proceso continuo que se adapta y evoluciona con la empresa, garantizando una seguridad sostenible en el tiempo (Rodríguez, Cruzado, Mejía, & Alarcón, 2020).

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) desde una perspectiva teórica requiere una comprensión holística y multifacética que abarque diversas metodologías y prácticas. Esencialmente, la gestión estratégica en el contexto de un SGSI se centra en la alineación de los objetivos de seguridad con los objetivos empresariales generales, asegurando que las iniciativas de seguridad informática refuercen y habiliten la estrategia organizacional. Desde el punto de vista de la mejora continua y las técnicas de gestión de procesos empresariales (BPM), el Ciclo PDCA (Planificar, Hacer, Verificar, Actuar) ofrece un marco robusto para la implementación y mejora continua del SGSI. Este enfoque iterativo permite a las organizaciones adaptarse dinámicamente a los cambios en el entorno de seguridad cibernética y asegurar que las políticas y controles estén actualizados y sean efectivos Alemán-Novoa, H. C. I. (2015).

La aplicación teórica del SGSI también debe considerar el tamaño y tipo de organización, así como la industria específica en la que opera. Por ejemplo, una entidad financiera puede requerir un enfoque más riguroso en términos de control de acceso y gestión de transacciones en comparación con una empresa educativa que podría enfocarse más en la protección de datos personales y propiedad intelectual. Además, la implementación efectiva de un SGSI debe incorporar políticas claras, estándares reconocidos como ISO/IEC 27001 y marcos de referencia como NIST o COBIT para establecer un lenguaje común y prácticas consistentes dentro de la organización. Estos estándares proporcionan las directrices necesarias para desarrollar un SGSI que no solo sea técnico desde el punto de vista del área de TI sino también integrado en la gestión estratégica general de la empresa (Rodríguez, Cruzado, Mejía, & Alarcón, 2020).

Bajo el contexto de la industria portuaria chilena, que es fundamental para la economía del país debido a su rol en el comercio internacional y la logística, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en una empresa portuaria

mediana (aproximadamente 450 trabajadores) es crucial. Esta empresa, que opera como terminal portuario, utiliza sistemas informáticos avanzados, incluyendo un Terminal Operation System (TOS) para la gestión de operaciones portuarias y sistemas financieros para la administración económica. Los procesos críticos para la transferencia de contenedores, que incluyen la carga, descarga y almacenamiento, dependen en gran medida de la integridad y disponibilidad de estos sistemas. La detención de las operaciones debido a un ciberataque tendría un impacto negativo, no solo en la empresa, sino también en la cadena de suministro y la economía nacional (Álvarez, 2023).

Además, es imperativo que la empresa cumpla con la Ley Marco de Ciberseguridad (Ley 21.663), donde se fijan normas para empresas que se catalogan como Prestadoras de Servicios Esenciales (PSE) al considerarse que forman parte de sectores que son fundamentales para la economía y la seguridad del país. Al entrar el sector portuario dentro de esta categoría, el marco incluye exigencias como lo son la implementación de medidas de protección, evaluación de riesgos, capacitación del personal y la adopción de políticas de seguridad robustas para garantizar la continuidad operativa y la protección de la información crítica (Karmy, 2024).

Siguiendo con los lineamientos de la Ley Marco de Ciberseguridad, las entidades PSE (o incluso cualquiera que no tenga ese carácter) pueden o no ser calificadas como Operadores de Importancia Vital (OIV). Esto lo realiza la Agencia Nacional de Ciberseguridad (ANCI) en base a ciertos criterios como la dependencia de sistemas informáticos y redes, y el grado de afectación que la interrupción de entrega de servicios pueda causar al orden público. En caso de ser catalogada como OIV la empresa portuaria, la ley impondrá deberes específicos entre los cuales está implementar un Sistema de Gestión de Seguridad de la Información (Karmy, 2024).

Tanto para asegurar la continuidad operacional y la recuperación ante incidentes de ciberseguridad, como para el cumplimiento legal de la empresa portuaria, se debe determinar ¿qué características de la industria portuaria son relevantes y se deben considerar para el diseño de un sistema de gestión de seguridad de la información? ¿cuál de la metodología de mejora continua es óptima para su aplicación en un sistema de gestión de seguridad de la información? Se pretende mediante el análisis del sector portuario chileno en general y de la empresa portuaria en particular, y las metodologías de mejora continua,

poder diseñar un Sistema de Gestión de Seguridad de la Información para la implementación de controles de ciberseguridad de la empresa terminal portuario chileno, siguiendo normas y estándares de entidades internacionales.

Capítulo II: Objetivos

1. Objetivo General

Proponer el diseño de un sistema de gestión mediante el uso de metodologías de mejora continua, para la implementación de controles de seguridad de la información en una empresa portuaria de Chile.

2. Objetivos Específicos

Analizar las características de la industria portuaria en Chile para identificar información relevante para el diseño de un sistema de gestión de seguridad de la información.

Investigar metodologías de mejora continua con el fin de determinar la más apropiada para aplicar en un sistema de gestión de seguridad de la información.

Diseñar un sistema de gestión de seguridad de la información para una empresa portuaria de Chile, basado en estándares internacionales y a través de metodologías de mejora continua.

Diseñar estrategia de implementación del sistema de gestión de seguridad de la información para una empresa portuaria de Chile.

Capítulo III: Metodología

1. Análisis de la industria Portuaria en Chile

Para comprender a fondo la industria portuaria chilena, es necesario investigar diversas fuentes de información, incluyendo informes de la Cámara Marítima y Portuaria de Chile (CAMPORT), estudios de caso, y publicaciones académicas. Estas fuentes proporcionan datos sobre distintos aspectos relevantes de la industria, como lo son la infraestructura portuaria y el volumen de carga manejado.

Además, se identifican y describen los actores clave en la industria portuaria, incluyendo autoridades portuarias, operadores logísticos, proveedores de servicios tecnológicos y clientes. Para fortalecer este análisis, se cuenta con la cooperación de personal de la empresa con experiencia y con cargos a nivel de jefatura, principalmente de las áreas de Operaciones y Comercial, dado su conocimiento a nivel táctico y estratégico sobre el negocio, la logística y competitividad portuaria, lo que permite evaluar de manera precisa los desafíos y oportunidades del sector, asegurando un enfoque realista y aplicable a la implementación del SGSI.

Este enfoque integral se desarrolla en el Capítulo IV: Marco Teórico, y proporciona una base sólida para el diseño e implementación de un SGSI robusto y resiliente, adaptado a las necesidades y desafíos específicos de una empresa portuaria en Chile.

2. Investigación de estándares internacionales y metodologías de mejora continua

Es fundamental comprender los estándares y normas que definen los lineamientos a seguir por empresas internacionales y las metodologías de mejora continua que pueden aplicarse. Para esto se lleva a cabo una revisión de literatura en el Capítulo IV: Marco Teórico, donde se investigan normas internacionales y herramientas de mejora continua-

Además, esta actividad cuenta con el apoyo de un proveedor externo especializado en ciberseguridad, quien aporta conocimientos técnicos y experiencia en la implementación de controles de seguridad en el área de Informática. Su participación permite evaluar la

aplicabilidad de estándares y metodologías en el contexto digital, asegurando una integración efectiva dentro del SGSI.

a. Normas y Estándares Internacionales

- ISO/IEC 27001: Esta norma internacional especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI. Se enfoca en la gestión de riesgos y la implementación de controles de seguridad adecuados.
- ISO/IEC 27005: Esta norma proporciona directrices para la gestión del riesgo de seguridad de la información, ayuda a las organizaciones a identificar, evaluar y tratar los riesgos que podrían comprometer la seguridad de la información. En Chile, la autoridad marítima exige el cumplimiento de esta norma para asegurar una gestión adecuada de los riesgos en el sector portuario.
- ISO 22301: Relacionada con la continuidad del negocio, esta norma puede complementar un SGSI al asegurar que la organización pueda continuar operando durante y después de un incidente de seguridad.
- Controles CIS: Conjunto de medidas de seguridad prioritarias diseñadas para proteger contra las amenazas más comunes. Estos controles se dividen en tres niveles de implementación (IG), que ayudan a las organizaciones a priorizar y aplicar los controles de manera efectiva.

b. Metodologías de Mejora Continua

Se exploran metodologías como Six Sigma, Lean, y el ciclo PDCA. Estas metodologías se centran en la mejora continua de procesos y pueden adaptarse para la gestión de la seguridad de la información.

3. Diseño de un sistema de gestión de seguridad de la información para una empresa portuaria de Chile

Una vez revisada la literatura y demás fuentes de información en el Capítulo IV: Marco Teórico, se definen las normas, estándares y metodologías de mejora continua a aplicar para el diseño del SGSI adaptado a la empresa portuaria. Este diseño se realiza de manera

conjunta por las distintas gerencias del terminal, dado que son los responsables de tomar decisiones estratégicas en materia de riesgos y seguridad. Su participación asegura que el SGSI esté alineado con los objetivos organizacionales y los requisitos operacionales, permitiendo una implementación efectiva y sostenible.

c. Definición del alcance

- **Identificación de Activos de Información:** Enumera todos los activos de información que necesitan protección, como bases de datos, sistemas de operación portuaria, y redes de comunicación.
- **Determinación de Límites:** Define los límites del SGSI, especificando qué partes de la organización y qué procesos estarán cubiertos por el sistema. Para esto cada gerencia debe identificar los procesos críticos de su operación.

d. Identificación de riesgos específicos

Se utiliza una metodología estructurada, como la sugerida por ISO/IEC 27005, para identificar, analizar y evaluar los riesgos de seguridad de la información:

- **Identificación de Riesgos:** Listar posibles amenazas y vulnerabilidades que podrían afectar los activos de información.
- **Análisis de Riesgos:** Realizar la evaluación de la probabilidad y el impacto de cada riesgo identificado.
- **Evaluación de Riesgos:** Clasificar de los riesgos según su nivel de criticidad para priorizar las acciones de mitigación.

La identificación y el análisis de riesgos es realizada por las gerencias de las áreas, con el asesoramiento de un proveedor de servicios de consultoría en ciberseguridad.

e. Selección de Controles de Seguridad

A partir del alcance y los riesgos identificados, se establecen los controles para proteger a la organización de los vectores de ataque más comunes. Estos se dividen en tres categorías:

- **Controles Técnicos:** Implementación de medidas técnicas como firewalls, antivirus, parches de remediación de vulnerabilidades, monitoreo y análisis de registros de sistemas y cifrado de datos.

- Controles Organizativos: Desarrollo de políticas y procedimientos de seguridad, formación y concienciación del personal.
- Controles Físicos: Medidas para proteger las instalaciones físicas, como controles de acceso y vigilancia.

La organización define que la responsable de seleccionar y priorizar los controles a aplicar es la Gerencia de Informática con la aprobación de la Gerencia General.

f. Desarrollo de políticas y procedimientos

Con los controles de seguridad definidos a aplicar en la empresa, se desarrollan las políticas y procedimientos que definan las directrices y responsabilidades para la gestión de la seguridad de la información, y documentan los pasos que se deben realizar por los distintos cargos y áreas de la empresa para la implementación y mantenimiento de los controles de seguridad.

4. Diseño de la estrategia de implementación de un sistema de gestión de seguridad de la información para una empresa portuaria de Chile

Una vez diseñado el SGSI, dado el carácter técnico y digital de la seguridad de la información, su estrategia de implementación es definida por el área de Informática, que cuenta con experiencia y conocimientos en la administración de sistemas tecnológicos y en la aplicación de controles de seguridad técnicos, además de la capacidad para responder ante incidentes de seguridad. Este equipo es responsable de gestionar la infraestructura tecnológica y garantizar que la seguridad de la información se integre adecuadamente en los procesos tecnológicos existentes de la empresa.

a. Planificación de la implementación

- Cronograma de Implementación: Desarrollo de un cronograma detallado que incluya todas las actividades necesarias para implementar el SGSI, con fechas y responsables asignados.
- Asignación de Recursos: Identificación y asignación de los recursos necesarios, incluyendo personal, tecnología y presupuesto.

b. Capacitación y Concientización

- Programas de Capacitación: Diseño de programas de formación para asegurar que el personal requerido comprenda las políticas y procedimientos de seguridad de la información.
- Campañas de Concientización: Realización de campañas para sensibilizar al personal sobre la importancia de la seguridad de la información y las mejores prácticas a seguir.

c. Integración de Procesos existentes

- Evaluación de Procesos Actuales: Revisión de los procesos operativos actuales, principalmente del área de informática, para identificar oportunidades de integración con el SGSI.
- Adaptación de Procesos: Modificación de los procesos existentes para incorporar los controles de seguridad de la información sin interrumpir las operaciones diarias.

d. Monitoreo y Mejora continua

- Sistema de Monitoreo: Implementación de herramientas y procedimientos para monitorear continuamente la efectividad del SGSI.
- Auditorías Internas: Realización de auditorías internas periódicas para evaluar el cumplimiento y la efectividad del SGSI.
- Revisión y Actualización: Uso del ciclo PDCA para revisar y actualizar continuamente el SGSI, asegurando su mejora continua.

Capítulo IV: Marco Teórico

1. Industria portuaria chilena

La industria portuaria es un pilar fundamental para el comercio global, facilitando el movimiento de bienes y servicios a través de fronteras internacionales. En Chile, los puertos son esenciales para la economía, ya que una gran parte del comercio exterior del país se realiza a través de ellos. En 2023, el 91% del comercio internacional se desarrolló por vía marítima (Camport, 2024), considerando que ese mismo año el comercio exterior representó el 61% del PIB de Chile según el Banco Mundial.

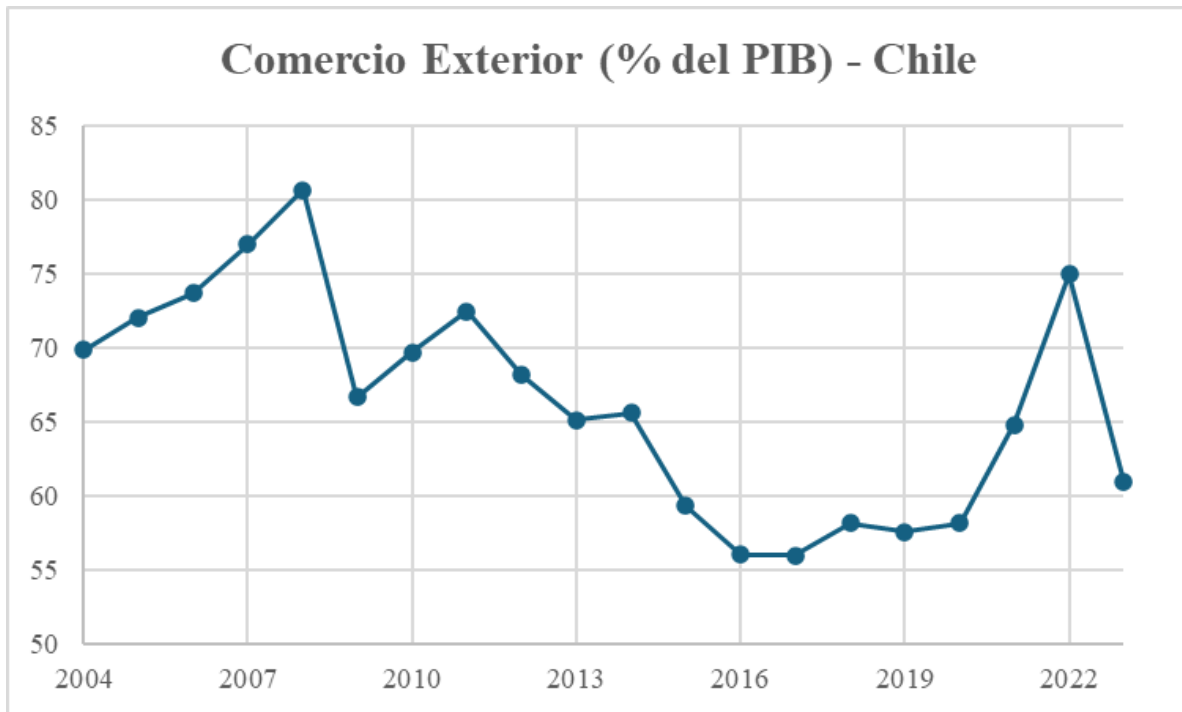


Ilustración 1 Comercio exterior (% del PIB) de Chile últimos 20 años.

Fuente: Banco Mundial (World Bank Open Data, 2025).

Esta importancia se refleja en la transformación significativa que ha tenido la infraestructura portuaria en Chile en las últimas décadas, impulsada por la asociación

público-privada y la necesidad de modernizar los puertos para acomodar el creciente tamaño de los buques portacontenedores (Cortés, 2022).

a. Infraestructura portuaria chilena

Los puertos chilenos están estratégicamente ubicados a lo largo de su extensa costa. Algunos de los puertos clave, organizados geográficamente de norte a sur, incluyen (Bhattacharjee, 2022):

- Arica: Situado en el norte de Chile, Arica es conocido por la exportación de productos agrícolas, particularmente cítricos y aceitunas.
- Iquique: Este puerto en la región de Tarapacá es un actor importante en el comercio exterior de Chile.
- Coquimbo: Ubicado en el centro de Chile, Coquimbo es un puerto más pequeño que sirve como centro comercial. Maneja una variedad de productos, incluyendo cemento, productos agrícolas, minerales y fertilizantes.
- Valparaíso: Históricamente significativo como escala para embarcaciones que navegaban por el Estrecho de Magallanes, Valparaíso sigue siendo un puerto crucial para contenedores y pasajeros.
- San Antonio: Ubicado cerca de Santiago, este es el puerto más activo de Chile y un importante centro para carga convencional, a granel, RoRo, productos en contenedores y petroleros. Maneja aproximadamente 12.150.000 toneladas de carga y 775.000 TEUs anualmente.
- Lirquén: Situado en la Bahía de Concepción, Lirquén maneja importaciones como productos en contenedores, fertilizantes y azúcar, mientras que exporta madera, pulpa y harina de pescado.
- Talcahuano: Este puerto juega un papel vital en las actividades industriales y comerciales de la Región del Biobío.
- Punta Arenas: Ubicado en el sur de Chile, Punta Arenas sirve como una puerta de entrada crucial para el comercio y el turismo.

Para satisfacer las crecientes demandas comerciales, Chile está llevando a cabo importantes proyectos de expansión portuaria. El más notable es el Puerto Exterior en San Antonio, un proyecto de \$2.3 mil millones de dólares que tiene como objetivo agregar una capacidad sustancial a través de una expansión en alta mar. Esta expansión creará dos frentes de atraque, cada uno con una capacidad de transferencia de aproximadamente tres millones de TEUs. Se espera que el proyecto esté terminado para 2035 (Bendersky, 2023).

Otro proyecto clave es la expansión del Terminal 2 en el Puerto de Valparaíso, con una inversión estimada de \$500 millones de dólares. Este proyecto tiene como objetivo aumentar la capacidad en un millón de TEUs para 2030. Estas expansiones son cruciales para mantener niveles de ocupación adecuados y mejorar la eficiencia de los puertos chilenos (Daily Cargo News, 2023).

b. Volumen y tipo de carga en puertos chilenos

Los puertos chilenos manejan un volumen sustancial de carga, lo que refleja el papel destacado del país en el comercio internacional. En 2022, el rendimiento total de los puertos de contenedores en Chile se reportó en 4.158.260 TEUs. Sin embargo, datos recientes indican una disminución en el manejo de carga. En abril de 2023, las concesionarias portuarias manejaron 1.679.084 toneladas, una disminución del 13,7% en comparación con el mismo mes de 2022. Esta tendencia a la baja continuó en el primer semestre de 2023, con una caída del 10% en el rendimiento del comercio exterior en comparación con el mismo período de 2022 (CEICdata.com, 2018).

Respecto al tipo de carga transferida en puertos chilenos, principalmente incluye:

- **Minerales:** Los puertos del norte de Chile manejan principalmente exportaciones de minerales, particularmente cobre, del cual Chile es el principal exportador mundial.
- **Productos agrícolas:** Los puertos del centro de Chile son cruciales para la exportación de productos agrícolas como frutas, vino y granos.
- **Contenedores:** La carga en contenedores es un componente importante del comercio exterior de Chile, con puertos como Valparaíso y San Antonio manejando volúmenes sustanciales de contenedores.

- **Productos forestales:** Los puertos del sur de Chile se especializan en la exportación de productos forestales, incluyendo madera, pulpa y papel.
- **Granel líquido:** Puertos como San Antonio tienen instalaciones dedicadas al manejo de carga líquida a granel, como petróleo y productos químicos.

c. Actores principales

Los terminales portuarios están compuestos por organizaciones públicas y privadas. Las empresas portuarias estatales desempeñan un papel importante en la gestión y regulación de las actividades portuarias. Estas empresas supervisan el desarrollo de infraestructura, la asignación de concesiones y las operaciones portuarias en general (Ministerio de Transportes y Telecomunicaciones, s.f.). Si bien la información específica sobre empresas públicas individuales es limitada, su papel para garantizar el funcionamiento eficiente de los puertos chilenos es crucial.

Otros actores que forman parte de la industria portuaria chilena son:

- **Agencias de Aduana:** Las agencias de aduana juegan un papel crucial en la industria portuaria, ya que son responsables de gestionar y facilitar el tránsito de mercancías a través de los puertos. Esto incluye la presentación de documentos, el pago de aranceles y la coordinación con las autoridades aduaneras para asegurar que las mercancías cumplan con todas las regulaciones y normativas.
- **Agencias de Líneas Navieras:** Las agencias de líneas navieras son intermediarias que representan a las compañías navieras y gestionan la carga y descarga de contenedores en los puertos. También se encargan de la logística y coordinación de rutas, asegurando que las mercancías lleguen a su destino en el tiempo y forma adecuados.
- **Aduana:** La aduana es una entidad gubernamental que regula y controla el comercio internacional a través de los puertos. Su función principal es recaudar aranceles y derechos de aduana, así como prevenir el contrabando y asegurar que todas las mercancías que ingresan y salen del país cumplan con las leyes y regulaciones vigentes.

- **Proveedores de Sistemas:** Los proveedores de sistemas de gestión de terminales (TOS) ofrecen soluciones tecnológicas que optimizan y automatizan los procesos de manejo de carga en los puertos. Estos sistemas permiten una mayor eficiencia y precisión en la gestión de contenedores, reduciendo tiempos de espera y mejorando la coordinación entre las diferentes partes involucradas en el proceso logístico.

2. Estándares internacionales de seguridad de la información

La seguridad de la información es una preocupación crítica para las organizaciones de todos los tamaños y en todas las industrias. Con la creciente frecuencia y sofisticación de los ciberataques, las organizaciones necesitan adoptar un enfoque sólido y proactivo para proteger sus valiosos activos y datos. Los estándares internacionales y las metodologías de mejora continua proporcionan un marco estructurado para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI).

a. ISO/IEC 27001

ISO/IEC 27001 es un estándar reconocido internacionalmente que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI). El estándar enfatiza un enfoque basado en riesgos, lo que permite a las organizaciones identificar, evaluar y tratar los riesgos de seguridad de la información adaptados a sus necesidades específicas. También especifica las mejores prácticas de gestión de seguridad y controles de seguridad integrales siguiendo un enfoque holístico de la seguridad de la información, considerando a las personas, los procesos y la tecnología (Schweizerische, 2013).

Los principios básicos de ISO/IEC 27001 giran en torno a la tríada CIA:

- **Confidencialidad:** Garantizar que la información sea accesible solo para personas y entidades autorizadas.

- Integridad: Mantener la exactitud e integridad de la información y prevenir modificaciones no autorizadas.
- Disponibilidad: Asegurar que la información y los sistemas sean accesibles para los usuarios autorizados cuando sea necesario.

ISO/IEC 27001 proporciona más de 100 controles organizados en 14 objetivos de control (ISO/IEC 27000 family, 2023), que abordan varios aspectos de la seguridad de la información, como:

- Políticas de seguridad de la información
- Organización de la seguridad de la información
- Seguridad de los recursos humanos
- Gestión de activos
- Control de acceso
- Criptografía
- Seguridad física y ambiental
- Seguridad de las operaciones
- Seguridad de las comunicaciones
- Adquisición, desarrollo y mantenimiento de sistemas
- Relaciones con proveedores
- Gestión de incidentes de seguridad de la información
- Aspectos de seguridad de la información de la gestión de la continuidad del negocio
- Cumplimiento

La implementación de ISO/IEC 27001 ofrece varios beneficios, que incluyen:

- Seguridad de la información mejorada: Al implementar los requisitos del estándar, las organizaciones pueden gestionar y proteger sistemáticamente sus activos de información.

- Reducción de riesgos: El enfoque basado en riesgos ayuda a las organizaciones a identificar y mitigar posibles amenazas, minimizando la probabilidad y el impacto de los incidentes de seguridad.
- Cumplimiento mejorado: ISO/IEC 27001 ayuda a las organizaciones a cumplir con los requisitos legales, regulatorios y contractuales relevantes.
- Mayor confianza del cliente: La certificación ISO/IEC 27001 demuestra el compromiso de una organización con la seguridad de la información, lo que aumenta la confianza entre los clientes y las partes interesadas.

Las organizaciones que manejan información confidencial, como las de los sectores de TI, finanzas, salud y gobierno, pueden beneficiarse significativamente del cumplimiento de ISO/IEC 27001. El estándar está reconocido internacionalmente, lo que lo hace adecuado para organizaciones que operan en diferentes regiones y jurisdicciones (Svobodová, 2023).

b. ISO/IEC 27005

ISO/IEC 27005 es un estándar internacional que proporciona directrices para la gestión de riesgos de seguridad de la información. Respalda los conceptos generales especificados en ISO/IEC 27001 y ayuda a las organizaciones a cumplir con los requisitos para abordar los riesgos de seguridad de la información. El estándar enfatiza un enfoque estructurado y sistemático para la gestión de riesgos, lo que permite a las organizaciones tomar decisiones informadas sobre cómo proteger sus activos de información y lograr sus objetivos de seguridad de la información. Ayuda a las organizaciones a lograr la confidencialidad, integridad y disponibilidad (CIA) de sus activos de información, alineándose con los principios fundamentales de seguridad (Meitarice et al, 2024).

Este estándar propone un proceso de gestión de riesgos que sigue estas siete etapas:

1. Establecimiento del contexto
2. Identificación de riesgos
3. Análisis de riesgos
4. Evaluación de riesgos
5. Tratamiento de riesgos

6. Aceptación de riesgos
7. Monitoreo y revisión

Estas etapas se pueden repetir en un proceso cíclico, y a lo largo de este proceso, debe haber una comunicación y consulta de riesgos adecuada.

Los principios básicos de ISO/IEC 27005 incluyen:

- **Establecimiento del contexto:** Definir el alcance y los límites de las actividades de gestión de riesgos.
- **Evaluación de riesgos:** Identificar, analizar y evaluar los riesgos de seguridad de la información.
- **Tratamiento de riesgos:** Seleccionar e implementar respuestas de riesgo apropiadas, como evitar, mitigar, transferir o aceptar el riesgo.
- **Aceptación de riesgos:** Determinar el nivel de riesgo residual que la organización está dispuesta a aceptar.
- **Comunicación y consulta de riesgos:** Interactuar con las partes interesadas durante todo el proceso de gestión de riesgos.
- **Monitoreo y revisión de riesgos:** Monitorear y revisar continuamente la efectividad de las actividades de gestión de riesgos.

Este estándar de análisis de riesgos se basa en métodos de evaluación estadísticos y matemáticos para evaluar y clasificar los riesgos, y tiene en cuenta las consecuencias financieras.

c. ISO 22301

ISO 22301 es un estándar internacional que proporciona los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la continuidad del negocio (SGCN). El estándar ayuda a las organizaciones a prepararse, responder y recuperarse de incidentes disruptivos, como desastres naturales, ciberataques o pandemias. ISO 22301 enfatiza un enfoque proactivo para la continuidad del negocio, lo que permite a las organizaciones minimizar el impacto de las interrupciones y garantizar la entrega

continua de productos y servicios. Fomenta una cultura de mejora continua y la adopción de un sistema de gestión reconocido internacionalmente (Estall, 2012)

Los principios básicos de ISO 22301 incluyen (ISO 22301:2019, 2025):

- Contexto de la organización: Comprender el entorno operativo de la organización e identificar posibles interrupciones.
- Liderazgo: Establecer un compromiso claro con la continuidad del negocio por parte de la alta dirección.
- Planificación: Desarrollar e implementar un plan de continuidad del negocio que describa los procedimientos para responder y recuperarse de incidentes disruptivos.
- Soporte: Proporcionar los recursos y la infraestructura necesarios para respaldar los esfuerzos de continuidad del negocio.
- Operación: Implementar y mantener el SGCN, incluida la realización de ejercicios y pruebas periódicas.
- Evaluación del desempeño: Monitorear y medir la efectividad del SGCN.
- Mejora: Mejorar continuamente el SGCN en función de las evaluaciones de desempeño y las lecciones aprendidas.

d. Controles CIS

Los Controles CIS son un conjunto priorizado de mejores prácticas de ciberseguridad desarrolladas por el Centro para la Seguridad de Internet (CIS). Los controles están diseñados para ayudar a las organizaciones a defenderse de los ciberataques más comunes y generalizados. Proporcionan una hoja de ruta clara y procesable para mejorar la postura de ciberseguridad, centrándose en medidas de seguridad esenciales que se pueden implementar con recursos limitados. Los Controles CIS son importantes porque minimizan el riesgo de violaciones de datos, fugas de datos, robo de propiedad intelectual, espionaje corporativo, pérdida de privacidad, denegación de servicio (DoS) y otras ciberamenazas. Al implementar los Controles CIS, las organizaciones pueden minimizar la cantidad de posibles puntos de entrada para los ciberatacantes, reduciendo así la superficie de ataque (Shamma, 2018).

En su versión 7.1 los Controles CIS están organizados en tres Grupos de Implementación (IG) (CIS Critical Security Controls v7.1, 2021):

- IG1: Este grupo incluye 56 controles fundamentales que representan la higiene cibernética esencial. Son adecuados para empresas pequeñas y medianas con recursos limitados y una tolerancia baja a tiempos de inactividad³. Estos controles cubren aspectos básicos como la gestión de activos, la protección de datos y la gestión de cuentas.
- IG2: Este grupo agrega 74 controles adicionales que abordan la complejidad operativa y requieren tecnología de nivel empresarial y experiencia especializada. Es adecuado para empresas que manejan información sensible y pueden soportar interrupciones cortas de servicio.
- IG3: Este grupo incluye todos los controles de los grupos anteriores más controles adicionales para proteger contra amenazas avanzadas. Es ideal para grandes organizaciones con múltiples departamentos y altos niveles de riesgo

Esta estructura escalonada permite a las organizaciones adaptar su implementación en función de sus recursos y perfil de riesgo. Por ejemplo, una pequeña empresa con recursos limitados podría comenzar con los controles IG1, mientras que una organización más grande con un programa de seguridad más maduro podría implementar los controles IG2 o IG3.

3. Metodologías de Mejora Continua

a. Six Sigma

Es una metodología basada en datos que se centra en mejorar la eficiencia de los procesos y reducir los defectos. Su objetivo es alcanzar un nivel de calidad casi perfecto, con solo 3.4 defectos por millón de oportunidades. Six Sigma utiliza un enfoque estructurado llamado DMAIC (Definir, Medir, Analizar, Mejorar, Controlar) para identificar y eliminar las causas de variación y mejorar los procesos. Mejora la satisfacción

del cliente al reducir y eliminar la variación del proceso que puede conducir a defectos y/o errores (Agrawal, 2024). Las cinco fases de DMAIC son:

- Definir: Definir el problema o la oportunidad de mejora.
- Medir: Medir el rendimiento actual del proceso.
- Analizar: Analizar los datos para identificar las causas raíz del problema.
- Mejorar: Implementar soluciones para abordar las causas raíz.
- Controlar: Controlar el proceso mejorado para asegurar que las ganancias se mantengan.

Aplicar Six Sigma a la gestión de la seguridad de la información puede ayudar a las organizaciones a:

- Identificar y mitigar riesgos de forma proactiva: Al analizar los procesos de seguridad, las organizaciones pueden identificar posibles vulnerabilidades e implementar controles para mitigar los riesgos.
- Reducir errores e ineficiencias: Six Sigma puede ayudar a optimizar las operaciones de seguridad y reducir el error humano, lo que lleva a mejores resultados de seguridad.
- Fomentar una cultura de mejora continua: Al enfatizar la toma de decisiones basada en datos y el monitoreo continuo, Six Sigma promueve un enfoque proactivo para la gestión de la seguridad.

b. Lean

La metodología Lean se centra en maximizar el valor para el cliente mientras se minimiza el desperdicio. Su objetivo es crear procesos eficientes y optimizados mediante la identificación y eliminación de actividades que no agregan valor. Los principios Lean se pueden aplicar a varios aspectos de la gestión de la seguridad de la información, incluida la respuesta a incidentes, la evaluación de riesgos y la capacitación en concienciación sobre seguridad. Los dos pilares principales del pensamiento Lean son la mejora continua y el respeto por las personas. La metodología Lean evolucionó a partir del Sistema de

Producción Toyota, que se desarrolló después de la Segunda Guerra Mundial para mejorar la eficiencia y la flexibilidad de la fabricación (Millard , 2023).

Algunos de los principios clave de Lean incluyen:

- Valor: Definir el valor desde la perspectiva del cliente.
- Flujo de valor: Identificar todos los pasos en un proceso y eliminar aquellos que no agregan valor.
- Flujo: Asegurar que el trabajo fluya sin problemas a través del proceso sin interrupciones.
- Extracción: Producir solo lo que se necesita, cuando se necesita.
- Perfección: Esforzarse continuamente por la perfección eliminando el desperdicio y mejorando la eficiencia.

Aplicar Lean a la gestión de la seguridad de la información puede ayudar a las organizaciones a:

- Optimizar los procesos de seguridad: Al eliminar pasos innecesarios y redundancias, las organizaciones pueden mejorar la eficiencia de sus operaciones de seguridad.
- Optimizar la asignación de recursos: Lean ayuda a las organizaciones a identificar y eliminar el desperdicio, liberando recursos que se pueden utilizar para iniciativas de seguridad más críticas.
- Mejorar la respuesta a incidentes: Al aplicar los principios Lean a los procesos de respuesta a incidentes, las organizaciones pueden reducir los tiempos de respuesta y minimizar el impacto de los incidentes de seguridad.

c. Ciclo PDCA

El ciclo PDCA (Planificar-Hacer-Verificar-Actuar) es un método de gestión iterativo de cuatro pasos que se utiliza para el control y la mejora continua de procesos y productos. Es una herramienta simple pero poderosa que se puede aplicar a varios aspectos de la gestión de la seguridad de la información. El concepto de PDCA se basa en el método científico,

enfaticando un enfoque sistemático e iterativo para la resolución de problemas y la mejora. PDCA es la base de la mejora continua o kaizen (SYDLE, 2021).

Los cuatro pasos del ciclo PDCA son:

- Planificar: Establecer los objetivos y procesos necesarios para entregar resultados de acuerdo con el resultado esperado.
- Hacer: Implementar el plan, ejecutar el proceso y hacer el producto.
- Verificar: Estudiar los resultados reales (medidos y recopilados) y compararlos con los resultados esperados (objetivos o metas) para determinar cualquier diferencia.
- Actuar: Solicitar acciones correctivas sobre diferencias significativas entre los resultados reales y los planificados. Analizar las diferencias para determinar sus causas raíz.

Aplicar PDCA a la gestión de la seguridad de la información puede ayudar a las organizaciones a:

- Mejorar continuamente los procesos de seguridad: Al revisar y ajustar regularmente las medidas de seguridad, las organizaciones pueden garantizar que sigan siendo efectivas y estén alineadas con los objetivos comerciales.
- Mejorar la gestión de riesgos: PDCA se puede utilizar para identificar, evaluar y tratar los riesgos de seguridad de la información de una manera sistemática e iterativa.
- Promover una cultura de seguridad proactiva: Al fomentar el monitoreo y la mejora continuos, PDCA ayuda a las organizaciones a crear una cultura de gestión de seguridad proactiva.

d. Integración de Ciclo PDCA con Estándares Internacionales

El ciclo PDCA se puede integrar con estándares internacionales como ISO/IEC 27001 e ISO 22301 para promover la mejora continua del SGSI y el SGCN. Por ejemplo, las organizaciones pueden usar PDCA para:

- Revisar y actualizar periódicamente las políticas y procedimientos de seguridad: La fase de Planificación se puede utilizar para revisar y actualizar las políticas y procedimientos de seguridad para garantizar que sigan siendo relevantes y efectivos.
- Realizar auditorías y evaluaciones de seguridad periódicas: Las fases de Hacer y Verificar se llevan a cabo mediante auditorías y evaluaciones de seguridad periódicas para identificar vulnerabilidades y áreas de mejora.
- Implementar acciones correctivas para abordar las debilidades identificadas: La fase de Actuar se puede utilizar para implementar acciones correctivas para abordar las debilidades identificadas y mejorar la postura general de seguridad.

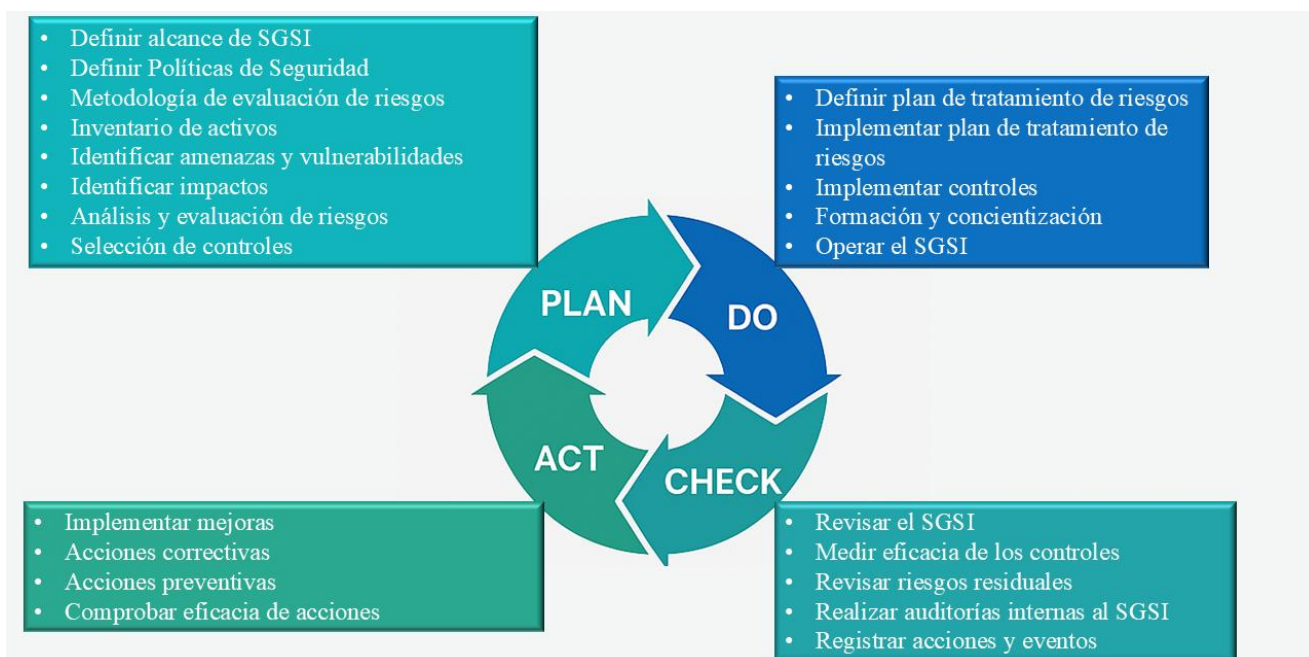


Ilustración 2 Ciclo PDCA aplicado a ISO 27001. Fuente: Elaboración propia.

Capítulo V: Desarrollo

2. Diseño del Sistema de Gestión de Seguridad de la Información para una empresa portuaria de Chile

Para iniciar con la identificación de activos, áreas y procesos bajo el SGSI se realiza el levantamiento de información con las gerencias y jefaturas de la organización, el estudio de la documentación oficial e interna y demás fuentes de información de la empresa, como sistemas de gestión e inventario.

a. Identificación de Activos de Información

Como primera etapa del diseño de un SGSI se lleva a cabo este proceso con el fin de determinar qué información necesita protección y qué recursos son necesarios para garantizar su seguridad.

Para iniciar, se establece la siguiente definición de **Activo de Información**:

Activo de Información: Elemento de tipo físico o digital que compone o contiene información que es de valor para la organización y que es generada, procesada y/o recibida en un área organizacional para el desarrollo de sus funciones.

A partir de esta definición se identifican los siguientes tipos de activos de información:

- **De Infraestructura Informática:** Servidores y bases de datos que componen los distintos sistemas informáticos dentro de la organización.
- **Documentos Físicos:** Contratos, informes impresos, y otros documentos en papel que contienen información de valor.
- **Dispositivos Informáticos:** Computadoras, tabletas, celulares y dispositivos de almacenamiento que son utilizados por los usuarios.
- **De Infraestructura de Red:** Routers, switches, firewalls, y otros componentes de la red que facilitan la transmisión de datos.

Tipo	Activos
De Infraestructura Informática.	Servidores virtuales de bases de datos.
De Infraestructura Informática.	Servidores virtuales de aplicaciones.
De Infraestructura Informática.	Servidores virtuales de respaldo.
De Infraestructura Informática.	Servidores físicos de almacenamiento y distribución de información.
De Infraestructura Informática.	Servidores físicos de respaldo.
Documentos Físicos.	Contratos con proveedores sobre acuerdos de servicio, detalles de términos y condiciones, precios y tarifas negociadas.
Documentos Físicos.	Contratos con Clientes. Contratos de venta y servicio. Condiciones de pago. Información de contacto y datos personales.
Documentos Físicos.	Informes financieros y contables. Informes de auditoría interna. Informes de rendimiento y evaluaciones de proyectos. Informes y datos de empleados.
Documentos Físicos.	Políticas y Procedimientos de la Empresa. Manuales de políticas corporativas. Procedimientos operativos estándar (SOP). Protocolos de seguridad y respuesta a incidentes.
Documentos Físicos.	Documentación Legal. Patentes y licencias. Documentación de litigios y disputas legales. Actas de reuniones y decisiones del consejo directivo.
Documentos Físicos.	Planes de negocio y estrategias de crecimiento. Proyecciones financieras y estudios de viabilidad. Análisis de mercado y estudios de competencia.
Documentos Físicos.	Diagramas de Gantt y cronogramas de proyecto. Especificaciones técnicas y hojas de requisitos. Actas de reuniones de proyectos y asignaciones de tareas.
Dispositivos Informáticos.	Computadores de escritorio para usuarios.
Dispositivos Informáticos.	Computadores de escritorio para tareas de monitoreo y medición.
Dispositivos Informáticos.	Notebooks de usuarios. Notebooks de usuarios administradores.
Dispositivos Informáticos.	Notebooks de respaldo y contingencia. Notebooks para pruebas.
Dispositivos Informáticos.	Tablets de usuarios.
Dispositivos Informáticos.	Tablets de operaciones.
Dispositivos Informáticos.	Handheld para operaciones.
Dispositivos Informáticos.	Smartphones de usuarios.

Dispositivos Informáticos.	Impresoras red.
Dispositivos Informáticos.	Dispositivos de almacenamiento externo de usuarios.
Dispositivos Informáticos.	Discos externos.
De Infraestructura de Red.	Switches.
De Infraestructura de Red.	Puntos de acceso para red inalámbrica.
De Infraestructura de Red.	Firewalls físicos.
De Infraestructura de Red.	Firewalls virtuales.

Tabla 1 Tipos de activos de información. Fuente: Elaboración propia.

b. Identificación de áreas y procesos de la organización

Junto con la identificación de activos de información, la determinación de las áreas de la organización que estarán bajo el SGSI permite establecer un marco claro y conciso para la implementación y gestión del sistema, considerando que la empresa opera las 24 horas continuas y su principal carga de transferencia son contenedores.

Esta identificación incluye departamentos, procesos, y sistemas tecnológicos. A continuación, se detallan las áreas del terminal portuario que deben ser cubiertas por un SGSI, con énfasis en el uso de información y sistemas críticos:

- **Área de Operaciones:** Esta área se encarga de gestionar las actividades relacionadas con el movimiento de carga en el puerto. Para esto hace uso de sistemas de gestión de la carga en el terminal, software y aplicaciones para la planificación y control de las operaciones de carga y descarga, además equipos críticos como dispositivos y maquinaria utilizados en las operaciones, manejando datos operativos como la información sobre horarios, rutas, y estado de las cargas. La protección de estos sistemas y datos es crucial para garantizar la continuidad y eficiencia de las operaciones portuarias.
- **Área de Administración y Finanzas:** Responsable de la gestión financiera y contable de la empresa portuaria. Hace uso de sistemas para la gestión de contabilidad, presupuestos, y finanzas, manejando datos financieros, información sobre transacciones financieras, reportes contables, y análisis financieros, además de registros de todas las transacciones económicas de la empresa. La seguridad de estos sistemas es esencial para proteger la integridad financiera y prevenir fraudes.

- **Área de Recursos Humanos:** Gestiona la información y los sistemas relacionados con el personal de la empresa portuaria para el manejo de la nómina, contrataciones, evaluaciones del desempeño y asignación de recursos humanos para la operación portuaria. Administra información sensible de los trabajadores, como datos personales, históricos laborales, y datos de salud, junto con los registros de nómina que incluyen información sobre salarios, beneficios, y otros pagos. Proteger la información sensible de los empleados es vital para cumplir con las normativas de privacidad y mantener la confianza del personal.
- **Área Comercial:** Encargada de gestionar las relaciones comerciales y la información de los clientes. Requiere el uso de sistemas para el seguimiento y gestión de relaciones con clientes, en los que se manejan información de contacto, contratos, y registros de transacciones con éstos, además de sistemas de facturación y ventas para la gestión de éstas. La seguridad de estos sistemas y datos es fundamental para mantener la confianza de los clientes y asegurar la continuidad de las operaciones comerciales.

Se incluye además dentro del alcance del SGSI el área de informática, diferenciándose de las otras áreas por su enfoque técnico más que funcional en cuanto al uso de información y sistemas críticos:

- **Área de Informática:** Se encarga de la gestión de los sistemas informáticos de la empresa portuaria. Abarcando desde procesos de desarrollo y mantenimiento de aplicaciones y sistemas utilizados en la organización, hasta administración de equipos y dispositivos informáticos y de comunicaciones, gestión de servidores, almacenamiento de datos, y bases de datos críticas para las operaciones. La seguridad de esta infraestructura informática es esencial para el funcionamiento continuo y seguro de todos los sistemas tecnológicos y la protección contra amenazas cibernéticas.

Se identifican áreas y procesos críticos de información, junto con los sistemas relacionados:

Área(s)	Proceso	Sistema
Operaciones y Comercial.	Revisión de contenedores que ingresan y salen del terminal, inspección física y verificación de documentación.	Sistema de Operación del Terminal.
Operaciones.	Registro y monitoreo de entrada y salida de contenedores. Asignación de espacio en terminal.	Sistema de Operación del Terminal.
Operaciones.	Conocimiento de embarque de transportista durante exportación.	Sistema de Operación del Terminal.
Operaciones y Comercial.	Creación, actualización y asignación de unidades (contenedores, vehículos).	Sistema de Operación del Terminal.
Operaciones y Comercial.	Grabación de eventos y actividades en contenedores.	Sistema de Operación del Terminal.
Operaciones y Comercial.	Creación, actualización y monitoreo de buques.	Sistema de Operación del Terminal.
Operaciones y Comercial.	Creación, actualización y notificación de las rotaciones de buques que llegan al puerto.	Sistema de Operación del Terminal.
Operaciones y Comercial.	Planificación y coordinación de las visitas de buques al puerto.	Sistema de Planificación y Control de Buques.
Operaciones.	Planificación y ejecución de operaciones de carga y descarga de contenedores.	Sistema de Planificación y Control de las Operaciones de Carga y Descarga.
Recursos Humanos.	Registro de ingreso y salida de trabajadores portuarios, y envío a Dirección del Trabajo.	Sistema de Control de Cumplimiento de la Normativa Laboral Portuaria.
Recursos Humanos.	Planificación, asignación y citación de trabajadores portuarios.	Sistema de Asignación de Recursos Humanos.
Recursos Humanos.	Pago de remuneraciones.	Sistema de Gestión de Personas.
Operaciones.	Acceso de personal autorizado a zona operativa.	Sistema de Control de Acceso.
Comercial.	Generación y descarga de manifiesto de carga para Aduana.	Sistema de Manifiesto de Aduana.
Comercial.	Reporte y publicación a clientes sobre mercancías procesadas y entregas de manera eficiente.	Sistema Web de Transacciones.
Comercial y Finanzas.	Generación de contratos y tarifas.	Sistema de Facturación de Servicios del Terminal.
Comercial y Finanzas.	Creación, provisión y facturación de documentos de cobro a clientes.	Sistema de Facturación de Servicios del Terminal.
Finanzas.	Pagos de facturas.	Sistema Web de Transacciones.
Comercial.	Entrega de información a Agencias de aduana.	Sistema Web de Transacciones.
Informática.	Compartición digital de la información dentro de la red interna de la organización.	Sistema de Almacenamiento Conectado a la Red.

Tabla 2 Áreas, procesos y sistemas críticos. Fuente: Elaboración propia.

c. Clasificación de riesgos

Una vez identificadas las áreas, procesos y sistemas, se deben clasificar los activos de información según su nivel de criticidad en la operación. Esto ayuda a priorizar los esfuerzos de protección y orientar la definición de los controles de seguridad a implementar. Un activo de información puede ser de criticidad Alta, Media o Baja:

- **Alta:** Aquellos cuya pérdida o compromiso tendría un impacto significativo en la continuidad operacional de la empresa. Forman parte fundamental de los procesos críticos de la organización.
- **Media:** Activos importantes para las operaciones diarias, pero cuya pérdida no paralizaría los procesos críticos de la empresa.
- **Baja:** Activos cuyo impacto en caso de pérdida o compromiso sería limitado y no genera impacto directo en las operaciones de la organización. No tienen influencia en los procesos críticos.

La identificación de procesos y sistemas críticos permite diferenciar los servidores que pertenecen a estos, obteniendo en total la siguiente información:

Tipo	Activos	Criticidad
De Infraestructura Informática.	Servidores virtuales de bases de datos de sistemas críticos.	Alta.
De Infraestructura Informática.	Servidores virtuales de bases de datos de sistemas no críticos.	Media.
De Infraestructura Informática.	Servidores virtuales de aplicaciones de sistemas críticos.	Alta.
De Infraestructura Informática.	Servidores virtuales de aplicaciones de sistemas no críticos.	Media.
De Infraestructura Informática.	Servidores virtuales de respaldo.	Baja.
De Infraestructura Informática.	Servidores físicos de almacenamiento y distribución de información.	Alta.
De Infraestructura Informática.	Servidores físicos de respaldo.	Baja.
Documentos Físicos.	Contratos con proveedores sobre acuerdos de servicio, detalles de términos y condiciones, precios y tarifas negociadas.	Alta.
Documentos Físicos.	Contratos con Clientes. Contratos de venta y servicio. Condiciones de pago. Información de contacto y datos personales.	Alta.
Documentos Físicos.	Informes financieros y contables. Informes de auditoría interna. Informes de rendimiento y evaluaciones de proyectos.	Alta.

	Informes y datos de empleados.	
Documentos Físicos.	Políticas y Procedimientos de la Empresa. Manuales de políticas corporativas. Procedimientos operativos estándar (SOP). Protocolos de seguridad y respuesta a incidentes.	Media.
Documentos Físicos.	Documentación Legal. Patentes y licencias. Documentación de litigios y disputas legales. Actas de reuniones y decisiones del consejo directivo.	Alta.
Documentos Físicos.	Planes de negocio y estrategias de crecimiento. Proyecciones financieras y estudios de viabilidad. Análisis de mercado y estudios de competencia.	Alta.
Documentos Físicos.	Diagramas de Gantt y cronogramas de proyecto. Especificaciones técnicas y hojas de requisitos. Actas de reuniones de proyectos y asignaciones de tareas.	Alta.
Dispositivos Informáticos.	Computadores de escritorio para usuarios.	Alta.
Dispositivos Informáticos.	Computadores de escritorio para tareas de monitoreo y medición.	Media.
Dispositivos Informáticos.	Notebooks de usuarios. Notebooks de usuarios administradores.	Alta.
Dispositivos Informáticos.	Notebooks de respaldo y contingencia. Notebooks para pruebas.	Media.
Dispositivos Informáticos.	Tablets de usuarios.	Media.
Dispositivos Informáticos.	Tablets de operaciones.	Alta.
Dispositivos Informáticos.	Handheld para operaciones.	Media.
Dispositivos Informáticos.	Smartphones de usuarios.	Media.
Dispositivos Informáticos.	Impresoras red.	Baja.
Dispositivos Informáticos.	Dispositivos de almacenamiento externo de usuarios.	Baja.
Dispositivos Informáticos.	Discos externos.	Baja.
De Infraestructura de Red.	Switches.	Alta.
De Infraestructura de Red.	Puntos de acceso para red inalámbrica.	Media.
De Infraestructura de Red.	Firewalls físicos.	Alta.
De Infraestructura de Red.	Firewalls virtuales.	Alta.

Tabla 3 Criticidad de activos de información. Fuente: Elaboración propia.

Junto con esta clasificación de los activos de información, se identifican las amenazas potenciales y las vulnerabilidades asociadas a estos, junto con determinar la probabilidad de que ocurra cada amenaza identificada (frecuencia muy baja, baja, media, alta y muy alta) y evaluar el impacto potencial de cada amenaza de los activos de información en la operación de la empresa portuaria (impacto bajo, moderado, alto, crítico y catastrófico).

- **Amenazas Comunes:** Ciberataques, accesos no autorizados, desastres naturales, fallos en sistemas críticos.
- **Vulnerabilidades:** Debilidades en la infraestructura de TI, falta de capacitación en seguridad, dependencia de proveedores externos.

Activos	Vulnerabilidad	Amenaza	Probabilidad	Impacto
Servidores virtuales de bases de datos de sistemas críticos.	Debilidad en infraestructura TI.	Denegación de servicio por ciberataque.	Muy Baja.	Catastrófico.
Servidores virtuales de bases de datos de sistemas críticos.	Dependencia de proveedores externos.	Fallos en sistemas críticos.	Media.	Crítico.
Servidores virtuales de bases de datos de sistemas no críticos.	Debilidad en infraestructura TI.	Denegación de servicio por ciberataque.	Muy Baja.	Alto.
Servidores virtuales de aplicaciones de sistemas críticos.	Debilidad en infraestructura TI.	Denegación de servicio por ciberataque.	Muy Baja.	Catastrófico.
Servidores virtuales de aplicaciones de sistemas críticos.	Dependencia de proveedores externos.	Fallos en sistemas críticos.	Media.	Crítico.
Servidores virtuales de aplicaciones de sistemas no críticos.	Debilidad en infraestructura TI.	Denegación de servicio por ciberataque.	Muy Baja.	Moderado.
Servidores virtuales de respaldo.	Debilidad en infraestructura TI.	Denegación de servicio por ciberataque.	Muy Baja.	Bajo.
Servidores físicos de almacenamiento y distribución de información.	Debilidad en infraestructura TI.	Denegación de servicio por ciberataque.	Muy Baja.	Catastrófico.
Servidores físicos de almacenamiento y distribución de información.	Debilidad en infraestructura TI.	Destrucción de activo por desastre natural.	Muy Baja.	Catastrófico.
Servidores físicos de respaldo.	Debilidad en infraestructura TI.	Denegación de servicio por ciberataque.	Muy Baja.	Bajo.
Servidores físicos de respaldo.	Debilidad en infraestructura TI.	Destrucción de activo por desastre natural.	Muy Baja.	Bajo.
Contratos con proveedores sobre acuerdos de servicio, detalles de términos y condiciones, precios y tarifas negociadas.	Falta de capacitación en seguridad.	Destrucción de copia única por desastre natural.	Muy Baja.	Catastrófico.
Contratos con Clientes. Contratos de venta y servicio. Condiciones de pago. Información de contacto y datos personales.	Falta de capacitación en seguridad.	Destrucción de copia única por desastre natural.	Muy Baja.	Catastrófico.
Informes financieros y contables. Informes de auditoría interna. Informes de rendimiento y evaluaciones de proyectos.	Falta de capacitación en seguridad.	Destrucción de copia única por desastre natural.	Muy Baja.	Catastrófico.

Informes y datos de empleados.				
Políticas y procedimientos de la empresa. Manuales de políticas corporativas. Procedimientos operativos estándar (SOP). Protocolos de seguridad y respuesta a incidentes.	Falta de capacitación en seguridad.	Destrucción de copia única por desastre natural.	Muy Baja.	Alto.
Documentación Legal. Patentes y licencias. Documentación de litigios y disputas legales. Actas de reuniones y decisiones del consejo directivo.	Falta de capacitación en seguridad.	Destrucción de copia única por desastre natural.	Muy Baja.	Catastrófico.
Planes de negocio y estrategias de crecimiento. Proyecciones financieras y estudios de viabilidad. Análisis de mercado y estudios de competencia.	Falta de capacitación en seguridad.	Destrucción de copia única por desastre natural.	Muy Baja.	Catastrófico.
Diagramas de Gantt y cronogramas de proyecto. Especificaciones técnicas y hojas de requisitos. Actas de reuniones de proyectos y asignaciones de tareas.	Falta de capacitación en seguridad.	Destrucción de copia única por desastre natural.	Muy Baja.	Catastrófico.
Computadores de escritorio para usuarios.	Debilidad en infraestructura TI.	Infección de equipo por código malicioso.	Media.	Alto.
Computadores de escritorio para usuarios.	Falta de capacitación en seguridad.	Accesos no autorizados a red interna.	Baja.	Crítico.
Computadores de escritorio para tareas de monitoreo y medición.	Debilidad en infraestructura TI.	Infección de equipo por código malicioso.	Baja.	Moderado.
Notebooks de usuarios. Notebooks de usuarios administradores.	Debilidad en infraestructura TI.	Infección de equipo por código malicioso.	Media.	Alto.
Notebooks de usuarios. Notebooks de usuarios administradores.	Falta de capacitación en seguridad.	Accesos no autorizados a red interna.	Baja.	Crítico.
Notebooks de respaldo y contingencia. Notebooks para pruebas.	Debilidad en infraestructura TI.	Infección de equipo por código malicioso.	Muy Baja.	Moderado.
Tablets de usuarios.	Debilidad en infraestructura TI.	Infección de equipo por código malicioso.	Media.	Moderado.
Tablets de usuarios.	Falta de capacitación en seguridad.	Accesos no autorizados a red interna.	Media.	Alto.
Tablets de operaciones.	Debilidad en infraestructura TI.	Infección de equipo por código malicioso.	Baja.	Alto.
Handheld para operaciones.	Debilidad en infraestructura TI.	Infección de equipo por código malicioso.	Baja.	Moderado.
Smartphones de usuarios.	Debilidad en infraestructura TI.	Infección de equipo por código malicioso.	Media.	Moderado.
Smartphones de usuarios.	Falta de capacitación en	Accesos no autorizados	Media.	Alto.

	seguridad.	a red interna.		
Impresoras red.	Debilidad en infraestructura TI.	Infección de equipo por código malicioso.	Baja.	Bajo.
Dispositivos de almacenamiento externo de usuarios.	Falta de capacitación en seguridad.	Infección de equipo por código malicioso.	Media.	Moderado.
Discos externos.	Falta de capacitación en seguridad.	Infección de equipo por código malicioso.	Media.	Alto.
Switches.	Debilidad en infraestructura TI.	Accesos no autorizados a red interna.	Baja.	Crítico.
Switches.	Debilidad en infraestructura TI.	Destrucción de activo por desastre natural.	Muy Baja.	Crítico.
Puntos de acceso para red inalámbrica.	Debilidad en infraestructura TI.	Accesos no autorizados a red interna.	Baja.	Alto.
Firewalls físicos.	Debilidad en infraestructura TI.	Accesos no autorizados a red interna.	Baja.	Crítico.
Firewalls físicos.	Debilidad en infraestructura TI.	Destrucción de activo por desastre natural.	Muy Baja.	Crítico.
Firewalls virtuales.	Debilidad en infraestructura TI.	Accesos no autorizados a red interna.	Baja.	Crítico.

Tabla 4 Probabilidad e impacto de amenazas. Fuente: Elaboración propia

Luego, mediante una matriz de riesgos se clasifican y priorizan los riesgos en función de su probabilidad e impacto.

		Impacto				
		Bajo	Moderado	Alto	Crítico	Catastrófico
		1	2	3	4	5
Probabilidad	Muy baja	2	4	6	8	10
	Baja	4	8	12	16	20
	Media	6	12	18	24	30
	Alta	8	16	24	32	40
	Muy alta	10	20	30	40	50

Tabla 5 Matriz de riesgos. Fuente: Elaboración propia

A partir esta matriz se clasifican los riesgos en categorías según su nivel, con el fin de definir los niveles de riesgo aceptables para la organización, planificar la implementación

de los controles de seguridad y priorizar los riesgos que requieren acciones inmediatas de mitigación.

Puntuación	Nivel de Riesgo	Mitigación
2 a 10	Aceptable	Largo Plazo
12 a 18	Tolerable	Medio Plazo
20 a 24	Intolerable	Corto Plazo
30 a 50	Extremo	Inmediata

Tabla 6 Nivel de riesgo y mitigación de riesgos evaluados. Fuente: Elaboración propia

d. Selección de controles de seguridad

Para gestionar los riesgos identificados la organización se basa en las mejores prácticas establecidas por la norma ISO 27001, la cual incluye 114 controles de seguridad agrupados en cuatro categorías: organizacionales, de personas, físicos y tecnológicos. Esta categorización orienta a la empresa en la selección de los controles y su posterior aplicación en función de la evaluación de riesgos realizada.

Los controles ISO se seleccionan considerando las siguientes características de la empresa:

- Empresa no cuenta con prácticas definidas para la seguridad de su información, ni con un área o personal para su organización, administración o gestión de los riesgos asociados a la información.
- Procesos críticos son totalmente dependientes de distintos sistemas informáticos, no pudiendo desarrollarse ante la indisponibilidad de estos servicios
- Infraestructura de estos sistemas informáticos está expuesta a vulnerabilidades tecnológicas, accesos no autorizados y fallas en la continuidad operacional, por lo que debe ser monitoreada y actualizada constantemente.
- La operación continua del terminal portuario, durante 24 horas al día los 7 días de la semana, requiere de una infraestructura informática robusta, que garantice su correcto funcionamiento de forma constante.

Control	Objetivo de Control	Subcontroles
6 – Organización de la seguridad de la información.	6.1 Organización Interna. 6.2 Dispositivos para movilidad y teletrabajo.	6.1.1 Funciones y responsabilidades de la Seguridad de la información. 6.1.2 Separación de funciones. 6.1.3 Contacto con autoridades. 6.1.4 Contacto con grupos de interés especial. 6.1.5 Seguridad de la información en la gestión de proyectos. 6.2.1 Política de dispositivos móviles. 6.2.2 Teletrabajo.
8 – Gestión de activos.	8.1 Responsabilidad de los activos. 8.2 Clasificación de la información. 8.3 Manipulación de soportes.	8.1.1 Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos. 8.1.4 Devolución de activos. 8.2.1 Clasificación de la información. 8.2.2 Etiquetado de la información. 8.2.3 Manejo de los activos. 8.3.1 Gestión de soportes extraíbles. 8.3.2 Eliminación de soportes. 8.3.3 Traslado de soportes físicos.
9 - Control de acceso.	9.1 Requisitos de negocio para el control de acceso. 9.2 Gestión del acceso de usuarios. 9.3 Responsabilidades del usuario. 9.4 Control de acceso al sistema y a las aplicaciones.	9.1.1 Política de control de acceso. 9.1.2 Acceso a las redes y a los servicios de red. 9.2.1 Registro de usuarios y cancelación del registro. 9.2.2 Gestión de acceso a los usuarios. 9.2.3 Gestión de derechos de acceso privilegiados. 9.2.4 Gestión de la información de autenticación secreta de los usuarios. 9.2.5 Revisión de derechos de acceso de usuario. 9.2.6 Remoción o ajuste de los derechos de acceso. 9.3.1 Uso de la información de autenticación secreta. 9.4.1 Restricción de acceso a la información. 9.4.2 Procedimientos de conexión (log-on) seguros. 9.4.3 Sistema de gestión de contraseñas. 9.4.4 Uso de programas de utilidad privilegiados. 9.4.5 Control de acceso al código de programas fuente.
10 – Criptografía.	10.1 Controles criptográficos.	10.1.1 Política sobre el empleo de controles criptográficos. 10.1.2 Gestión de claves.
12 - Seguridad de las operaciones.	12.1 Procedimientos operacionales y responsabilidades. 12.2 Protección ante software malicioso. 12.3 Respaldo. 12.4 Registros y supervisión.	12.1.1 Procedimientos documentados de operación. 12.1.2 Gestión de cambios. 12.1.3 Gestión de la capacidad. 12.1.4 Separación de los ambientes para desarrollo, prueba y operación. 12.2.1 Controles ante software malicioso. 12.3.1 Respaldo de la información. 12.4.1 Registro de eventos.

	12.5 Control de software en la producción. 12.6 Gestión de vulnerabilidad técnica. 12.7 Consideraciones sobre la auditoría de sistemas de información.	12.4.2 Protección de la información de registros (logs). 12.4.3 Registros del administrador y operador. 12.4.4 Sincronización de relojes. 12.5.1 Instalación de software en los sistemas operativos. 12.6.1 Gestión de vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7.1 Controles de auditoría de sistemas de información.
13 - Seguridad en las comunicaciones.	13.1 Gestión de la seguridad de red. 13.2 Intercambio de información.	13.1.1 Controles de red. 13.1.2 Seguridad de los servicios de red. 13.1.3 Separación en redes. 13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio de información. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y de no divulgación.
14 - Adquisición, desarrollo y mantenimiento de los sistemas de información.	14.1 Requisitos de seguridad de los Sistemas de información. 14.2 Seguridad den los procesos de desarrollo y soporte. 14.3 Datos de prueba.	14.1.1 Análisis y especificación de los requisitos de seguridad. 14.1.2 Aseguramiento de los servicios de aplicación en las redes públicas. 14.1.3 Transacciones en línea. 14.2.1 Política de desarrollo seguro. 14.2.2 Procedimiento de control de cambio del sistema. 14.2.3 Revisión técnica de aplicaciones después de cambios de las plataformas operativas. 14.2.4 Restricciones a los cambios en los paquetes de software. 14.2.5 Principios de la ingeniería de sistemas seguros. 14.2.6 Ambiente de desarrollo seguro. 14.2.7 Desarrollo subcontratado. 14.2.8 Pruebas de seguridad del sistema. 14.2.9 Pruebas de aceptación del sistema. 14.3.1 Protección de datos de prueba.
15 - Relación con proveedores.	15.1 Seguridad de la información en las relaciones con los proveedores. 15.2 Gestión de la entrega del servicio por terceras partes.	15.1.1 Política de seguridad de la información para las relaciones con los proveedores. 15.1.2 Tener en cuenta la seguridad en los acuerdos con proveedores. 15.1.3 Cadena de suministro de tecnologías de la información y las comunicaciones. 15.2.1 Seguimiento y revisión de los servicios de proveedores. 15.2.2 Gestión de cambios en los servicios de los proveedores.
16 - Gestión de incidentes de la seguridad de la información.	16.1 Gestión de incidentes y mejoras de seguridad de la información.	16.1.1 Responsabilidades y procedimientos. 16.1.2 Reporte de eventos de seguridad de la información. 16.1.3 Reporte de debilidades de seguridad de la información. 16.1.4 Evaluación y decisión sobre los eventos de seguridad de información. 16.1.5 Respuesta a incidentes de seguridad de la información. 16.1.6 Aprendiendo de los incidentes de seguridad de la información. 16.1.7 Recolección de evidencia.

Tabla 7 Selección de controles ISO. Fuente: Elaboración propia con base al contenido de la norma ISO 27001.

Además, la empresa utiliza como referencia los Controles Críticos de Seguridad CIS (CIS Controls), donde la selección de controles debe estar orientada al nivel de Implementación Group (IG) que corresponda a la empresa tras la evaluación de riesgos

Después de realizar la evaluación de riesgos, la empresa determina su nivel de IG basado en su perfil de riesgo y recursos disponibles. Esto permite seleccionar los controles adecuados y priorizar su implementación de acuerdo con las necesidades específicas:

- IG1: Implementar los 56 controles fundamentales para protegerse contra ataques comunes.
- IG2: Agregar los 74 controles adicionales para abordar la complejidad operativa y proteger información sensible.
- IG3: Implementar todos los controles de los grupos anteriores más controles adicionales para proteger contra amenazas avanzadas.

A partir de la evaluación de riesgos, donde los de mayor criticidad son 2 riesgos de nivel Intolerable y 15 Tolerables, se determina el nivel IG2 para la empresa, implicando la selección de los siguientes controles CIS para su implementación dentro de un año:

Control CIS	Controles Seleccionados
1: Inventario de Dispositivos autorizados y no autorizados	1.1 Utilizar una herramienta de descubrimiento activo 1.4 Mantener un inventario de activos detallado 1.5 Mantener la información del inventario de activo 1.6 Gestionar los activos no autorizados
2: Inventario de Software autorizados y no autorizados	2.1 Mantener un inventario de software autorizado 2.2 Asegurar que el software tenga soporte del fabricante 2.3 Utilizar herramientas de inventario de software 2.6 Gestionar el software no aprobado 2.7 Utilizar lista blanca de aplicaciones 2.10 Separar física o lógicamente las aplicaciones de alto riesgo
3: Gestión continua de vulnerabilidades	3.1 Ejecutar herramientas de escaneo automatizados de vulnerabilidades 3.3 Proteger las cuentas dedicadas a auditorías 3.4 Implementar herramientas de gestión automatizada de parches del sistema operativo 3.5 Implementar herramientas de gestión automatizada de parches de software 3.6 Comparar escaneos de vulnerabilidades consecutivos 3.7 Utilizar un proceso de calificación de riesgo

4: Uso controlado de privilegios administrativos	4.1 Mantener un inventario de cuentas administrativas 4.2 Cambiar contraseñas por defecto 4.3 Asegurar el uso de cuentas administrativas dedicadas 4.4 Usar contraseñas únicas 4.5 Usar autenticación multifactor para todoa cceso administrativo 4.6 Usar máquinas dedicadas para toda tarea administrativa 4.7 Limitar el acceso a herramientas de scripts 4.8 Registrar y alertar cambios de miembros en grupos administrativos
CIS Control 5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores	5.1 Establecer configuraciones seguras 5.2 Mantener imágenes seguras
CIS Control 6: Mantenimiento, monitoreo y análisis de logs de auditoria	6.1 Utilizar tres fuentes de tiempo sincronizadas. 6.2 Activar registros de auditoria. 6.3 Habilitar registros detallados. 6.4 Asegurar almacenamiento adecuado para registros. 6.6 Desplegar herramientas SIEM o de Análisis de registros 6.7 Revisar regularmente los registros. 6.8 Ajustar regularmente el SIEM
7: Protección de correo electrónico y navegador web	7.1 Asegurar el uso de navegadores y clientes de correo electrónico que cuenten con soporte 7.2 Deshabilitar plugins innecesarios de navegadores o clientes de correo electrónico 7.4 Mantener y aplicar filtros de URL basados en red 7.5 Suscribirse a servicios de categorización de URL 7.6 Registrar todas las peticiones de URLs 7.7 Utilizar servicios de filtrado DNS 7.8 Implementar DMARC y habilitar verificación del lado del receptor 7.9 Bloquear tipos de archivos innecesarios
8: Defensa contra malware	8.1 Utilizar software antimalware de gestión centralizada 8.2 Asegurar que el software antimalware y las firmas estén actualizadas 8.3 Habilitar características anti-explotación de sistemas operativos / implementar tecnologías anti-explotación 8.4 Configurar escaneo antimalware de dispositivos removibles 8.5 Configurar equipos para no autoejecutar contenido 8.6 Centralizar los registros antimalware 8.7 Habilitar registros de consultas DNS
9: Limitación y control de puertos de red, protocolos y servicios	9.4 Aplicar firewalls basados en host o filtrado de puertos
10: Capacidad de recuperación de datos	10.1 Asegurar los respaldos regulares automatizados 10.2 Realizar respaldos de sistemas completos 10.3 Probar los datos en los medios de respaldo 10.4 Asegurar la protección de las copias de respaldo

	10.5 Asegurar que las copias de respaldo tengan al menos un destino discontinuo
11: Configuración segura de equipos de red, tales como firewalls, switch y router	11.1 Mantener configuraciones de seguridad estandarizadas en equipos de red 11.4 Instalar la última versión estable de cualquier actualización de seguridad en todos los equipos de red
12: Defensa Perimetral	12.1 Mantener un inventario de los bordes de la red 12.3 Denegar comunicaciones con direcciones IPs maliciosas conocidas 12.4 Denegar comunicaciones sobre puertos no autorizados 12.6 Desplegar sensores IDS basados en red 12.9 Desplegar servidor proxy de filtrado de capa de aplicación 12.11 Requerir autenticación multifactor en todos los inicios de sesión remoto
13: Protección de Datos	13.4 Permitir solamente el acceso a proveedores de servicios de nube o correo autorizados 13.6 Cifrar el disco duro de todos los dispositivos móviles 13.7 Gestionar dispositivos USB 13.8 Gestionar las configuraciones de lectura/escritura de sistemas para medios removibles externos
14: Control de acceso basado en la necesidad de conocer protección de datos	14.6 Proteger la información mediante lista de control de acceso
15: Control de acceso inalámbrico	15.1 Mantener un inventario de puntos de acceso inalámbrico autorizados 15.2 Detectar puntos de acceso inalámbricos conectados a la red cableada 15.4 Deshabilitar el acceso inalámbrico en dispositivos si no se requiere 15.6 Inhabilitar las capacidades de red inalámbrica punto a punto en clientes inalámbricos 15.7 Usar estándar de cifrado avanzado (AES) para cifrar datos inalámbricos 15.10 Crear una red inalámbrica separada para dispositivos personales y no confiables
16: Monitoreo y control de cuentas	16.1 Mantener un inventario de sistemas de autenticación 16.2 Configurar un punto de autenticación centralizado 16.3 Requerir Autenticación Multifactor 16.5 Cifrar la transmisión de nombres de usuario y credenciales de autenticación 16.6 Mantener un inventario de cuentas 16.7 Establecer un proceso para revocar el acceso 16.8 Deshabilitar cualquier cuenta no asociada 16.10 Asegurar que todas las cuentas tengan fecha de caducidad 16.11 Bloquear sesiones de estaciones de trabajo tras inactividad
17: Implementar programa de concientización y entrenamiento en seguridad	17.3 Implementar un programa de concienciación de seguridad 17.4 Actualice el contenido de concienciación con frecuencia 17.5 Entrenar a la fuerza laboral en la autenticación segura 17.6 Capacitar a la fuerza laboral en la identificación de ataques de ingeniería social 17.7 Capacitar a la fuerza laboral en manejo de datos sensibles 17.8 Capacitar a la fuerza laboral sobre las causas de la exposición involuntaria a los datos 17.9 Capacite a la fuerza laboral sobre cómo identificar y reportar incidentes

18: Seguridad de software de aplicación	18.9 Sistemas separados de producción y no producción 18.11 Usar plantillas de configuración de hardening estándar para bases de datos
19: Respuesta y manejo de incidentes	19.1 Documentar los procedimientos de respuesta de incidentes 19.2 Asignar cargos y responsabilidades para la respuesta a incidentes 19.3 Designar personal de gestión para apoyar el manejo de incidentes 19.6 Publicar información relacionada con la notificación de anomalías e incidentes informáticos 19.7 Llevar a cabo sesiones periódicas de escenarios de incidentes para el personal
20: Pruebas de penetración y equipo rojo	20.1 Establecer un programa de prueba de penetración 20.2 Llevar a cabo pruebas periódicas de penetración externa e interna 20.6 Usar herramientas de prueba de penetración y exploración de vulnerabilidades en conjunto 20.8 Controlar y monitorear las cuentas asociadas con las pruebas de penetración

Tabla 8 Selección de controles CIS. Fuente: Elaboración propia con base al contenido de los Controles CIS V7.1.

e. Desarrollo de políticas y procedimientos

Una vez establecido el alcance de los controles de seguridad a implementar en la organización, el diseño del SGSI finaliza con el desarrollo de políticas y procedimientos, los cuales proporcionan un marco claro para la gestión de la seguridad de la información, asegurando que todos los miembros de la organización comprendan sus roles y responsabilidades en la protección de los activos de información.

A partir del marco de la de la ISO 27001 se construyen las siguientes políticas:

- Política de Seguridad de la Información
- Política de Control de Acceso
- Política de Gestión de Incidentes
- Política de Gestión de Activos
- Política de Seguridad en Comunicaciones
- Política de Adquisición, Desarrollo y Mantenimiento de Sistemas
- Política de Criptografía
- Política de Seguridad en las Operaciones
- Política de Relación con Proveedores

Las cuales se estructuran de la siguiente forma:

- **Política de Seguridad de la Información**
 - **Objetivo:** Establecer las directrices generales y los principios básicos para la gestión de la seguridad de la información en la organización.
 - **Contenido:**
 - Propósito y Alcance: Describir el propósito de la política y su alcance dentro de la organización.
 - Definiciones Clave: Proporcionar definiciones claras de los términos utilizados.
 - Roles y Responsabilidades: Especificar los roles y responsabilidades de los empleados, la alta dirección, y los terceros en relación con la seguridad de la información.
 - Cumplimiento: Incluir directrices para el cumplimiento con las normativas y estándares aplicables, como ISO 27001 y CIS Controls.
 - Revisión y Actualización: Establecer un procedimiento para la revisión y actualización periódica de las políticas.

- **Política de Control de Acceso**
 - **Objetivo:** Regular el acceso a los sistemas y datos de la organización para garantizar que solo personas autorizadas puedan acceder a información sensible.
 - **Contenido:**
 - Principios de Acceso: Definir los principios de control de acceso, como el acceso basado en roles (RBAC).
 - Gestión de Cuentas: Describir los procedimientos para la creación, modificación y eliminación de cuentas de usuario.
 - Autenticación y Autorización: Especificar los mecanismos de autenticación y autorización, como contraseñas, autenticación multifactor (MFA) y permisos.
 - Monitoreo y Auditoría: Incluir directrices para el monitoreo de accesos y la realización de auditorías periódicas.

- **Política de Gestión de Incidentes**

- **Objetivo:** Establecer un marco para la identificación, notificación, gestión y resolución de incidentes de seguridad de la información.
- **Contenido:**
 - Definición de Incidente: Proporcionar una definición clara de lo que constituye un incidente de seguridad de la información, incluyendo ejemplos de tipos comunes de incidentes.
 - Notificación de Incidentes: Describir el proceso para notificar incidentes de seguridad, incluyendo quién debe ser notificado y cómo, incluyendo canales y herramientas de comunicación.
 - Respuesta a Incidentes: Establecer los pasos a seguir en la respuesta a incidentes, desde la detección hasta la resolución. Definir los roles y responsabilidades del equipo de respuesta a incidentes, incluyendo el líder del equipo y otros miembros clave.
 - Investigación y Análisis: Incluir directrices para la recopilación y preservación de evidencias, análisis de la causa raíz y evaluación del impacto.
 - Documentación del Incidente: Mantener registros detallados de todos los incidentes, incluyendo el contexto, las acciones tomadas y los resultados.
 - Recuperación y Restauración: Describir las medidas para restaurar los sistemas y servicios afectados a su estado normal de operación.
 - Comunicación y Reporte: Desarrollar un formato estándar para los informes de incidentes, incluyendo la información clave que debe ser reportada.
 - Entrenamiento y Concienciación: Incluir programas de formación para asegurar que todo el personal esté familiarizado con la política y los procedimientos de gestión de incidentes. Realizar simulacros regulares de incidentes para evaluar y mejorar la capacidad de respuesta.

- **Política de Gestión de Activos**

- **Objetivo:** Establecer directrices claras para la identificación, clasificación, protección y gestión de los activos de información dentro de la empresa portuaria.
- **Contenido:**
 - Definición de Activos: Incluir una definición clara de lo que constituye un activo de información (datos, hardware, software, personal, infraestructura de red).
 - Identificación y Clasificación de Activos: Describir el proceso para identificar y clasificar todos los activos de información según su importancia y sensibilidad.
 - Inventario de Activos: Mantener un inventario actualizado de todos los activos de información, con detalles sobre su ubicación, propietario y clasificación.
 - Protección de Activos: Definir las medidas de seguridad necesarias para proteger los activos de información contra amenazas y vulnerabilidades.
 - Gestión del Ciclo de Vida: Incluir directrices para la adquisición, uso, mantenimiento y disposición segura de los activos de información

- **Política de Seguridad en Comunicaciones**

- **Objetivo:** Establecer directrices para gestionar y proteger las infraestructuras de telecomunicaciones de la empresa portuaria, garantizando la seguridad y disponibilidad de los sistemas de comunicación y redes.
- **Contenido:**
 - Definición de Infraestructura de Telecomunicaciones: Incluir una definición clara de lo que constituye la infraestructura de telecomunicaciones, como redes LAN, WAN, equipos de comunicación, y servicios de telecomunicaciones.

- Gestión de Redes: Describir los procedimientos para la administración de redes, incluyendo la configuración, monitoreo y mantenimiento de las redes.
 - Seguridad de las Telecomunicaciones: Definir las medidas de seguridad necesarias para proteger las comunicaciones y redes contra accesos no autorizados y ciberataques.
- **Política de Adquisición, Desarrollo y Mantenimiento de Sistemas**
 - **Objetivo:** Definir los lineamientos para asegurar que todos los sistemas y aplicaciones desarrollados o adquiridos por la empresa portuaria cumplan con los requisitos de seguridad de la información desde su inicio hasta su término.
 - **Contenido:**
 - Adquisición de Sistemas: Establecer que todos los sistemas y aplicaciones adquiridos deben cumplir con los requisitos de seguridad de la organización, además de describir los criterios para la evaluación y selección de proveedores de tecnología.
 - Ciclo de Vida de Desarrollo Seguro: Incluir directrices para la incorporación de prácticas de seguridad en todas las fases del ciclo de vida del desarrollo, desde la planificación hasta la implementación.
 - Revisión y Pruebas de Seguridad: Establecer procedimientos para la revisión y pruebas de seguridad de sistemas y aplicaciones antes de su implementación.
 - Mantenimiento de Sistemas: Describir los procedimientos para la gestión de actualizaciones y parches de seguridad.
 - Control de Cambio: Establecer procedimientos para gestionar los cambios en sistemas y aplicaciones de manera controlada y segura.

- **Política de Criptografía**

- **Objetivo:** Establecer directrices para la implementación y gestión de técnicas criptográficas que protejan la confidencialidad, integridad y disponibilidad de la información sensible de la empresa portuaria
- **Contenido:**
 - Requisitos de Criptografía:
 - i. Confidencialidad: Utilizar criptografía para proteger la información sensible contra accesos no autorizados.
 - ii. Integridad: Asegurar que la información no sea alterada durante su almacenamiento o transmisión.
 - iii. Autenticación: Verificar la identidad de usuarios y dispositivos que acceden a la información criptografiada.
 - Selección de Algoritmos Criptográficos: Establecer criterios para la selección de algoritmos criptográficos, asegurando que cumplan con los estándares internacionales (como AES, RSA, SHA-256).
 - Gestión de Claves Criptográficas
 - i. Generación y Almacenamiento de Claves: Describir los procedimientos para la generación, almacenamiento seguro y distribución de claves criptográficas.
 - ii. Rotación de Claves: Incluir directrices para la rotación periódica de claves y la gestión de claves comprometidas.
 - Uso de Certificados Digitales: Describir el uso de certificados digitales para asegurar la autenticidad y la integridad de las comunicaciones y transacciones electrónicas.
 - Implementación y Uso
 - i. Criptografía en Transmisión: Utilizar cifrado durante la transmisión de datos sensibles a través de redes inseguras (como SSL/TLS para comunicaciones web).
 - ii. Criptografía en Reposo: Proteger datos almacenados mediante cifrado en discos duros, bases de datos y dispositivos móviles.

- **Política de Seguridad en las Operaciones**
 - **Objetivo:** Definir los lineamientos para garantizar que las operaciones diarias relacionadas con los sistemas informáticos se realicen de manera segura y eficiente, protegiendo los activos de información y los sistemas críticos de la organización contra amenazas y vulnerabilidades
 - **Contenido:**
 - Protección de Sistemas Críticos
 - i. Monitoreo y Supervisión: Implementar sistemas de monitoreo continuo para detectar y responder a incidentes de seguridad en tiempo real.
 - ii. Seguridad de la Infraestructura: Asegurar que la infraestructura tecnológica y física que soporta las operaciones esté protegida contra amenazas y vulnerabilidades.
 - Gestión de Parches y Actualizaciones de Sistemas: Implementar procedimientos para la instalación regular de parches y actualizaciones de software para corregir vulnerabilidades y mejorar la seguridad.
 - Monitoreo Continuo: Implementar sistemas de monitoreo para detectar y responder a incidentes de seguridad en tiempo real.
 - Protección de Datos
 - i. Seguridad de la Información: Proteger la información almacenada y transmitida mediante el uso de cifrado y otras medidas de seguridad.
 - ii. Copia de Seguridad y Recuperación: Realizar copias de seguridad periódicas y establecer procedimientos de recuperación de datos para garantizar la continuidad del negocio.
 - Auditorías Regulares: Realizar auditorías periódicas para evaluar la efectividad de las medidas de seguridad y el cumplimiento de las políticas.

- **Política de Relación con Proveedores**
 - **Objetivo:** Establecer directrices para la gestión y control de las relaciones con los proveedores de servicios y productos, asegurando que cumplan con los requisitos de seguridad de la información de la empresa portuaria.
 - **Contenido:**
 - Selección de Proveedores
 - i. Criterios de Evaluación: Establecer criterios claros para la evaluación y selección de proveedores, asegurando que cumplan con los requisitos de seguridad y calidad.
 - ii. Proceso de Evaluación: Describir el proceso de evaluación y selección, incluyendo la revisión de capacidades y antecedentes de seguridad del proveedor.
 - Contratación de Proveedores
 - i. Acuerdos de Nivel de Servicio (SLA): Establecer la necesidad de incluir SLAs que especifiquen los requisitos de seguridad y el nivel de servicio esperado.
 - ii. Requisitos de Seguridad: Incluir cláusulas de seguridad en los contratos con los proveedores para asegurar el cumplimiento con las políticas de la organización.
 - Gestión de la Relación con Proveedores
 - i. Monitoreo y Evaluación: Describir los procedimientos para el monitoreo continuo y la evaluación periódica del desempeño de los proveedores.
 - ii. Auditorías de Seguridad: Realizar auditorías de seguridad regulares a los proveedores para asegurar el cumplimiento con los acuerdos contractuales y las normativas de seguridad.
 - Acceso a Información y Sistemas
 - i. Control de Acceso: Establecer directrices para controlar el acceso de los proveedores a la información y sistemas críticos de la organización.

- ii. Revisión de Accesos: Incluir procedimientos para la revisión y revocación de accesos de los proveedores cuando ya no sean necesarios.

Todas las políticas son revisadas por los gerentes de las distintas áreas cuyos procesos se vean afectados y autorizadas por el Gerente General de la empresa. Una vez construidas las políticas, éstas se utilizan como guía para el desarrollo de los procedimientos, junto con el marco de referencia de los controles CIS.

Los procedimientos por desarrollar abordan los controles CIS requeridos según el nivel de IG2 evaluado de la empresa y se configuran de la siguiente forma:

- **Objetivo**

- Descripción: Define el propósito del procedimiento y los resultados esperados.
- Ejemplo: *Garantizar la seguridad de los sistemas informáticos mediante la implementación de controles de acceso adecuados.*

- **Alcance**

- Descripción: Indica a quiénes y a qué áreas se aplica el procedimiento. Indica los controles de seguridad abordados en el procedimiento.
- Ejemplo: *Este procedimiento se aplica a todos los empleados y sistemas informáticos de la organización. Aborda los controles CIS 14: Control de acceso basado en la necesidad de conocer*

- **Definiciones Generales**

- Descripción: Proporciona definiciones claras de términos técnicos y específicos utilizados en el procedimiento.
- Ejemplo:
 - *Control de Acceso: Medidas para garantizar que solo las personas autorizadas puedan acceder a los sistemas y datos.*
 - *Autenticación: Proceso de verificar la identidad de un usuario.*

- **Responsables**

- Descripción: Designación de roles y responsabilidades específicas para la implementación y mantenimiento del procedimiento.
- Ejemplo:
 - *Administrador de TI: Responsable de la implementación y mantenimiento del control de acceso.*
 - *Usuario Final: Debe seguir las directrices del procedimiento para acceder a los sistemas.*
 - *Auditor de Seguridad: Realiza revisiones periódicas para asegurar el cumplimiento del procedimiento.*

- **Procedimiento Paso a Paso**

- Descripción: Detalla las acciones que deben realizarse, en orden secuencial, para llevar a cabo el procedimiento.
- Ejemplo:
 - *Identificación de Usuario: El usuario ingresa sus credenciales.*
 - *Verificación de Credenciales: El sistema verifica la autenticidad de las credenciales.*
 - *Autorización de Acceso: El sistema otorga o deniega el acceso según las políticas establecidas.*

- **Diagrama de Flujo**

- Descripción: Representación visual del procedimiento, mostrando cada paso y las decisiones a tomar.
- Ejemplo:

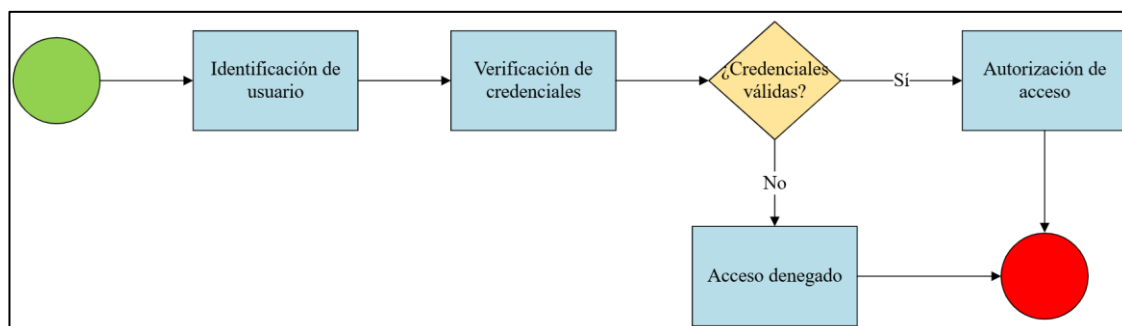


Ilustración 3 Diagrama de flujo ejemplo procedimiento. Fuente: Elaboración propia.

- **Registro de Operación de Procedimiento e Indicadores**
 - Descripción: Documentación de todas las acciones realizadas y medición del rendimiento del procedimiento.
 - Ejemplo:
 - *Registro de Accesos: Registro de intentos de acceso, tiempo de respuesta, y acciones realizadas.*
 - *Indicadores: Tasa de éxito en la autenticación, número de accesos denegados.*
- **Control de Versión de Documento**
 - Descripción: Mantener un historial de revisiones del procedimiento, incluyendo fechas y descripciones de cambios.
 - Ejemplo:
 - *Versión 1.0: Publicación inicial del procedimiento.*
 - *Versión 1.1: Actualización de los pasos de verificación de credenciales (Fecha de Revisión: 15/01/2023).*

Capítulo VI: Implementación

1. Planificación de la implementación

Una vez diseñado el Sistema de Gestión de Seguridad de la Información (SGSI), es crucial diseñar una estrategia de implementación efectiva para asegurar su correcto funcionamiento.

La primera fase corresponde a la planificación y evaluación inicial y su objetivo es establecer una base sólida para la implementación de los controles de seguridad, garantizando que se comprende completamente la situación actual de seguridad y se define un plan claro para el proyecto. Para esto la organización designa a la Gerencia de Informática como equipo responsable de la implementación de los controles de seguridad, debido a que gran parte de estos controles forman parte de los procesos del área, relacionados con las tecnologías de la información.

La Gerencia de Informática en conjunto con un asesor externo de ciberseguridad deben realizar la evaluación inicial de la situación de seguridad de la empresa, con el fin de identificar brechas y áreas de mejoras para la implementación de controles. Dentro de la evaluación se deben desarrollar los siguientes pasos:

- Recopilar y revisar políticas, procedimientos y prácticas de seguridad de los procesos existentes.
- Realizar entrevistas con el personal clave para entender los procesos y el funcionamiento actual.

A partir de esta evaluación el equipo responsable reconoce el estado actual de los controles de seguridad en la organización. Para este reconocimiento se califica la maduración de los controles de seguridad en 5 niveles:

- Nivel 1: No Implementado
 - El control no ha sido implementado en la organización.

- No hay evidencia de la existencia del control o de acciones para su implementación.
 - No se realizan prácticas relacionadas con el control.
- Nivel 2: Implementado Parcialmente
 - El control ha sido implementado de manera informal o parcial, pero no está completamente desarrollado o documentado.
 - Existe alguna evidencia de implementación, pero carece de formalidad y no cubre todos los aspectos necesarios.
 - Hay prácticas de seguridad en uso, pero no están documentadas o son inconsistentes.
- Nivel 3: Implementado y Documentado Formalmente
 - El control está completamente implementado y formalmente documentado en políticas y procedimientos.
 - El control es conocido y seguido por el personal relevante, y existe documentación formal que lo respalda.
 - Hay un procedimiento escrito y aprobado que detalla el control, y el personal está capacitado en su uso.
- Nivel 4: Monitoreado y Evaluado Regularmente
 - Además de estar implementado y documentado, el control es monitoreado y evaluado de manera regular para asegurar su efectividad.
 - Se realizan auditorías y revisiones periódicas del control para identificar y corregir fallas.
 - El control es parte de un programa de auditoría interna que evalúa su cumplimiento y efectividad regularmente.
- Nivel 5: Mejora Continua
 - El control no solo es implementado, documentado y monitoreado, sino que también es sujeto a un proceso de mejora continua.

- Se aplican prácticas de mejora continua, basadas en retroalimentación, auditorías y análisis de desempeño para optimizar el control constantemente.
- El control es revisado regularmente y mejorado basado en las lecciones aprendidas, nuevas amenazas y cambios en el entorno tecnológico.

2. Cronograma de la implementación

La organización establece que para la implementación del SGSI diseñado, el nivel de maduración de los controles requerido es el nivel 3, por lo tanto tras la evaluación del estado inicial, el equipo responsable define el alcance de la implementación tanto en el corto como en el largo plazo de la siguiente manera:

- Corto Plazo: Generación de 37 Procedimientos. Implementación de Controles CIS v7.1
- Mediano y Largo Plazo: Implementación de Controles ISO 27001

En el corto plazo, los controles CIS a implementar son abordados en las políticas y procedimientos de la siguiente forma:

Control CIS	Política	Procedimientos
1: Inventario de Dispositivos autorizados y no autorizados	Política de Gestión de Activos	- Procedimiento de Administración e Inventario de activos Hardware. - Procedimiento de Escaneo de Equipos Informáticos
2: Inventario de Software autorizados y no autorizados	Política de Gestión de Activos	- Procedimiento de Administración de lista blanca de softwares. - Procedimiento de solicitud de software de usuarios.
3: Gestión continua de vulnerabilidades	Política de Seguridad en las Operaciones	- Procedimiento de escaneo y detección de vulnerabilidades. - Procedimiento de Gestión de vulnerabilidades - Procedimiento de Remediación de vulnerabilidades
4: Uso controlado de privilegios administrativos	Política de Control de Acceso	- Procedimiento de Control de cuentas de administrador - Procedimiento de Administración de Cuentas de administrador - Procedimiento de solicitud de uso de cuentas de Administrador
5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles,	Política de Gestión de Activos	- Procedimiento de Configuración de Equipos Informáticos - Procedimiento de Configuración de Servidores - Procedimiento de Configuración de Celulares

estaciones de trabajo y servidores		
6: Mantenimiento, monitoreo y análisis de logs de auditoría	Política de Seguridad en las Operaciones	- Procedimiento de Configuración de Registros de Auditoría - Procedimiento de Análisis de Registros de Auditoría
7: Protección de correo electrónico y navegador web	Política de Seguridad en las Operaciones	- Procedimiento de Administración de navegadores web y Plugins - Procedimiento de solicitud de Plugins de usuarios - Procedimiento de Administración de lista blanca de sitios Web - Procedimiento de solicitud de acceso a sitios web de usuarios. - Procedimiento de configuración de clientes de correo electrónico
8: Defensa contra malware	Política de Seguridad en las Operaciones	- Procedimiento de Administración de Consola de Antivirus.
9: Limitación y control de puertos de red, protocolos y servicios	Política de Seguridad en las Operaciones	- Procedimiento de Administración de Consola de Antivirus.
10: Capacidad de recuperación de datos	Política de Seguridad en las Operaciones	- Procedimiento de Gestión de Respaldos de Sistemas - Procedimiento de Pruebas de Respaldos de Sistemas.
11: Configuración segura de equipos de red, tales como firewalls, switch y router	Política de Seguridad en Comunicaciones	- Procedimiento de Configuración Segura de Equipos de Red - Procedimiento de Administración de Equipos de Red
12: Defensa Perimetral	Política de Seguridad en Comunicaciones	- Procedimiento de Configuración Segura de Equipos de Red - Procedimiento de Administración de Consola de Firewall
13: Protección de Datos	Política de Criptografía	- Procedimiento de Cifrado de Información
14: Control de acceso basado en la necesidad de conocer protección de datos	Política de Control de Acceso	- Procedimiento de Administración de Cuentas de Usuarios en Sistemas - Procedimiento de Control de Cuentas de Usuarios en Sistemas
15: Control de acceso inalámbrico	Política de Seguridad en Comunicaciones	- Procedimiento de Configuración Segura de Equipos de Red - Procedimiento de Administración de Acceso Inalámbrico
16: Monitoreo y control de cuentas	Política de Control de Acceso	- Procedimiento de Control de Cuentas de Usuarios en Sistemas
17: Implementar programa de concientización y entrenamiento en seguridad	Política de Seguridad de la Información	- Procedimiento de Capacitaciones en Seguridad - Procedimiento de Concientización de Usuarios
18: Seguridad de software de aplicación	Política de Adquisición, Desarrollo y Mantenimiento de Sistemas	- Procedimiento de Configuración Segura de Aplicaciones
19: Respuesta y manejo de incidentes	Política de Gestión de Incidentes	- Procedimiento de Respuesta a Incidente - Procedimiento de Recuperación Ante Incidentes
20: Pruebas de penetración y equipo rojo	Política de Gestión de Incidentes	- Procedimiento de Pruebas de penetración de Sistemas - Procedimiento de Pruebas de Equipo Rojo

Tabla 9 Implementación de Controles CIS en Políticas y Procedimientos. Fuente: Elaboración Propia.

La configuración de los procedimientos permite un posterior seguimiento, monitoreo y auditoría de la aplicación de los controles al requerir un registro de la operación descrita en los documentos.

A partir de esta definición se establece el siguiente cronograma para la generación de la documentación y la implementación de los controles de dentro de un plazo de 1 año, considerando la integración de los procesos ya existentes dentro de la organización formándose además dentro de la organización un equipo interno para la implementación de los controles (Equipo SGSI), que además se encarga de capacitar a los equipos del área de Informática durante la implementación de los controles de seguridad.

Actividad	Participantes
Diseño de Procedimientos para Control 1	- Equipo SGSI - Asesor Externo - Jefatura Área Informática
Implementación Control 1	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 2	- Equipo SGSI - Asesor Externo - Jefatura Área Informática
Implementación Control 2	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 3	- Equipo SGSI - Asesor Externo - Jefatura Área Informática
Implementación Control 3	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 5	- Equipo SGSI - Asesor Externo - Jefatura Área Informática
Implementación Control 5	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 6	- Equipo SGSI - Asesor Externo - Jefatura Área Informática

Implementación Control 6	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 10	- Equipo SGSI - Asesor Externo - Jefatura Área Informática
Implementación Control 10	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 7	- Equipo SGSI - Asesor Externo - Jefatura Área Informática
Implementación Control 7	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 8	- Equipo SGSI - Asesor Externo - Jefatura Área Informática
Implementación Control 8	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 9	- Equipo SGSI - Asesor Externo - Jefatura Área Informática
Implementación Control 9	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 4	- Equipo SGSI - Asesor Externo - Jefatura Área Informática
Implementación Control 4	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 17	- Equipo SGSI - Asesor Externo - Gerencia Área Informática - Gerencia Área Recursos Humanos
Implementación Control 17	- Equipo SGSI - Asesor Externo - Jefatura Área Informática

Diseño de Procedimientos para Control 11	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Implementación Control 11	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 12	- Equipo SGSI - Asesor Externo - Jefatura Área Informática
Implementación Control 12	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 13	- Equipo SGSI - Asesor Externo - Jefatura Área Informática
Implementación Control 13	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 14	- Equipo SGSI - Asesor Externo - Jefatura Área Informática
Implementación Control 14	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 15	- Equipo SGSI - Asesor Externo - Jefatura Área Informática
Implementación Control 15	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 16	- Equipo SGSI - Asesor Externo - Jefatura Área Informática
Implementación Control 16	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 18	- Equipo SGSI - Asesor Externo - Jefatura Área Informática
Implementación Control 18	- Equipo SGSI - Jefatura Área Informática

	- Equipo Área Informática
Diseño de Procedimientos para Control 19	- Equipo SGSI - Asesor Externo - Gerencia Área Informática
Implementación Control 19	- Equipo SGSI - Gerencia Área Informática - Jefatura Área Informática - Equipo Área Informática
Diseño de Procedimientos para Control 20	- Equipo SGSI - Asesor Externo - Gerencia Área Informática - Jefatura Área Informática
Implementación Control 20	- Equipo SGSI - Jefatura Área Informática - Equipo Área Informática

Tabla 10 Actividades y participantes implementación controles. Fuente: Elaboración propia.

Actividad	Mes											
	1	2	3	4	5	6	7	8	9	10	11	12
Diseño de Procedimientos para Control 1												
Implementación Control 1												
Diseño de Procedimientos para Control 2												
Implementación Control 2												
Diseño de Procedimientos para Control 3												
Implementación Control 3												
Diseño de Procedimientos para Control 5												
Implementación Control 5												
Diseño de Procedimientos para Control 6												
Implementación Control 6												
Diseño de Procedimientos para Control 10												
Implementación Control 10												
Diseño de Procedimientos para Control 7												
Implementación Control 7												
Diseño de Procedimientos para Control 8												
Implementación Control 8												
Diseño de Procedimientos para Control 9												
Implementación Control 9												
Diseño de Procedimientos para Control 4												
Implementación Control 4												
Diseño de Procedimientos para Control 17												

Implementación Control 17												
Diseño de Procedimientos para Control 11												
Implementación Control 11												
Diseño de Procedimientos para Control 12												
Implementación Control 12												
Diseño de Procedimientos para Control 13												
Implementación Control 13												
Diseño de Procedimientos para Control 14												
Implementación Control 14												
Diseño de Procedimientos para Control 15												
Implementación Control 15												
Diseño de Procedimientos para Control 16												
Implementación Control 16												
Diseño de Procedimientos para Control 18												
Implementación Control 18												
Diseño de Procedimientos para Control 19												
Implementación Control 19												
Diseño de Procedimientos para Control 20												
Implementación Control 20												

Tabla 11 Cronograma Implementación Controles. Fuente: Elaboración propia.

3. Recursos para la implementación

La implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa requiere una inversión estratégica en dos recursos clave: capital humano e infraestructura informática. El capital humano incluye:

- Personal Se requiere la asignación de personal especializado en ciberseguridad y gestión de riesgos, así como expertos en la integración de sistemas TI. La empresa presupuesta la contratación de 5 personas:
 - 2 profesionales en gestión de riesgos y ciberseguridad. Costo mensual 50 UF cada uno.
 - 3 profesionales técnicos especialistas en informática. Costo mensual 35 UF cada uno.
- La contratación de consultores externos para la formación continua del equipo interno en cuanto al conocimiento y la capacidad de respuesta ante incidentes. Se presupuestan de la siguiente forma:

- Consultor y Asesor en Ciberseguridad. Costo mensual: 140 UF.
- Consultora y Asesor en Gestión de riesgos. Costo mensual: 22 UF.

La infraestructura TI, por su parte, abarca los sistemas tecnológicos esenciales para la proteger la información y aplicar los controles de seguridad a implementar, como antivirus, herramientas de monitoreo, redes seguras y centros de datos con medidas de seguridad avanzadas.

En particular para la implementación de los controles de seguridad, se presupuestan los siguientes costos, según la herramienta y servicio:

- **Sistema de administración de equipos de usuarios:** Solución que proporciona monitoreo en tiempo real de dispositivos y software, asegurando que solo activos autorizados operen dentro de la red de la empresa. Además, automatiza la detección de vulnerabilidades y la aplicación de parches de seguridad, fortaleciendo la protección contra amenazas cibernéticas. Esencial para la implementación de los controles CIS, Familias 1, 2 y 3.
 - Costo Mensual: 40 UF.
- **SIEM (siglas en ingles de Gestión de Información y Eventos de Seguridad):** Solución de gestión de registros de eventos en sistemas informáticos (logs) que facilita la implementación del Control CIS Familia 6, encargado del monitoreo y análisis de registros de auditoría. Permite la recopilación centralizada de eventos de seguridad desde múltiples fuentes, la detección automatizada de actividades sospechosas y el análisis forense de incidentes, asegurando trazabilidad y cumplimiento normativo.
 - Costo Mensual: 80 UF.
- **Consola de Antivirus y Servicio SOC:** Solución avanzada de seguridad que facilita la implementación de los Controles CIS Familia 8 y 19 con el respaldo de un servicio de Centro de Operaciones de Seguridad (SOC). Permite protección en tiempo real contra amenazas mediante inteligencia artificial,

detección proactiva de ransomware y análisis de comportamiento para identificar ataques. Además, integra capacidades de monitoreo continuo y respuesta gestionada, permitiendo la contención rápida de incidentes y el análisis forense.

- Costo Mensual: 72 UF.

- **Servicio de respaldo y recuperación de información:** Sistema de gestión y recuperación de datos, facilita la implementación del Control CIS Familia 10, enfocado en capacidades de recuperación de datos. Sus herramientas permiten realizar copias de seguridad automatizadas, garantizar la disponibilidad de información crítica y ejecutar pruebas de restauración para asegurar la continuidad operativa. Además, proporciona protección contra pérdida de datos y ransomware, integrando cifrado y almacenamiento seguro.

- Costo Mensual: 300 UF.

- **DLP (siglas en inglés de Prevención de Pérdida de Datos):** Sistema esencial para la implementación del Control CIS Familia 13, ya que sus herramientas monitorean, detectan y previenen la fuga de datos sensibles, asegurando su protección contra accesos no autorizados. Estas soluciones identifican información crítica en archivos y correos electrónicos, bloquean transferencias no autorizadas, aplican cifrado avanzado y generan alertas para garantizar el cumplimiento normativo.

- Costo Mensual: 50 UF.

Capítulo VII: Conclusiones

La investigación responde a la pregunta ¿qué características de la industria portuaria son relevantes y se deben considerar para el diseño de un sistema de gestión de seguridad de la información? destacando dos factores clave. En primer lugar, el impacto económico del sector portuario en Chile exige la implementación de un SGSI robusto, dado que cualquier interrupción en las operaciones, que funcionan las 24 horas del día, puede generar consecuencias financieras significativas, afectando el comercio exterior y la logística nacional. Minimizar los riesgos de ciber incidentes que puedan detener la actividad portuaria es una prioridad estratégica para garantizar la continuidad operativa. Además, el crecimiento tecnológico en los sistemas portuarios ha incrementado la superficie de ataque, aumentando la exposición a amenazas y vulnerabilidades. La digitalización de procesos, la interconexión entre sistemas TI y operacionales, y el uso de tecnologías avanzadas requieren un enfoque de seguridad adaptativo y proactivo, que considere controles técnicos y organizativos alineados con estándares internacionales.

La pregunta ¿cuál de la metodología de mejora continua es óptima para su aplicación en un sistema de gestión de seguridad de la información? se responde indicando que la metodología más adecuada es el ciclo PDCA (Plan-Do-Check-Act), ampliamente utilizada en la ISO/IEC 27001 para la gestión de seguridad de la información. Su enfoque iterativo permite una implementación progresiva y mejora continua, asegurando que el SGSI evolucione de manera sistemática a medida que se identifican nuevas amenazas y se optimizan los controles.

El trabajo cumple el objetivo de diseñar un SGSI para una empresa portuaria en Chile, con el enfoque PDCA garantizando su adaptación al entorno y fortaleciendo la seguridad de manera estructurada. Además, se diseña la estrategia de implementación del SGSI confeccionado, en donde la planificación prioriza la implementación de controles técnicos relacionados con CIS v7.1 en el corto plazo, enfocándose en la participación del área de Informática. Esto asegura una base sólida de seguridad en el menor tiempo posible, atendiendo de inmediato a los riesgos críticos identificados en la interconexión de sistemas TI y operacionales, ambos fundamentales en la industria portuaria chilena. Por otro lado, los controles organizacionales de la ISO 27001, que demandan la participación de toda la

organización y la integración de procesos transversales, se planifican para el mediano y largo plazo. Esto se alinea con el enfoque analítico previo, ya que se reconoce que la maduración de prácticas, la estandarización y el fortalecimiento de la cultura de seguridad requieren de una evolución continua, formalizada mediante un modelo iterativo de mejora continua (PDCA). Así, se contempla que, a medida que se formalicen y documenten los procedimientos—especialmente aquellos ya existentes de manera informal en el área de Informática—la organización podrá aumentar su capacidad para coordinar respuestas y ajustar controles ante el cambio.

Durante la evaluación inicial, se identificaron prácticas no documentadas dentro del área de informática, lo que puso de relieve la necesidad de formalizar y sistematizar estos procedimientos. Este hallazgo, enmarcado en el análisis crítico de la situación actual, resalta la importancia de la documentación para estandarizar operaciones y facilitar el entrenamiento del personal, garantizando así su correcta implementación y seguimiento. La diagramación y el seguimiento constante de procesos son prácticas esenciales que potencian la mejora continua del SGSI, permitiendo optimizar la gestión de la información.

Además, se debe establecer un programa de capacitación y concienciación en paralelo a la implementación de políticas y procedimientos. Este programa, basado en el enfoque analítico que reconoce la importancia del capital humano en la seguridad, está diseñado para asegurar que todos los empleados comprendan y sigan las directrices establecidas. Las capacitaciones, al reducir la resistencia al cambio y mejorar las prácticas laborales, contribuyen a una implantación uniforme de nuevas políticas y procedimientos, fortaleciendo la cultura de seguridad y promoviendo la responsabilidad en la protección de los activos de información.

Finalmente, tras la implementación inicial, es crucial establecer un sistema de monitoreo que incluya la actualización de documentos, revisiones periódicas—anuales o ante cambios significativos en el sistema—y auditorías internas constantes. Este proceso iterativo, fundamentado en el ciclo PDCA, no solo evalúa la efectividad de los controles implementados, sino que también garantiza la mejora continua y la adaptación del SGSI frente a nuevas amenazas y dinámicas del entorno. Con estos pasos se asegura la maduración progresiva y sostenible de los controles de seguridad, optimizando recursos y esfuerzos en un contexto tan exigente como el de la industria portuaria en Chile.

La estrategia escalonada y complementaria propuesta permite una implementación ordenada y eficaz del SGSI. Se aprovechan los beneficios de una base técnica inmediata y se planifica un fortalecimiento organizacional progresivo, integrando recomendaciones normativas y metodologías de mejora continua para garantizar la protección integral de la información y la continuidad operativa de la organización.

Referencias Bibliográficas

- Álvarez, N. (2023). Evaluación de la estructura de ciberseguridad en el puerto de Valparaíso. <https://repositoriobibliotecas.uv.cl/items/733bfca5-f9e9-48db-996f-7c75187eb5e6>
- Agrawal, V. (2024). *What is Six Sigma? A comprehensive guide for beginners*. Simplilearn.com; Simplilearn. <https://www.simplilearn.com/what-is-six-sigma-a-complete-overview-article>
- Bhattacharjee, S. (2022). *8 major ports in Chile*. Marine Insight. <https://www.marineinsight.com/know-more/8-major-ports-in-chile/>
- Bendersky, S. (2023). *Outer Harbor: The Largest Port Expansion Project in Chile's History*. AAPA Seaports. <https://www.aapaseaports.com/index.php/2023/06/16/outer-harbor-the-largest-port-expansion-project-in-chiles-history/>
- Camport (2024). Análisis Comparativo Comercio Exterior. *Camport.cl*. https://www.camport.cl/wp-content/uploads/2024/09/Reporte-Camport-COMEX-en-jun-2024_V3.pdf
- CEICdata.com. (2018, 1 junio). *Chile Container port throughput*. <https://www.ceicdata.com/en/indicator/chile/container-port-throughput>
- CIS Critical Security Controls v7.1*. (2021). CIS. <https://www.cisecurity.org/controls/v7-1>
- Cortés Zambrano, C. (2022). Gobernanza en ciudades portuarias y los desafíos de los consejos de coordinación ciudad puerto.
- Daily Cargo News. (2023). MARITIME COUNTRY PROFILE: Chile. *The DCN*. <https://www.thedcn.com.au/magazine-issues/maritime-country-profile-chile/>
- Estall, H. (2012). *Business continuity management systems: Implementation and certification to ISO 22301*. BCS, The Chartered Institute

- FortiGuard Labs (2022). Reporte de ciberataques en América Latina. *Fortinet*.
<https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-reporte-ciberataques-america-latina-2021>
- ISO/IEC 27000 family. (2023). ISO- ISO/IEC 27000 family — Information security management. <https://www.iso.org/standard/iso-iec-27000-family>
- ISO 22301:2019. (2025). ISO. <https://www.iso.org/standard/75106.html>
- Karmy, J. (2024). Ley 21.663: Lo que debes saber del Marco de Ciberseguridad 2024 en Chile. *Tecnoera*. <https://www.tecnoera.cl/contenido/novedades/ley-21-663-lo-que-debes-saber-del-marco-de-ciberseguridad-2024-en-chile>
- Kaspersky. (2024, November 4). *América Latina enfrenta más de 3.1 millones de ataques de malware por día, alerta Kaspersky*. /. <https://latam.kaspersky.com/about/press-releases/america-latina-enfrenta-mas-de-31-millones-de-ataques-de-malware-por-dia-alerta-kaspersky>
- Meitarice, S., Febyana, L., Fitriansyah, A., Kurniawan, R., & Nugroho, R. A. (2024). Risk Management Analysis of Information Security in an Academic Information System at a Public University in Indonesia: Implementation of ISO/IEC 27005: 2018 and ISO/IEC 27001: 2013 Security Controls. *Journal of Information Technology and Cyber Security*, 2(2).
- Millard, M. (2023). *The fundamentals and advantages of the Lean methodology*. Kainexus.com. <https://blog.kainexus.com/the-fundamentals-of-the-lean-methodology>
- Ministerio de Transportes y Telecomunicaciones. (s. f.). *Empresas portuarias | Ministerio de Transportes y Telecomunicaciones*. <https://mtt.gob.cl/empresas-portuarias>
- Schweizerische, S. N. V. (2013). Information technology-Security techniques-Information security management systems-Requirements. *ISO/IEC International Standards Organization*.
- Shamma, B. (2018). Implementing CIS Critical Security Controls for Organizations on a Low-Budget (Master's thesis, University of Houston).

- Svobodová, K. (2023). ISO/IEC 27001: The Scope, Purpose, and How to Comply. *Safetica*.
<https://www.safetica.com/blog/iso-27001-iec-27001-the-scope-purpose-and-how-to-comply>
- SYDLE. (2021). *PDCA cycle: What are the stages and how does it work? See examples*.
Blog SYDLE; SYDLE. <https://www.sydle.com/blog/pdca-cycle-61ba2a15876cf6271d556be9>
- Valades, B. (2022). Ciberataques en Latinoamérica aumentaron un 38% en 2021.
Segurilatam. https://www.segurilatam.com/actualidad/ciberataques-en-latinoamerica-aumentaron-un-38-en-2021_20220111.html
- World Bank Open Data. (2025). Comercio (% del PIB) - Chile. *World Bank Open Data*.
<https://datos.bancomundial.org/indicador/NE.TRD.GNFS.ZS?locations=CL>