Universidad de Valparaíso
CHILE
Facultad de Ingeniería

Trabajo Final del proyecto para optar
al Grado de Magister en Administración y gestión Portuaria

# EVALUACIÓN DE LA ESTRUCTURA DE CIBERSEGURIDAD EN EL PUERTO DE VALPARAÍSO

**Nicolás Álvarez Pérez**

Junio 2023

# II. APROBACIÓN

EVALUACIÓN DE LA ESTRUCTURA DE CIBERSEGURIDAD EN EL PUERTO DE VALPARAÍSO

Nicolás Álvarez Pérez

| COMISIÓN REVISORA | NOTA | FIRMA |
|---|---|---|
| Felipe Caselli<br>Profesor Guía | _____ | _____ |
| Filler<br>Revisión | _____ | _____ |
| Filler<br>Revisión | _____ | _____ |

# III. DECLARACIÓN

Este trabajo, o alguna de sus partes, no ha sido presentado anteriormente en la Universidad de Valparaíso, institución universitaria chilena o extranjera u organismo de carácter estatal, para evaluación, comercialización u otros propósitos. Salvo las referencias citadas en el texto, confirmo que el contenido intelectual de este trabajo final de graduación es resultado exclusivamente de mis esfuerzos personales.

La Universidad de Valparaíso reconoce expresamente la propiedad intelectual del autor sobre esta Memoria de Titulación. Sin embargo, en caso de ser sometida a evaluación para los propósitos de obtención del Grado de Magíster en Administración y Gestión Portuaria, el autor renuncia a los derechos legales sobre la misma y los cede a la Universidad de Valparaíso, la que estará facultada para utilizarla con fines exclusivamente académicos.

# IV. TABLA DE CONTENIDOS

# V. RESUMEN

La ciberseguridad es un aspecto crítico de las operaciones marítimo-portuarias, correspondiendo a la principal herramienta para reducir los riesgos asociados y evitar daños a la infraestructura, paralización de operaciones y pérdidas monetarias, por esto se busca evaluar la estructura de ciberseguridad en el puerto de Valparaíso. La evaluación se realizó mediante un estudio de caso y análisis de literatura relevante, considerando entrevistas para determinar la percepción desde dentro de la industria. Para este estudio se solicitó la participación diez organizaciones involucradas en las operaciones marítimo-portuarias en el área de Valparaíso, estás siendo empresas privadas o entes públicos. Las entrevistas fueron semiestructuradas con personal dedicado a los procesos de ciberseguridad, entender la situación actual de la cadena logística, mediante preguntas enfocadas a la situación de ciberseguridad interna y externa. Se identificaron oportunidades de mejoras y admisiones que la concienciación de ciberseguridad dentro de las organizaciones es baja, resultando en problemas que directamente se pueden atribuir al factor humano, igualmente se determinaron que los avances legislativos y normativos a nivel estatal no responden a las problemáticas actuales, por lo que las mismas organizaciones deben utilizar normativas externas para atenuar los riesgos presentes.

Palabras claves: Ciberseguridad, Sistemas portuarios, Sistemas de gestión de riesgo

# 1. INTRODUCCIÓN

El transporte marítimo es fundamental para el comercio mundial y al mismo tiempo es una de las principales industrias que facilitan el crecimiento económico de Chile. Los puertos y terminales marítimos son las instalaciones importantes en términos de movimiento de carga y mercancías en el mundo (UNCTAD, 2022). A medida que estas infraestructuras se vuelven más dependientes de las nuevas tecnologías para administrar, facilitar y acelerar los procedimientos de transferencia de carga, el riesgo de las amenazas a la protección de las redes computacionales y de comunicación se ha convertido en una preocupación considerable (Zarzuelo, 2020).

En la actualidad diversas industrias se encuentran en riesgo de ser afectadas por ataques cibernéticos, causando consecuencias de gran alcance, en el caso particular de la industria marítimo-portuaria estas repercusiones pueden ser económicas, interrupción en transporte de energía, alimentos o de seguridad nacional.

Debido a la importancia del puerto de Valparaíso en el ámbito logístico de la zona centro de Chile, es de particular interés garantizar que las instalaciones se encuentren protegidas contra las amenazas digitales, para esto, se necesita tener una comprensión holística de las condiciones de ciberseguridad presentes en las organizaciones o empresas logísticas que operen o contribuyan a la operación portuaria, analizando los métodos de transferencias de información, las vulnerabilidades presentes y las prácticas actuales en relación a la seguridad cibernética. El propósito de este estudio es abordar esta necesidad examinando el estado de la ciberseguridad en el puerto de Valparaíso y proponiendo un marco de trabajo completo utilizando las normas más efectivas para la industria marítima.

El estudio se ejecutará a través de una revisión de literatura e investigaciones actuales para identificar las amenazas y vulnerabilidades de ciberseguridad que enfrentan las organizaciones del rubro marítimo, esto tanto a nivel nacional como internacional. Para lograr esto se solicitarán entrevistas con entidades públicas y privadas que desempeñan labores en el ámbito de la logística portuaria en la zona de Valparaíso. Con la información recopilada mediante las entrevistas se determinarán las principales fallas del sistema y se podrán recomendarán respuestas a estas problemáticas.

# 2. OBJETIVOS

El objetivo general de este trabajo final es el de proponer un marco de ciberseguridad para el puerto que integre las mejores prácticas y estándares de la industria y los organismos reguladores.

Esta investigación se guiará bajo los siguientes objetivos específicos:

1. Evaluar los protocolos, estándares y directivas existentes que guían el desarrollo de políticas de ciberseguridad a nivel portuario.

2. Analizar los procesos de gestión de riesgo en relación con la ciberseguridad de los entes involucrados en las operaciones del puerto de Valparaíso.

3. Evaluar el nivel de preparación que posee el puerto de Valparaíso y las organizaciones relacionadas con el ámbito logístico portuario

Al lograr estos objetivos, el estudio proporcionará una comprensión integral del estado de la ciberseguridad en el puerto de Valparaíso y los posibles riesgos e impactos de los ciberataques en las operaciones portuarias. La información recopilada a través de esta investigación también contribuirá al desarrollo de políticas y estrategias de ciberseguridad efectivas para los entes portuarios y las partes interesadas, así mejorando la resiliencia del sistema logístico de Valparaíso en su totalidad.

# 3. MARCO TEORICO

La ciberseguridad es un tema de alta importancia en todos los sectores industriales, comerciales y financieros. Con los avances en digitalización y la adopción de tecnologías emergentes como IoT (Internet de las cosas), Inteligencia Artificial, Blockchain, 5G y sistemas de automatización, los recintos portuarios se han vuelto cada vez más vulnerables a los ciberataques debido a la baja comprensión de los requisitos de seguridad que estas tecnologías se deben desplegar (Nam, 2019). Este trabajo final de proyecto propone un marco conceptual para entender y abordar los retos de la ciberseguridad en los en la estructura logística correspondiente.

## 3.1 CIBERSEGURIDAD

La ciberseguridad se ha convertido en un aspecto fundamental pero poco concientizado a lo largo del mundo, considerando que la mayoría de las actividades comerciales, de manufactura y transmisión de información dependen de acceso a redes para su correcta operación. A continuación, se examinarán en profundidad la definición y los conceptos básicos de la ciberseguridad.

De acuerdo con lo establecido por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) la ciberseguridad es "La prevención de daño a, protección de y restauración de equipos electrónicos, servicios y comunicaciones que usan tecnologías de la información y las comunicaciones, de daños causados por amenazas, tanto internas como externas, para garantizar su disponibilidad, integridad, autenticidad, confidencialidad y utilidad" (Committee on National Security Systems, 2015). Esta definición es una de las tantas que se han generado en el sector de la ciberseguridad, pero corresponde a una de las más referenciadas y utilizadas para aplicar los protocolos y estándares que existen en las industrias.

La ciberseguridad se ha convertido en un aspecto esencial para garantizar la continuidad de las operaciones comerciales, privacidad de los datos, rápida entrega de servicios y la seguridad nacional. Según un informe de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en 2020, el coste económico global de los ciberataques podría superar los 6 billones de dólares para 2021 y este aumentaría progresivamente en los próximos 5 años (OECD, 2020). Los costos para recuperar la normalidad operativa después de un ataque cibernético a una empresa u organización pueden ser restrictivamente altos, no solo desde un punto de vista monetario, sino de confianza externa.

La ciberseguridad es fundamental cuando se aplica a la infraestructura crítica, como los sistemas portuarios. Los puertos son esenciales para el funcionamiento de nuestra sociedad y economía y su defensa es de vital importancia. Un informe de la Agencia Europea para la Ciberseguridad (ENISA) destacó que los sistemas portuarios son una parte integral de la infraestructura crítica y que su protección contra amenazas cibernéticas es crucial para la seguridad y prosperidad de la Unión Europea (ENISA, 2019), utilizando dicha determinación y lo establecido en la Ley núm. 21.542 en la cual se dan lineamientos para lo que el estado de Chile considera infraestructura crítica esta también se podría establecer

bajo este concepto en caso de que se las instalaciones se encuentren en peligro grave o inminente.

Los siguientes son una serie de conceptos básicos que encapsulan los ámbitos más comunes de la ciberseguridad:

A. **Amenaza Cibernética**: Las amenazas cibernéticas se refieren a cualquier circunstancia o evento potencial que puede comprometer la seguridad de la información digital (NIST, 2019).

B. **Vulnerabilidad**: Corresponden a una debilidad en un sistema que puede ser explotada por una amenaza cibernética (NIST, 2019).

C. **Ataque Cibernético**: Es un intento malicioso de degradar, alterar, destruir o acceder de manera no autorizada a un sistema o a la información que contiene (NIST, 2019).

D. **Resiliencia Cibernética**: Es la capacidad que poseen las organizaciones de prepararse y adaptarse a las amenazas cibernéticas, así como de recuperarse y aprender de ellas para modificar sus protocolos de respuesta (NIST, 2019).

La ciberseguridad es un aspecto fundamental de la protección de la red de información, especialmente en la infraestructura crítica como los sistemas portuarios. Los conceptos básicos de la ciberseguridad proporcionan un marco para entender y abordar las amenazas cibernéticas, estos términos son importantes para comprender las normativas y protocolos establecidos por las organizaciones NIST y ENISA, o los lineamientos de ISO/IEC 27001.

## 3.2 AMENAZAS Y VULNERABILIDADES

Es fundamental conocer las amenazas y vulnerabilidades más comunes que afectan a los sistemas de información, a continuación, se presentan algunos ejemplos de estas:

A. **Phishing**: Se trata de un intento de adquirir información confidencial, como nombres de usuario, contraseñas y detalles de tarjetas de crédito, a menudo a través de un correo electrónico o mensaje de texto que parece ser de una organización de confianza (ENISA, 2019).

B. **Ingeniería Social**: Se refiere a las tácticas que los delincuentes emplean para engañar a los individuos y persuadirlos a revelar información confidencial o realizar acciones que puedan comprometer la seguridad de los sistemas informáticos. Estos ataques pueden tomar muchas formas, desde tailgating y pretexting, hasta manipulación interpersonal y baiting (IBM, 2022), enfocándose en explotar la confianza humana y las debilidades en lugar de las vulnerabilidades tecnológicas.

C. **Autorización**: Los "ataques de autorización" en el contexto de la ciberseguridad portuaria se refieren a las tácticas que los ciberdelincuentes utilizan para comprometer los mecanismos de autenticación de un sistema. Estos eventos pueden involucrar el robo de credenciales, la manipulación de sistemas de

verificación o el uso de software especializados para obtener acceso no autorizado a redes y datos críticos de las organizaciones.

D. **Ransomware**: Es un tipo de software malicioso que cifra los archivos del usuario y exige un pago para su recuperación. Un ejemplo relevante fue un evento conocido como “WannaCry” del año 2017, dicho ataque afectó a cerca de 300,000 sistemas en 150 países, el fin de este era encriptar los computadores para así obtener un rescate vía bitcoin (NPR, 2017).

E. **Ataques DDoS (Distributed Denial of Service)**: Son ataques en los que múltiples sistemas infectados inundan la red de una víctima con tráfico para hacerla inaccesible. En 2020, Amazon Web Services reportó el ataque DDoS más grande registrado, con un peak de 2.3 Tbps (AWS, 2021).

F. **Ataques de fuerza bruta (Brute Force)**: Estos ataques intentan adivinar las contraseñas de los usuarios mediante la repetición de todas las combinaciones posibles hasta encontrar la correcta.

G. **Ataques de inyección SQL**: Estos ataques se producen cuando un atacante tiene acceso y la capacidad insertar código malicioso en una consulta SQL, lo que puede llevar a la manipulación de la base de datos y al robo de información.

H. **Malware**: Los ataques de malware implican la introducción de software malicioso en un sistema con la intención de causar daño o robar información, uno de los ejemplos más importantes en la historia de la logística moderna fue el caso de NotPetya que afecto a una serie de empresas internacionales entre las cuales se encontraba la naviera Maersk, causando serios problemas en la cadena logística-portuaria, se estima que las perdidas relacionadas con este ciberataque son de aproximadamente 300 millones de dólares por parte de Maersk, sin considerar los daños a otros entes durante el suceso (WIRED, 2018).

Las vulnerabilidades a la ciberseguridad corresponden a falencias en los sistemas de información, siendo estas explotadas comprometiendo la integridad, confidencialidad y disponibilidad de los datos, entre las debilidades más comunes se encuentran las siguientes:

A. **Software desactualizado**: Software que no se ha actualizado regularmente puede contener vulnerabilidades, esto no solo se limita a aplicaciones, sino también a páginas web, con un estimado del 95% de los sitios web conteniendo código obsoleto (Demir, Urban, Wittek, & Pohlmann, 2021) pudiendo este ser explotado por delincuentes para acceder a información privada.

B. **Configuración insegura**: La configuración insegura corresponde a una situación en la cual un sistema o aplicación se configura con opciones o parámetros que no la protegen contra amenazas a su integridad, tal como el uso de contraseñas predeterminadas, existencia de puertos abiertos en accesos públicos o protocolos de red innecesarios. Según lo determinado en un estudio de protocolos de seguridad, la mayoría de las redes que utilizan WPA2 poseen configuraciones inseguras y cerca del 86% de estas pueden sufrir de robos de credenciales (Hue, et al., 2021).

C. **Falta de conciencia sobre ciberseguridad**: Muchas veces, los usuarios pueden no estar al tanto de las mejores prácticas de ciberseguridad, lo que puede resultar en acciones inseguras, como acceder a enlaces sospechosos o descargar archivos sin verificar el origen (KnowBe4, 2021).

D. **Uso de Software o Hardware No Seguro**: Al usar software o hardware de fuentes no confiables o que no han sido revisados por expertos en seguridad, se pueden introducir vulnerabilidades en los sistemas (DHS, 2020).

E. **Interconexión y Dependencia de Sistemas**: La interconexión de sistemas y la vinculación de servicios de terceros pueden aumentar la superficie de ataque y la posibilidad de un fallo en cascada. Estudios han demostrado que la infraestructura de puertos marítimos tiene una alta dependencia de redes colaborativas, aumentando la probabilidad de ser afectado por ataques fuera de su red interna (Polatidis, Pavlidis, & Mouratidis, 2017).

F. **Falta de Controles de Seguridad Física**: Los sistemas informáticos también son vulnerables a amenazas físicas, como el robo de aparatos, la entrada no autorizado a ciertas instalaciones, uso de dispositivos no autorizados para el acceso de red organizacional y explotación de instrumentos integrados al IoT (CISA, 2021).

Considerando las vulnerabilidades cibernéticas en el contexto logístico-portuario, es evidente que los peligros y riesgos son diversos y multifacéticos, con nuevos obstáculos generándose constantemente. Desde los ataques de fuerza bruta hasta los más sofisticados como phishing y ransomware, los sistemas portuarios se enfrentan a un abanico de amenazas cibernéticas que ponen a prueba su resiliencia, preparación y su capacidad de recuperación.

En el año 2018 el gobierno de Chile instauró el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), siendo esta una entidad que se dedica a catalogar e informar vulnerabilidades descubiertas y que puedan ser explotadas en las redes de información, igualmente generan alertas e informes sobre potenciales peligros cibernéticos, desde el nivel industrial hasta el de usuario (CSIRT, 2021). Un aspecto que merece especial atención es el factor humano, que frecuentemente es considerado como el punto más débil la ciberseguridad. Los errores humanos, ya sea por falta de capacitación, negligencia, o incluso por acciones malintencionadas, pueden resultar en serios efectos negativos a la protección de datos. Estas fallas permiten a los delincuentes acceso a sistemas críticos, información sensible de clientes o procesos internos, interrumpir operaciones y causar daños significativos en caso de que el método de ataque sea particularmente destructivo.

## 3.3 SISTEMAS PORTUARIOS

Los sistemas portuarios son entidades complejas y comprenden una serie de factores que interactúan para facilitar sus funciones, incluyendo la transferencia de mercancías, la gestión de la logística, el manejo de la seguridad y más. Entre estos componentes se pueden destacar la infraestructura, herramientas digitales y equipos físicos.

La infraestructura de los puertos corresponde a los componentes físicos que permiten el correcto funcionamiento de las operaciones de transferencia de carga, pasajeros y atención a de naves, entre las más relevantes se encuentran:

A. **Terminales**: Las terminales son las áreas donde los buques son cargados y descargados. Incluyen grúas, muelles, almacenes y otros equipamientos necesarios para el manejo de la carga.

B. **Almacenes y Depósitos**: Los almacenes son esenciales para el depósito temporal de mercancías que llegan o salen del puerto. Los depósitos se utilizan para el almacenamiento a largo plazo o para bienes especiales como contenedores refrigerados.

C. **Infraestructuras de Servicio**: Esto incluye estaciones de combustible, talleres de reparación, instalaciones de inspección de aduanas y servicios de emergencia que apoyan las operaciones diarias del puerto.

D. **Red de Carreteras y Ferrocarriles**: Los puertos también incluyen redes de viales y ferrocarriles para facilitar el transporte terrestre de mercancías desde y hacia el puerto.

Las herramientas digitales que facilitan la gestión de las operaciones portuarias, estas pueden enfocarse en la planificación, ejecución y control de la transferencia de carga o identificación de los usuarios y mercancía, los sistemas más comunes en los puertos son:

A. **Sistema de Gestión de Terminales (TOS)**: El TOS es un software que ayuda a gestionar las operaciones del puerto, incluyendo la planificación, ejecución y seguimiento de las actividades de la terminal.

B. **Sistema de Información Geográfica (GIS)**: El GIS es una herramienta que ayuda en la gestión y planificación de los recursos del puerto, proporcionando datos espaciales de forma detallada en las instalaciones portuarias.

C. **Sistema de Identificación Automática (AIS)**: El AIS es un sistema de seguimiento empleado para identificar y localizar buques, proporcionando información en tiempo real sobre su posición y rumbo (IMO, 1998).

D. **Sistema de Manejo de Tráfico de Buques (VTMS)**: El VTMS es un sistema de seguimiento y monitoreo que ayuda a mejorar la seguridad y eficiencia de los movimientos de naves en los puertos y vías navegables circundantes.

E. **Sistemas de Seguridad Cibernética**: Estos sistemas son esenciales para proteger la infraestructura de TI del puerto contra las amenazas cibernéticas y garantizar la integridad y confidencialidad de los datos.

Los equipos físicos utilizados para las operaciones portuarias, seguridad y comunicación se pueden dividir en los siguientes grupos:

A. **Equipos de Manipulación de Carga**: Esto incluye grúas, montacargas y otros equipos utilizados para cargar y descargar mercancías de los buques.

B. **Sistemas de Vigilancia**: Los puertos utilizan una variedad de sistemas de vigilancia, incluyendo cámaras de CCTV, radar y sensores, para monitorear las actividades del puerto y garantizar la seguridad.

C. **Tecnología de la Información y la Comunicación (TIC)**: Los sistemas de TIC son fundamentales para la gestión y operación de los puertos modernos, proporcionando las redes y los esquemas de trabajo que soportan las operaciones de información y comunicación.

Los sistemas portuarios son entidades complejas que incorporan una amplia gama de elementos físicos y tecnológicos. Cada uno de estos componentes desempeña un papel vital en las operaciones del puerto, es de notar que los equipos y la infraestructura portuaria ha empezado a adoptar el IoT de manera más agresiva en la última década (Bures, et al., 2021).

## 3.4 IMPORTANCIA ESTRATÉGICA DE LOS SISTEMAS PORTUARIOS

Los puertos son nodos clave en la red de comercio internacional facilitando la mayor parte del intercambio mundial, ya que aproximadamente el 80% del volumen global de mercancías se transportan vía naves, considerando esto y la realidad de los considerables costos navieros y una menor conectividad marítima pueden resultar en índices de inflación más altos, escasez de alimentos y problemas en las cadenas de suministros (UNCTAD, 2022).

Los terminales marítimos también son puntos focales para la seguridad nacional, siendo estos los principales lugares de entrada y salida para los bienes, debido a esto su integridad es fundamental para prevenir el contrabando, la inmigración ilegal y ataques terroristas. Posteriormente de los atentados del 11 de septiembre de 2001 y sus consecuencias económicas, políticas y sociales, Estados Unidos aumentó significativamente los requerimientos en sus puertos a través de la Ley de Seguridad del Transporte Marítimo, proceso que se expandió a otros países vía el código ISPS (IMO, 2022), de esta manera se empieza a priorizar la protección en la infraestructura portuaria de una forma estandarizada y completa.

Los puertos tienen un impacto económico significativo a nivel local, generando empleo, promoviendo el desarrollo de industrias que apoyan las operaciones portuarias y atrayendo

inversiones tanto a la infraestructura como al capital intelectual a través de proyectos de investigación y avance de tecnologías. Terminal Pacífico Sur ha reportado 810.142 TEU's movilizados durante el año 2022, con un total de 391 recaladas de naves (TPS, 2022), representando una arista económica fundamental en el progreso de la ciudad de Valparaíso.

Los puertos son considerados infraestructuras críticas debido a que son esenciales para la movilización de productos y servicios, como el suministro de alimentos, energía y otros bienes, en el caso de Valparaíso también se debe considerar el movimiento de personas durante la temporada de cruceros entre octubre y abril.

Durante la pandemia de COVID-19, por ejemplo, los puertos desempeñaron un papel vital en el mantenimiento de las cadenas de suministro a pesar de las interrupciones globales, incorporando nuevas tecnologías de manera acelerada para sobrellevar los atrasos y alzas en los costos de transporte (Bocayuva, 2021).

Las áreas portuarias también son centros de innovación y desarrollo tecnológico, ubicados a la vanguardia de las tecnologías emergentes, como la automatización, la digitalización y la sustentabilidad. En la actualidad, varios puertos europeos se encuentran experimentando con nuevas técnicas relacionadas con el IoT y el Blockchain para mejorar su eficiencia y sostenibilidad (Henesey, et al., 2020). Utilizando estos nuevos protocolos de ubicación y rápida comunicación, simulación, entre otras, se pueden realizar mejores planes de carga que responden a la realidad de la situación en los buques y los muelles.

## 3.5 FRAMEWORKS

Un framework corresponde a un compendio de estándares, buenas prácticas y normativas que permiten administrar los riesgos de tecnologías digitales (NIST, 2019), estos proveen un mapeo con los objetivos de seguridad específicos que busca resolver. Entre los frameworks más relevantes para las organizaciones del rubro portuario se encuentran las siguientes:

- NIST CSF V1.1
- ISO 27001
- COBIT
- ISA

Estos poseen variados objetivos y enfoques que los diferencian sustantivamente, por lo que se debe estudiar e identificar sus cualidades específicas para poder adoptar los mejores componentes de cada una de estas. A continuación, se desarrolla una tabla comparativa que busca diferenciar de manera superficial los distintos aspectos de los sistemas mencionados.

Tabla 3.5: Comparación de Frameworks

| | NIST Cybersecurity Framework | ISO 27001 | COBIT | ISA/IEC 62443 |
|---|---|---|---|---|
| **Objetivo** | Mejorar la ciberseguridad de infraestructuras críticas. | Establece un Sistema de Gestión de Seguridad de la Información (SGSI). | Organizar la gobernanza y gestión de TI empresarial. | Estandarizar y regular la seguridad de los sistemas de automatización y control industrial. |
| **Estructura** | Cinco funciones: Identificar, Proteger, Detectar, Responder, Recuperar. | Especifica requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI. | Cinco principios y siete habilitadores con un modelo de referencia de procesos. | Separado en diferentes estándares enfocados en diferentes aspectos de los sistemas de control industrial. |
| **Certificación** | No cuenta con programa de certificación. | Certificación disponible. | Autoevaluación COBIT, no hay certificación formal. | No cuenta con programa de certificación. |
| **Industrias Primarias** | Todas las industrias. | Todas las industrias. | Principalmente gestión de TI en todas las industrias. | Sistemas de control industrial en todas las industrias. |
| **Flexibilidad** | Altamente flexible y personalizable. | Requiere evaluación de riesgos y permite personalización. | Adaptable para las necesidades específicas de la organización. | Personalizable basado en los sistemas de control industrial específicos. |
| **Enfoque** | Enfoque basado en riesgos. | Enfoque basado en riesgos. | Enfoque orientado a procesos. | Enfoque de defensa en profundidad. |
| **Gestión de Riesgos** | Componente explícito de gestión de riesgos. | Parte integral del SGSI, clave para definir el alcance. | Gestión de riesgos explícita, formando parte de la gobernanza y gestión de TI empresarial. | Incorporado, pero más enfocado en la seguridad y protección de los sistemas. |

Elaboración propia en base a NIST (2020), ISO (2022), ISACA (2019), ISA (2018)

## 3.6 ESTRATEGIAS DE CIBERSEGURIDAD PARA LOS SISTEMAS PORTUARIOS

Para desarrollar una estrategia de ciberseguridad en el ámbito portuario se necesita de un plan de gestión de riesgos cibernéticos, esta es una labor que toma tiempo y planificación y su implementación requiere de la participación del liderazgo ejecutivo. Es vital que el enfoque de este proyecto se alinee con los planes operacionales generales de los puertos, considerándose los requisitos específicos de las actividades administrativas y operativas.

La estrategia de ciberseguridad portuaria tiene la obligación de incluir las metas para integrar y desarrollar las capacidades de seguridad cibernética en los entornos operativos, siendo esta de alto nivel y lo suficientemente flexible para acomodar tanto los cambios tecnológicos como las amenazas emergentes. Los requisitos regulatorios por parte de nuevas legislaciones deben ser reconocidos e incorporados en el programa establecido. Una vez definido el enfoque del plan, se puede implementar la estrategia de gestión de riesgos cibernéticos.

El plan de ciberseguridad ha de considerar, reconocer y abordar las amenazas y vulnerabilidades identificadas durante el proceso de planificación ejecutiva, como la existencia de redes no segmentadas, entes u organizaciones externas y la presencia de peligros cibernéticos previamente mencionados. La estructura diseñada debe poseer mecanismos de retroalimentación para ser efectivo, ya que el campo de la tecnología se encuentra evolucionando constantemente.

Para desarrollar la estrategia y el plan, la organización debe buscar entender sus riesgos específicos a través de la aplicación de evaluaciones que contemplen e identifiquen las amenazas. Si bien no hay una única solución correcta para dar respuesta a la gestión de riesgos cibernéticos, las consideraciones específicas que buscan cumplir con las necesidades de la industria son:

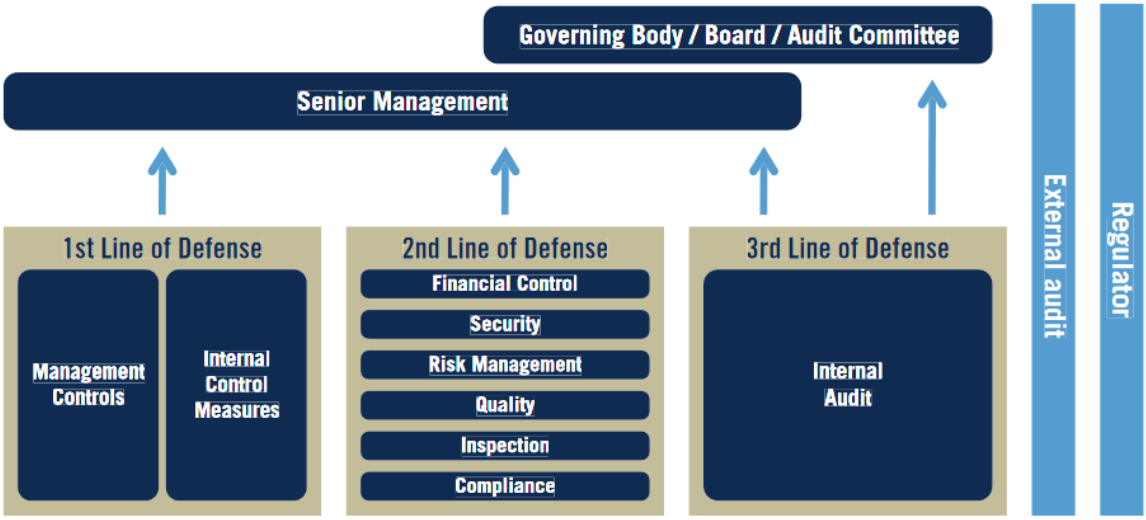
1. Identificar e incorporar controles de ciberseguridad a partir de un marco de ciberseguridad testeado, el instaurado por el NIST, ISO/IEC, COSO y COBIT (Jarjoui & Murimi, 2021).
2. Utilizar “Defense-in-Depth” (defensa en profundidad) para asegurar los accesos vía distintas capas o layers de seguridad, tanto físicas como por permisos o segmentación (Security, 2022).

La defensa en profundidad aprovecha la implementación de múltiples capas de controles de seguridad en una red dependiente de los sistemas de TI. Este paradigma se logra mediante la superposición de varias medidas de protección, de manera que proporcionen redundancia al sistema. Estas regulaciones cubren distintas áreas tal como física (resguardo de perímetro, CCTV), técnicas (hardware, autenticación, encriptación) y administrativas (políticas internas y procedimientos).

### 3.6.1 MODELO DE TRES LÍNEAS

El modelo de tres líneas es una estructura diseñada para facilitar la gestión de riesgos dentro de una organización, esta se divide en tres áreas principales.

Ilustración 3.6.1: Gráfica de Modelo de tres líneas




Fuente: IIA,2020

La primera línea de defensa tiene la tarea de poner en práctica los controles de seguridad y las acciones basadas en los principios y mejores prácticas de la ciberseguridad, tal como se plantea en el marco de gestión de riesgos que la organización ha implementado (IIA, 2020). Por ejemplo, pueden incluirse normativas que los usuarios deben cumplir al crear contraseñas. Los encargados de la ciberseguridad deberán asegurar de que los usuarios sigan los protocolos establecidos.

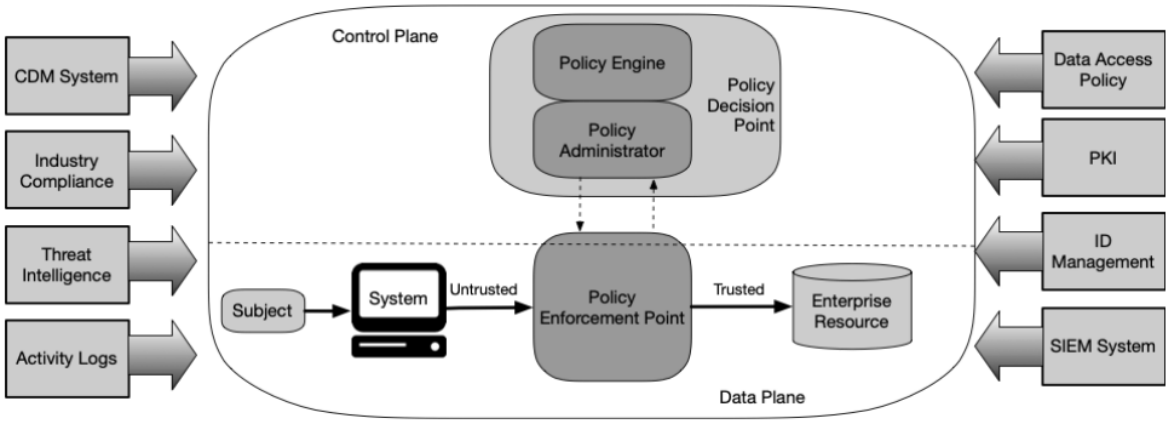
La segunda línea de defensa utiliza las mejores prácticas que respaldan las acciones centradas en la gestión de riesgos. Estas actividades están diseñadas para desarrollar, facilitar y supervisar la efectividad de los controles de la primera línea de defensa (Deloitte, 2021). Esto tiene la posibilidad de variar entre puertos porque dependen del nivel de integración que este posee, una organización puede tener múltiples roles de cumplimiento que cubren seguridad (Código ISPS), privacidad de datos, financiera y la cadena de suministro.

La tercera línea de defensa corresponde a la auditoría interna que puede verificar junto con la segunda línea, dependiendo de lo establecido en la gestión de riesgos y si estas actividades son llevadas a cabo por la primera línea (IIA, 2020).

## 3.6.2 ESTRUCTURA DE CERO CONFIANZA

La estructura de cero confianza es un paradigma de la ciberseguridad, el cual se enfoca en que la fiabilidad de acceso nunca se entrega de forma implícita y debe ser continuamente evaluada (NIST, 2020), este mecanismo apunta a una modalidad de aplicación más técnico que el modelo de tres líneas, pero representa una serie de puntos de validación que lo hacen un sistema efectivo.

Ilustración 3.6.2: Componentes de Cero Confianza




Fuente: NIST, 2020

Entre los componentes más importantes de esta estructura se encuentran los siguientes:

A. **Identidad de usuario:** Cada usuario tiene una identidad única que se pueda autenticar con seguridad antes de acceder a cualquier recurso.
B. **Autenticación fuerte:** Un método de verificación la identidad de un usuario, normalmente a través de la autenticación multifactorial.
C. **Autorización de mínimo privilegio:** Esto significa dar a los usuarios o entidades solo el nivel de acceso que necesitan para realizar sus tareas y nada más.
D. **Segmentación de la red:** En lugar de confiar en un perímetro de red seguro, la arquitectura de cero confianza divide la red en segmentos para limitar el movimiento lateral de las posibles amenazas.
E. **Evaluación continua de la seguridad:** Se ejecuta un seguimiento constante de la actividad en la red y se evalúa la confianza en tiempo real.

Las mejores prácticas de defensa en profundidad se basan en el principio de crear varios escalones de protección para dificultar el acceso no deseado de una entidad agresora. Dichas capas brindan múltiples oportunidades para proteger, detectar y responder a un evento. Cuando una capa defensiva falla o es superada por un agresor, las capas restantes aseguran que la organización todavía puede detener la situación en desarrollo. Por ejemplo, el firewall provee una medida de defensa para la organización, ya que este prohíbe ciertos accesos y asegura que la comunicación sea monitoreada. En el caso de que un atacante logre superar el firewall, una segunda capa de defensa, como el resguardo de puntos finales, proporcionando otro obstáculo al autor de los ataques.

# 4. METODOLOGÍA

El propósito de este estudio es entender a detalle los desafíos y las soluciones en ciberseguridad de los sistemas portuarios. Dada la naturaleza del tema, se ha optado por un enfoque cualitativo de investigación, que permite explorar a profundidad las experiencias, las perspectivas y las prácticas de las empresas portuarias en relación con la ciberseguridad.

## 4.1 DISEÑO DE LA INVESTIGACIÓN

La investigación se basa en un enfoque de estudio de caso, mediante el cual se busca obtener una comprensión detallada de la ciberseguridad en los sistemas portuarios. Este método involucra la recolección de datos cualitativos a través de entrevistas y cuestionarios a empresas relacionadas con las operaciones portuario-logísticas en el puerto de Valparaíso.

La metodología del estudio implica una serie de pasos esenciales. Primero, se identifican las vulnerabilidades y debilidades de seguridad cibernética del puerto. El proceso facilita evaluar el impacto potencial de un ataque a la infraestructura crítica, las operaciones y la reputación de la organización. A continuación, se desarrollará un marco de evaluación de riesgos que permitirá determinar la probabilidad y la gravedad de diferentes amenazas. Este procedimiento también ayudará a identificar los activos y sistemas críticos que necesitan protección.

El estudio también incluirá un evaluación de los marcos, reglamentos y normativas de seguridad cibernética relevantes que se aplican a la industria marítima, así como las normas o regulaciones específicas desarrolladas por la autoridad portuaria o las agencias gubernamentales. Se elaborará un conjunto de recomendaciones y directrices para las organizaciones correspondientes y las partes interesadas con el fin de mejorar la resiliencia y seguridad del sistema portuario frente a las amenazas. Este marco propuesto se basará en los hallazgos de la investigación y abordará las áreas críticas de la ciberseguridad, incluyendo la gestión de riesgos, la respuesta a incidentes, el control de acceso y la protección de la red.

## 4.2 SELECCIÓN DE PARTICIPANTES

Para este estudio, se han seleccionado como participantes a diez empresas que forman parte del sistema logístico portuario en Valparaíso, uno de los puertos más importantes y concurridos de Chile. Estas organizaciones han sido elegidas por su papel vital en el funcionamiento y la gestión del puerto, proporcionando así una visión diversa y representativa de las prácticas y desafíos de ciberseguridad en la estructura portuaria de Valparaíso.

La selección de los participantes se ha realizado con base en su tamaño, su función dentro del sistema logístico portuario, su grado de exposición a los riesgos cibernéticos y su papel en la implementación de medidas de ciberseguridad. En este sentido, se han incluido

organizaciones que ofrecen una variedad de prestaciones logísticas, como agencias de naves, empresas de almacenamiento, transporte, servicios de información y entes estatales.

Para cada empresa seleccionada, se han identificado los individuos que cumplen un papel clave en la gestión de la ciberseguridad. Estos incluyen encargados de seguridad (PFSO), gerentes de TI y otros responsables de la implementación y supervisión de las medidas de ciberseguridad. De esta forma la investigación nos permite obtener una visión detallada de las estrategias de ciberseguridad, los desafíos y las soluciones que se implementan para superar las vulnerabilidades.

La selección de las diez empresas y sus respectivos responsables de ciberseguridad proporciona una base sólida para la investigación y permite explorar a fondo las prácticas y desafíos de ciberseguridad en el sistema portuario de Valparaíso. Sin embargo, es fundamental tener en cuenta que, aunque estas organizaciones son representativas del sistema logístico portuario en Valparaíso, sus experiencias y conductas pueden no ser generalizables a todos los sistemas portuarios.

## 4.3 RECOLECCIÓN Y ANÁLISIS DE DATOS

Para recoger los datos necesarios para el estudio, se utilizarán dos instrumentos principales: entrevistas y análisis de literatura relevante.

Las entrevistas serán semiestructuradas, permitiendo una conversación abierta con los participantes, pero también asegurando que ciertos asuntos clave sean abordados. Estas se realizarán con directores de seguridad, encargados de TI y otros responsables de la ciberseguridad en las empresas del rubro logístico seleccionadas. Las preguntas de la entrevista se centrarán en temas como la percepción del riesgo cibernético, las estrategias de implementadas y los desafíos y las oportunidades en la mejora de esta área.

El análisis de literatura se centrará en los desarrollos tecnológicos, normativos y de seguridad desde el año 2018, debido a que este es un campo en constante cambio, se establece un máximo de 5 años para la recopilación de información vía estudios. Esta revisión se enfocará en artículos de revistas de investigación y tecnología.

Para el estudio de la información recopilada a través de entrevistas en esta investigación cualitativa, se adoptará un enfoque de análisis temático. Este es un método flexible y útil para identificar, analizar e informar patrones o temas dentro de los datos.

El primer paso del procedimiento es la transcripción y preparación de la información, todas las entrevistas serán grabadas con el consentimiento de los participantes y posteriormente transcritas para su análisis. Esto permite convertir la información recolectada a un formato que sea fácilmente manejable y analizable. Una vez que las respuestas se encuentren preparadas, se comparan cuidadosamente, este proceso de familiarización es esencial para obtener una comprensión profunda del contenido de los datos y del contexto en el que estas se producen.

Se le asignan rótulos descriptivos a segmentos específicos de la información que representan una idea o un concepto único. Estas etiquetas ayudan a resumir y categorizar los datos, facilitando el reconocimiento de tendencias y temáticas emergentes. Un tema se considera un patrón de respuesta o significado dentro del conjunto de datos. Los temas pueden surgir de las etiquetas ya designadas o a través de patrones en las respuestas de las entrevistas.

La revisión es un proceso iterativo en el que se refinan los temas identificados y se establecen como puntos coherentes. Durante esta etapa, se verifica si la información puede ser combinada, descartada por completo o redestinada a algún otro tema. Después de revisar las temáticas, se procede a definir y nombrarlos. En este paso, se identifica el núcleo de lo que cada tema representa y se determina cual aspecto de los datos captura.

El último paso en el proceso de evaluación de datos es la elaboración del informe de los hallazgos. Esta es la etapa en la que se transforma el análisis en una narrativa coherente y significativa.

## 4.4 CONSIDERACIONES ÉTICAS

Durante todo el proceso de investigación, se seguirán estrictas pautas éticas para garantizar la privacidad y confidencialidad de los participantes. Las empresas y los individuos participes en el estudio serán informados de los propósitos, procedimientos y usos de la información, para esto se les pedirá su consentimiento antes de participar. Además, todas las respuestas son tratadas de forma anónima y confidencial.

Esto implica realizar una revisión exhaustiva de las medidas, políticas y procedimientos de seguridad cibernética y evaluar su eficacia para mitigar los riesgos que asociados amenazas cibernéticas. La investigación también evaluará el nivel de conciencia de los peligros entre el personal del puerto y las partes interesadas, así como su preparación para responder a un ataque cibernético.

# 5. RESULTADOS

## 5.1 NIVEL DE CONCIENCIA SOBRE LA CIBERSEGURIDAD

La investigación reveló que el grado de conciencia y capacitación en ciberseguridad entre las entidades que operan en el sistema portuario de Valparaíso es más bajo de lo que se consideraría óptimo. A pesar de los avances tecnológicos y la creciente digitalización de las operaciones portuarias, el nivel de comprensión sobre los riesgos y amenazas cibernéticas es limitado.

En particular, los participantes expresaron preocupación por el alto riesgo asociado con los ataques de phishing y la apertura de enlaces peligrosos. A pesar de que estos son conocidos vectores comunes para atentar contra la integridad de la seguridad, los entrevistados indicaron que tanto la conciencia como la capacitación con relación a estas amenazas específicas son insuficientes.

Las prácticas seguras en línea y la capacidad para reconocer y manejar los intentos de phishing son fundamentales para la seguridad de cualquier red informática y este parece ser un área de particular vulnerabilidad para el sistema portuario de Valparaíso.

Esta falta de conocimientos y preparación pone de manifiesto la necesidad de una mayor formación y concienciación en ciberseguridad. Es esencial que las empresas de la industria logístico-portuaria se comprometan a formar a su personal en estas áreas críticas, para garantizar no solo la seguridad de sus propias operaciones, sino también la integridad y protección del sistema portuario en su conjunto.

La inversión en capacitación en ciberseguridad, la sensibilización sobre los riesgos y la promoción de una cultura de prevención son esenciales para mitigar estas amenazas. El fortalecimiento de la resiliencia de las operaciones portuarias en Valparaíso pasa por una apuesta decidida en el conocimiento y la formación en seguridad cibernética.

## 5.2 VULNERABILIDADES CIBERNÉTICAS

A través de las entrevistas realizadas, se pudo identificar una serie de susceptibilidades críticas en la seguridad cibernética en el sistema logístico de Valparaíso. En primer lugar, el error humano fue señalado como una de las principales vulnerabilidades. Este factor subraya aún más la necesidad de una mayor formación y concienciación en ciberseguridad, para minimizar los riesgos asociados a la interacción insegura de los usuarios con los sistemas digitales.

En segundo punto, se destacó la presencia de firmware y hardware anticuados en algunas partes del sistema portuario. Este problema no solo aumenta la vulnerabilidad a ataques cibernéticos, sino que también limita la capacidad de la infraestructura existente para soportar las últimas medidas de seguridad. Es vital que se efectúen inversiones para actualizar estos sistemas y reducir el riesgo.

Además, la complejidad de la estructura logística, compuesta por numerosas organizaciones y empresas, también se identificó como una fuente significativa de vulnerabilidad. Dada la interdependencia de las entidades que forman parte de este sistema, un ataque a una sola organización o empresa puede tener un efecto dominó, ralentizando o incluso paralizando las operaciones del puerto.

Esta realidad subraya la necesidad de una estrategia de seguridad cibernética integral y coordinada que abarque la totalidad de los integrantes interesados dentro del sistema portuario. Una perspectiva fragmentada no solo es insuficiente, sino que también podría exacerbar las vulnerabilidades existentes. Es imperativo que todas las organizaciones y empresas implicadas en el sistema portuario adopten un enfoque unificado y coherente para la gestión de la ciberseguridad, reconociendo que la seguridad del sistema en su conjunto depende de la seguridad de cada una de sus partes.

## 5.3 INTEGRACIÓN DE LA CIBERSEGURIDAD EN LA GESTIÓN DE RIESGOS

Los datos recolectados a través de las entrevistas indican un avance progresivo en la integración de la ciberseguridad dentro del marco de gestión de riesgos de diversas organizaciones que forman parte del sistema portuario. Sin embargo, dicha incorporación ha mostrado un alcance limitado hasta la fecha, enfocándose en aspectos aislados y específicos de la ciberseguridad.

Se observa una propuesta de expansión de esta integración, particularmente en entidades de mayor tamaño. Este avance es crucial, ya que permitirá a estas organizaciones adquirir una comprensión sistemática y exhaustiva de los riesgos cibernéticos a los que están expuestos, posibilitando el desarrollo de medidas de mitigación más eficientes.

A pesar de estos avances, algunos de los entrevistados admitieron que sus respectivas organizaciones aún no han reconocido la necesidad de integrar la ciberseguridad en su gestión de riesgos. No obstante, coinciden en que la reciente auge de ataques en nivel internacional obligará a sus gerencias a incorporar la ciberseguridad en su gestión de riesgos en el futuro próximo.

Estas percepciones enfatizan la necesidad de un cambio de paradigma y un mayor compromiso por parte de todas las entidades que conforman el sistema portuario, en el sentido de considerar a la ciberseguridad como un componente esencial de su gestión de riesgos. Esta modificación implica reconocer que la ciberseguridad no es simplemente un asunto técnico que puede ser relegado a los profesionales de TI, sino una cuestión estratégica con implicancias a nivel de toda la organización que requiere de dedicación y la atención de la alta dirección.

## 5.4 POLÍTICAS Y NORMATIVAS VIGENTES

A través de las entrevistas realizadas a representantes del sector privado, se identificó una ausencia de confianza hacia el statu quo en relación con la promoción de legislación y regulación eficaz en el sector de la ciberseguridad. Este escepticismo se fundamenta en una percepción de falta de conciencia o entendimiento por parte del estado respecto a los efectos negativos que los ataques de ciberseguridad pueden infligir en la cadena logística de la región de Valparaíso y el resto de Chile. Esta situación se atribuye a la naturaleza compleja y dinámica de la ciberseguridad, la cual demanda un enfoque proactivo y conocimientos técnicos especializados. Por el contrario, las entrevistas realizadas con el sector público reflejaron una visión optimista en este tema. Estos sujetos sostuvieron que se están haciendo esfuerzos continuos para modernizar las tecnologías y estándares vigentes en la ciberseguridad. Esta diferencia en las percepciones puede ser explicada por la posición privilegiada de estos individuos, quienes se encuentran en una situación más propicia para observar y apreciar los avances realizados en el ámbito mencionado.

Sin embargo, tanto la perspectiva de la industria privada como la del área pública enfatizan la necesidad de mejorar y actualizar continuamente las políticas y normativas relacionadas con la ciberseguridad. Esta tarea es fundamental para proteger la cadena logística del país y requiere de un compromiso y esfuerzo conjunto entre el sector público y privado. El entendimiento y la conciencia acerca de la importancia de la ciberseguridad deben ser promovidos a todos los niveles para garantizar una defensa efectiva contra las crecientes amenazas cibernéticas.

# 6. MARCO DE CIBERSEGURIDAD

El marco de ciberseguridad funciona como un documento que orienta y guía la toma de decisiones en los sistemas de gestión, para así reducir los riesgos asociados a las operaciones que involucren sistemas de información, para esto se deben establecer los riesgos con los cuales se van a trabajar.

## 6.1 EVALUACIÓN DE RIESGOS

Utilizando la información recopilada mediante las entrevistas y la literatura moderna con relación a las amenazas emergentes, se genera una tabla de riesgos y su matriz correspondiente para visualizar las amenazas asociadas a la ciberseguridad en el rubro logístico-portuario:

Tabla 6.1: Riesgos de Ciberseguridad

| Grupo Riesgo | Subgrupo | Riesgo | Riesgo | Probabilidad Inherente | Impacto Inherente |
|---|---|---|---|---|---|
| Procesos de TI | Disponibilidad | R1 | Ataques de fuerza bruta | Improbable (2) | Insignificantes (1) |
| Procesos de TI | Integridad | R2 | Inyecciones SQL | Improbable (2) | Menores (2) |
| Procesos de TI | Infraestructura | R3 | Ataques DDoS | Moderado (3) | Menores (2) |
| Procesos de TI | Acceso | R4 | Ingeniería Social | Moderado (3) | Menores (2) |
| Procesos de TI | Acceso | R5 | Phishing | Moderado (3) | Moderadas (3) |
| Procesos de TI | Disponibilidad | R6 | Malware | Probable (4) | Mayores (4) |
| Procesos de TI | Disponibilidad | R7 | Ransomware | Probable (4) | Catastrófica (5) |
| Procesos de TI | Acceso | R8 | Manipulación de autorizaciones | Improbable (2) | Mayores (4) |

Elaboración propia basándose en entrevistas

El proceso de evaluación apunta a entender e identificar los riesgos a los sistemas, activos y capacidad operativa del puerto, para esto se utiliza la primera función del framework NIST, identificar, la cual busca a precisar y determinar los procesos de los siguientes puntos:

A. Gestión de activos
B. Entorno empresarial
C. Gobernanza
D. Evaluación de riesgos
E. Estrategia de control de riesgos
F. Gestión de riesgos en la cadena de suministros

Se identifican los datos, dispositivos, personal, sistemas e infraestructura que permiten la correcta operación de la organización, alineando estos activos con la estrategia de riesgos que posee el puerto.

Tabla 6.2: Gestión de Activos (ID.AM)

| Subcategoría NIST | Aplicación |
|---|---|
| **ID.AM-1**: Se hará inventario de los dispositivos físicos y sistemas dentro de la organización. | • Computadores / Servidores<br>• Aparatos celulares<br>• Cámaras CCTV<br>• Lectores RFID<br>• Sensores dedicados<br>• Equipos de red<br>• Controles de acceso<br>• Grúas y vehículos automatizados<br>• Sistemas de navegación |
| **ID.AM-2:** Identificar Las plataformas de software y aplicaciones dentro de la organización. | • Sistema de gestión de puerto (PMS)<br>• Recursos empresariales (ERP)<br>• Gestión de operación de terminales (TOS)<br>• Sistema de información geográfica (GIS)<br>• Sistema de seguridad<br>• Gestión de mantenimiento (CMMS) |
| **ID.AM-3:** Se mapean los flujos de comunicación y datos de la organización | Identificación de transmisión de información, formulación de políticas, protocolos y control de transferencia de información. |
| **ID.AM-4:** Se catalogan los sistemas de información externos. | • Identificación automática (AIS)<br>• Sistema de Aduanas<br>• DIRECTEMAR<br>• Autoridad Portuaria |
| **ID.AM-5:** Los recursos se priorizan en función de su clasificación, criticidad y valor comercial. | Clasificación de la información manejada por la empresa en relación con sus requisitos legales, de su valor y del nivel de operatividad crítica. |
| **ID.AM-6:** Se establecen roles y responsabilidades de ciberseguridad para la fuerza laboral. | Asignación de responsabilidades en las jefaturas correspondientes, formulando planes de contingencia relacionados con los aspectos de ciberseguridad. |

Elaboración propia basada en Framework V1.1 Core

Se identifican aspectos del entorno empresarial, priorizando la misión, objetivos, stakeholders y las actividades de la organización, utilizando esta información se establecen las responsabilidades y roles afectos a la gestión de riesgos de ciberseguridad.

Tabla 6.3: Entorno Empresarial (ID.BE)

| Subcategoría NIST | Aplicación |
|---|---|
| **ID.BE-1:** Identificación de la organización en la cadena de suministro | El puerto de Valparaíso es parte de la cadena de suministros con un amplio impacto en la logística de la Región de Valparaíso, Metropolitana y la Región de O'Higgins. |
| **ID.BE-2:** Identificación del lugar de la organización en la infraestructura crítica. | Los puertos marítimos en Chile corresponden a infraestructura crítica por su importancia en el movimiento de activos, energía y alimentos, además de ser la principal vía de entrada y salida de estos. |
| **ID.BE-3:** Se establecen las prioridades de la misión organizacional, los objetivos y las actividades. | La organización debe ser consecuente con su misión, considerando la seguridad de la información y el riesgo asociado a las operaciones, activos, individuos u otras organizaciones. |
| **ID.BE-4**: Se establecen las dependencias y las funciones críticas para la entrega de servicios. | • Servicios de navegación y pilotaje<br>• Servicios de aduanas<br>• Inspección sanitaria/fitosanitaria<br>• Servicios de seguridad<br>• Servicios de remolcadores<br>• Abastecimiento<br>• Manejo de basura/residuos<br>• Estibadores |
| **ID.BE-5**: Se establecen los requisitos de resiliencia para soportar la entrega de servicios críticos en todos los estados operativos. | Establecer un plan de contingencia para la información que se base en las funciones críticas del puerto, incluyendo los objetivos de recuperación, prioridades y las métricas correspondientes, utilizando los roles y responsabilidades asignados. |

Elaboración propia basada en Framework V1.1 Core

Se procede a identificar las políticas, procedimientos, procesos de administración y los requisitos de las regulaciones legales, de riesgo, ambientales y operativas del puerto, para así desarrollar de forma holística el proceso de gestión de riesgo de ciberseguridad.

Tabla 6.4: Gobernanza (ID.GV)

| Subcategoría NIST | Aplicación |
|---|---|
| **ID.GV-1:** Se establece la política de seguridad de la información organizacional. | Se genera una política de seguridad de información con base en la confidencialidad, integridad, disponibilidad, cumplimiento y responsabilidad. |
| **ID.GV-2:** Las responsabilidades de seguridad de la información se coordinan y alinean con los roles internos y los socios externos. | Establecer las responsabilidades del director de seguridad de información, equipo de TI y de todos los trabajadores dentro de la organización, además de proveedores externos y clientes, esto incluye, pero no se limita a uso de redes, permisos de acceso, gestión de contraseñas y respuestas ante incidentes. |
| **ID.GV-3:** Se comprenden y se gestionan los requisitos legales y regulatorios en materia de ciberseguridad, incluyendo las obligaciones de privacidad y libertades civiles. | Establecer las responsabilidades legales mediante un equipo legal interno que analiza y asesore a las distintas áreas de la organización para el cumplimiento de las normas, esto seguido por la capacitación del personal y el empleo de auditorías para la verificación del cumplimiento con las leyes. |
| **ID.GV-4**: Los procesos de gobernanza y gestión de riesgos abordan los riesgos de ciberseguridad. | Los procesos de gestión de riesgos abordan temas de ciberseguridad mediante la identificación, evaluación, monitoreo y reportes de riesgos, estos informan sobre la situación actual para así generar respuestas a estos. |

Elaboración propia basada en Framework V1.1 Core

En la evaluación de riesgos se establecen los riesgos de ciberseguridad para las operaciones del puerto, los activos y las personas.

Tabla 6.5: Evaluación de Riesgos (ID.RA)

| Subcategoría NIST | Aplicación |
|---|---|
| **ID.RA-1:** Se identifican y documentan las vulnerabilidades de los activos. | Se evalúa de manera periódica los sistemas de IT para identificar vulnerabilidades, tanto en forma de software obsoleto, servicios discontinuados, configuraciones inseguras o mal uso de dispositivos. |
| **ID.RA-2:** Se recibe información de amenazas cibernéticas y de vulnerabilidad | La organización participa en el intercambio de información relevante a la ciberseguridad, tanto de fuentes dedicadas |

| | |
|---|---|
| de los foros y fuentes de intercambio de información. | a materias de ciberseguridad como otras organizaciones portuarias. |
| **ID.RA-3:** Se identifican y documentan las amenazas, tanto internas como externas. | Se evalúan las amenazas, considerando posibles actores internos y externos que puedan afectar los procesos de seguridad, tanto de forma deliberada o accidental. |
| **ID.RA-4:** Se identifican los posibles impactos comerciales. | Se genera un análisis de impacto para el puerto, así identificando como las amenazas y las vulnerabilidades podrían afectar los procesos operacionales del puerto. |
| **ID.RA-5**: Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo. | Se genera una matriz de riesgo importante para la organización, esta deberá comprender las amenazas cibernéticas ya mencionadas con sus impactos y probabilidades. |
| **ID.RA-6:** Se identifican y priorizan las respuestas al riesgo. | Se deben identificar las respuestas correspondientes a cada amenaza, estas pueden abarcar protocolos de mitigación, transferencia, aceptación o evitación del riesgo. |

Elaboración propia basada en Framework V1.1 Core

El puerto genera prioridades, restricciones, tolerancia a los riesgos y las suposiciones son establecidas para apoyar las decisiones de riesgo operacional.

Tabla 6.6: Estrategia de Gestión de Riesgos (ID.RM)

| Subcategoría NIST | Aplicación |
|---|---|
| **ID.RM-1:** Se establecen, gestionan y acuerdan los procesos de gestión de riesgos con miembros organizacionales | Se generan instancias en las cuales distintas áreas de la organización puedan acordar los procesos de gestión de riesgo relacionados a la ciberseguridad, este punto de control refuerza la gestión desarrollada por la alta dirección. |
| **ID.RM-3**: La determinación de la tolerancia al riesgo de la organización se basa en su papel en la infraestructura crítica y en el análisis de riesgos específicos del sector | El puerto de Valparaíso es de alta importancia para la economía local y nacional, siendo parte de la infraestructura crítica del país, debido a esto la tolerancia de riesgos es baja, por ende, todos los niveles de la organización deben cumplir con los procesos de seguridad establecidos. |

Elaboración propia basada en Framework V1.1 Core

Tabla 6.7: Gestión de Riesgos de la cadena de suministros (ID.SC)

| Subcategoría NIST | Aplicación |
|---|---|
| **ID.SC-1:** Se identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión de riesgos de la cadena de suministro cibernético por parte de los stakeholders. | Se establece un proceso de gestión de riesgos de la cadena de suministro que incluye la evaluación de la ciberseguridad de los proveedores, la inclusión de requisitos de ciberseguridad en los contratos y la supervisión continua de la ciberseguridad de estos. |
| **ID.SC-2:** Identificar, priorizar y evaluar a los proveedores y socios de sistemas de información críticos, componentes y servicios utilizando un proceso de evaluación de riesgos de la cadena de suministro cibernético | Se identifican los proveedores de sistemas de información, tal como acceso a redes, servicios de red de telecomunicaciones, software portuario, entre otros, para luego priorizarlos dependiendo de su importancia para las operaciones portuarias. |
| **ID.SC-3:** Los proveedores y socios están obligados por contrato a implementar medidas adecuadas diseñadas para cumplir con los objetivos del programa de SGSI o del Plan de gestión de riesgos de la cadena de suministros | En contratos y negocios con proveedores de servicio se establecen cláusulas que obligan la implementación de procesos de ciberseguridad adecuados, estos pueden ser variados desde uso de ciertas plataformas de comunicación hasta protocolos de reacción para mantener el proceso operacional. |
| **ID.SC-4:** Supervisión de los proveedores y socios para confirmar que han cumplido con sus obligaciones según lo requerido | Se realizan auditorías periódicas de los proveedores para garantizar el cumplimiento de las cláusulas pactadas. |
| **ID.SC-5:** Planificación, pruebas de respuesta y recuperación se efectúa con proveedores/prestadores de servicios críticos | Se desarrollan planes de respuesta y recuperación en caso de ataques cibernéticos, estos deben ser transversales en la cadena logístico-portuario de Valparaíso para asegurar la continua operación. |

Elaboración propia basada en Framework V1.1 Core

## 6.2 DESARROLLO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El desarrollo del SGSI es un paso fundamental de la implementación de la ISO 27001, para esto se deben definir los roles y responsabilidades de la seguridad de información a nivel transversal dentro del puerto, adicionalmente se debe establecer el contexto organizacional identificando los stakeholders con sus necesidades y expectativas. Una vez definido se utiliza como base para generar una política de seguridad de información, respondiendo a los requisitos tanto del puerto como a los de la cadena logística regional que dependen de las operaciones portuarias.

La alta gerencia deberá determinar el alcance del SGSI, nominando que información, ubicaciones y tecnologías serán incluidos en el sistema para así realizar una evaluación de

riesgos y los controles necesarios para atender y tratar posibles eventos considerados dentro del SGSI. Los controles óptimos para resolver amenazas a la ciberseguridad corresponden a los delineados por el NIST, ya que se enfocan al área técnica de la ciberseguridad. Las herramientas seleccionadas son implementadas, de esta forma se establecen procedimientos correspondientes.

El SGSI debe contemplar la formación e instrucción de seguridad de la información a todos los miembros de la organización, desarrollando una cultura de seguridad a través de campañas de concienciación. El monitoreo y medición de los controles de seguridad implementados se realiza por medio de auditorías internas, revisión de los controles y mediante los indicadores correspondientes a cada control. Utilizando los resultados de las evaluaciones de efectividad de los controles, se identifican las posibles mejoras al sistema, tal como modificaciones o implementación de nuevos controles, verificación de roles y responsabilidades.

Se establecen y se aplican los procesos para la gestión de incidentes de información, incluyendo la identificación y clasificación de los eventos, la respuesta a estos, la investigación, análisis de las causas y la implementación de acciones correctivas para prevenir la recurrencia de situaciones similares. Adicionalmente, se integra la gestión de la continuidad del negocio en el SGSI para asegurar que los procesos críticos y los datos relevantes para la organización se encuentren disponibles en caso de ataques cibernéticos que puedan causar una interrupción a las operaciones.

El sistema de gestión puede incluir adicionalmente los sistemas de profundidad y cero confianza para reforzar la seguridad de los activos de la empresa, considerando que este uso de tecnología es compatible con la implementación de controles y representan metodologías eficientes en el proceso de seguridad cibernética.

## 6.3 IMPLEMENTACIÓN DE CONTROLES

El Anexo A de la ISO 27001 proporciona un conjunto de controles de seguridad de la información, de los cuales los más relevantes para la aplicación en el puerto de Valparaíso corresponden a:

A. **A.9 Control de acceso**: Controles basados en la autenticación de dos factores para los sistemas críticos, asignación de acceso basada en el principio de mínimo privilegio y el uso de registros de auditoría para rastrear todas las actividades de los usuarios utilizando las estrategias de cero confianza.
B. **A.12 Operaciones de seguridad**: Controles como la protección contra malware, la gestión de las vulnerabilidades técnicas y los procedimientos de respaldo.
C. **A.13 Seguridad en las comunicaciones**: Controles estableciendo encriptación para proteger los datos y procedimientos para el intercambio seguro de información.
D. **A.14 Adquisición, desarrollo y mantenimiento de sistemas de información**: Controles como los requisitos de seguridad en las especificaciones de los sistemas de información y los procedimientos de pruebas de seguridad, asegurándose de mantener los sistemas actualizados en materia de seguridad.
E. **A.16 Gestión de incidentes de seguridad de la información**: Controles como las responsabilidades y procedimientos en caso de incidentes de seguridad, la

notificación de los eventos de seguridad y la recopilación de información posterior a algún evento.

F. **A.17 Aspectos de la continuidad del negocio de la seguridad de la información**: Controles como la identificación de los requisitos de la continuidad del negocio y la implementación de un plan de continuidad del negocio.

Los controles basados en el NIST CFS 1.1 y definidos específicamente en la publicación especial NIST 800-53 rev.5 (NIST, 2020), se enfocan principalmente en la tríada de confidencialidad, integridad y disponibilidad, por lo que se pueden definir como controles enfocados en las necesidades operativas que los controles de gestión de la ISO 27001, entre los más relevantes para su aplicación se encuentran los siguientes:

A. **Acceso (AC)**: Controles que ayudan a limitar y controlar el acceso a sistemas y recursos de información basados en roles y responsabilidades definidos, como Gestión de cuentas (AC-3) y Mínimo privilegio (AC-6).
B. **Conciencia y Capacitación (AT)**: Estos controles aseguran que el personal del puerto esté adecuadamente capacitado y consciente de las amenazas cibernéticas, como los controles de Concienciación de seguridad (AT-2) y Capacitación en base de roles (AT-3).
C. **Auditoría y Responsabilidad (AU)**: Controles que proporcionan mecanismos para responsabilizar a los usuarios y rastrear las actividades del usuario en el sistema, como Auditoría de eventos (AU-2), Revisión de registros (AU-6) y Protección de información de auditoría (AU-9).
D. **Evaluación, Autorización y Monitoreo (CA)**: Estos controles ayudan a determinar la eficacia de los controles de seguridad implementados y a identificar deficiencias de seguridad, como evaluación de controles (CA-2), Intercambio de información (CA-3) y Monitero Continuo (CA-7).
E. **Gestión de Configuración (CM)**: Ayudan a establecer y mantener la integridad de los productos y sistemas de tecnológicos, a través del control de las configuraciones, entre estos controles se cuenta con el Control de configuración base (CM-2), Configuración de cambio de controles (CM-3) y Restricción de acceso a configuraciones (CM-5).
F. **Planificación de Contingencias (CP)**: Estos controles ayudan a garantizar que la organización pueda recuperarse y continuar operando en caso de una interrupción o ataque que afecte las operaciones, estos controles incluyen Plan de contingencia (CP-2), Backup de sistemas (CP-9) y Recuperación de sistemas (CP-10).
G. **Identificación y Autenticación (IA)**: Estos controles establecen requisitos para la identificación y autenticación de usuarios, procesos o dispositivos, tal como los controles de Autenticación de usuario (IA-2) e Configuración de autenticador (IA-5).
H. **Respuesta a Incidentes (IR)**: Estos controles se centran en la capacidad de la organización para manejar y responder a los incidentes de seguridad, tal como los controles de Capacitación de respuesta de incidentes (IR-2), Manejo de incidentes (IR-4) y Monitoreo de incidentes (IR-5).
I. **Mantenimiento (MA)**: Estos controles establecen políticas y procedimientos para el mantenimiento de los sistemas de información, como Mantenimiento Controlado (MA-2) y Herramientas de mantenimiento (MA-3).
J. **Protección del Sistema y Comunicaciones (SC)**: Controles dedicados a salvaguardar la información que se encuentra en tránsito o almacenada, como los

controles de Separación de sistema y funcionalidad de usuario (SC-2), Confidencialidad e integridad de transmisión (SC-8) y Protección criptográfica (SC-13) y Aplicaciones en plataformas independientes (SC-27).

K. **Seguridad Física y Ambiental (PE)**: Estos controles están diseñados para proteger el sistema y su entorno físico, incluyendo controles tal como Autorización de acceso físico (PE-2), Monitoreo de acceso físico (PE-6) y Controles ambientales (PE-14).

## 6.4 CONCIENCIACIÓN DE CIBERSEGURIDAD

Desarrollar un programa de formación integral para el personal del puerto de Valparaíso es esencial para garantizar que todos comprendan sus responsabilidades con respecto al SGSI y el Marco de NIST. Este programa podría estructurarse de la siguiente manera:

A. **Introducción al SGSI y al Marco de NIST**: Capacitación que ofrece una visión general del SGSI y el Marco de NIST, incluyendo los objetivos de ambos, cómo se implementan y por qué son importantes para la seguridad de la información en el puerto.
B. **Roles y responsabilidades**: Cada empleado debe entender su papel específico dentro del SGSI y el Marco de NIST, esto incluye la comprensión de las políticas y procedimientos de seguridad de la información y cibernética.
C. **Entrenamiento específico del cargo**: Dependiendo del rol, puede ser necesario proporcionar formación más detallada en áreas específicas, como la gestión de incidentes de seguridad, el mantenimiento de la seguridad de los sistemas y el seguimiento de los procedimientos de respuesta a incidentes.
D. **Formación continua**: La formación debe ser un esfuerzo continuo para asegurar que los empleados estén actualizados con las últimas amenazas de seguridad, las actualizaciones al SGSI y el Marco de NIST y cualquier cambio en sus responsabilidades.

Para desarrollar la concienciación sobre el reconocimiento de amenazas, el seguimiento de procedimientos y la notificación de incidentes, el puerto de Valparaíso podría implementar las siguientes estrategias:

A. **Charlas de concienciación sobre seguridad**: Las sesiones de formación regulares que se centran en identificar las amenazas comunes de seguridad cibernética y física pueden ser útiles para mantener al personal alerta y consciente de las posibles amenazas.
B. **Simulacros de amenazas**: Realizar simulacros de amenazas puede ser una manera efectiva de enseñar al personal cómo identificar y responder a las amenazas de seguridad.
C. **Herramientas de seguimiento de procedimientos**: Las herramientas que ayudan al personal a seguir los procedimientos correctos, como las listas de comprobación y las guías de procesos, pueden ayudar a asegurar que todos los integrantes de la organización sigan los mismos estándares.
D. **Sistema de notificación de incidentes**: Debe establecerse un sistema claro y fácil de usar para notificar los incidentes de seguridad. Este sistema necesita ser comunicado de forma transversal y accesible para todo el personal.

E. **Reforzar la importancia de la notificación**: Es crucial enfatizar a los empleados que deben notificar cualquier incidente o actividad sospechosa, sin importar cuán insignificante pueda parecer. Este mensaje debe ser una parte central de la formación y las comunicaciones regulares.

## 6.5 REVISIÓN Y MONITOREO

El monitoreo y revisión del SGSI y del Marco de NIST en el puerto de Valparaíso implican una serie de pasos estratégicos:

A. **Monitoreo continuo**: Se debe establecer un proceso de monitorización continua para detectar anomalías o violaciones de las políticas y procedimientos de seguridad. Asumiendo el uso de sistemas de detección de intrusiones, análisis de registros y revisiones periódicas de los procesos de seguridad.
B. **Revisiones periódicas del SGSI**: Se debe llevar a cabo una verificación periódica del SGSI para asegurarse de que está funcionando como se espera y así identificar áreas de mejora mediante la evaluación de la eficacia de los controles de seguridad, la identificación de áreas de riesgo y la implementación de cambios para mejorar la seguridad.
C. **Revisión del cumplimiento del Marco de NIST**: La ejecución del marco de NIST necesita ser revisada regularmente para asegurarse de que se están siguiendo todas las directrices y controles. Esta revisión se realiza mediante la evaluación de los procesos de Identificación, Protección, Detección, Respuesta y Recuperación y la implementación de cambios si es necesario.

La realización de auditorías, la corrección de incidentes y respuestas y el seguimiento de las políticas y procedimientos son partes cruciales del mantenimiento y mejora continua del SGSI y la aplicación del Marco de NIST en el Puerto de Valparaíso.

Las auditorías son una herramienta esencial para asegurar la efectividad del SGSI y la conformidad con el Marco de NIST. Estas requieren ser exhaustivas, cubriendo todas las áreas del SGSI y del Marco de NIST y deberían buscar identificar cualquier área de mejora potencial. Los hallazgos de la auditoría se documentan y las acciones correctivas necesarias deben llevarse a cabo de manera oportuna.

Cuando se producen incidentes de seguridad, es vital que se ejecute una verificación exhaustiva. Esto debería incluir una evaluación de cómo se manejó el incidente, qué medidas se tomaron en respuesta y qué se puede aprender de los eventos para prevenir o manejar mejor las situaciones similares en el futuro. Las lecciones aprendidas deben integrarse en el SGSI y en la aplicación del Marco de NIST para fortalecer las defensas del puerto.

Es esencial efectuar correcciones regulares para asegurarse de que se están siguiendo todas las políticas y procedimientos de seguridad. Mediante el análisis de los registros de seguridad, la observación directa de las prácticas de trabajo y la revisión de la conformidad con las políticas durante las auditorías, se pueden identificar incumplimientos de las políticas o procedimientos para así implementar medidas correctivas.

## 6.6 MEJORA CONTINUA

El primer paso en la mejora continua es la identificación de las áreas que necesitan potenciar, esto se logra a través de las revisiones y auditorías mencionadas anteriormente. Por ejemplo, si una auditoría revela que ciertos controles de seguridad no están funcionando como se esperaba, o si una revisión de incidentes muestra que hubo un retraso en la respuesta a una amenaza, estas serían áreas identificadas para mejorar.

Es vital que todas las verificaciones y auditorías se documenten de manera detallada y clara, incluyendo las recomendaciones de mejora y que estas se presenten a los responsables de la toma de decisiones.

Una vez identificadas las áreas de mejora, el próximo paso es actualizar el SGSI y la aplicación del Marco de NIST para abordar estas necesidades. Esto puede implicar una variedad de acciones, como la implementación de nuevos controles de seguridad, la modificación de políticas o procedimientos existentes, o la formación y educación adicionales para el personal.

Por ejemplo, si se identificó que la respuesta a los incidentes fue más lenta de lo esperado, se podría implementar un nuevo procedimiento para acelerar la detección y reacción a las amenazas. Si una auditoría reveló que ciertos controles de seguridad no estaban funcionando como se esperaba, estos controles podrían ser revisados y mejorados.

Todas las actualizaciones y cambios en el SGSI y en la aplicación del Marco de NIST deben ser documentados y comunicados de manera efectiva a todos los stakeholders relevantes. Además, debe haber un proceso para comprobar el impacto de estas modificaciones y asegurar que están teniendo el efecto deseado en la mejora de la seguridad.

Estos pasos aseguran que el puerto de Valparaíso esté constantemente mejorando su seguridad y adaptándose a las nuevas amenazas y desafíos. La mejora continua es un componente vital de cualquier sistema de gestión de seguridad eficaz.

# 7. CONCLUSIONES

La ciberseguridad en el entorno marítimo, en particular en la industria portuaria, se ha convertido en un tema de alta importancia durante la última década. A medida que aumenta la dependencia en las nuevas tecnologías para optimizar la eficiencia y la productividad, también se intensifican los riesgos cibernéticos. Esta tendencia se vuelve muy preocupante considerando el auge de ciberataques en distintas industrias, siendo los más dañinos los ataques bajo la categoría de ransomware, que buscan secuestrar información crítica, negando el acceso y operación de esta para así exigir un rescate ante su liberación.

A través de entrevistas realizadas con encargados de la ciberseguridad en empresas logísticas relacionadas con el puerto de Valparaíso, este trabajo ha identificado una serie de oportunidades de mejoras en el sistema de ciberseguridad del puerto, destacando especialmente los errores humanos y la falta de preparación como los puntos débiles más significativos. Este hallazgo corrobora la literatura actual, que destaca la importancia de la formación y la concienciación en ciberseguridad para todos los actores involucrados en las operaciones portuarias.

En respuesta a estos desafíos, el Marco de Ciberseguridad NIST CFS 1.1 y la próxima versión 2.0, junto con la norma ISO 27001, ofrecen una serie de herramientas y pautas sólidas que, si se aplican correctamente, pueden minimizar significativamente estos riesgos. Este trabajo ha detallado cómo se pueden implementar estas herramientas en el puerto de Valparaíso, con una consideración especial a las medidas de control que se corresponden directamente con las preocupaciones surgidas de las entrevistas realizadas.

Por ejemplo, se han presentado estrategias para mejorar la formación del personal y la concienciación sobre las amenazas cibernéticas. Además, se ha proporcionado una guía para el establecimiento de procesos de auditoría y revisión que pueden ayudar a mantener el sistema de gestión de seguridad de la información (SGSI) del puerto actualizado y acorde a las mejores prácticas y las amenazas emergentes.

No obstante, es significativo entender que la ciberseguridad no es un destino que se alcanza una vez y se mantiene estático. Es un proceso continuo que requiere un compromiso constante con la formación, la actualización de sistemas y prácticas, y la adaptación a un entorno de amenazas que evoluciona constantemente. Este trabajo de grado propone, por tanto, no solo una solución a los desafíos actuales de la ciberseguridad del puerto de Valparaíso, sino también una hoja de ruta para una gestión eficaz de la ciberseguridad en el futuro.

En conclusión, se ha demostrado que, a través de una cuidadosa implementación y mantenimiento de marcos de ciberseguridad reconocidos, es posible fortalecer la resiliencia del puerto de Valparaíso frente a las amenazas cibernéticas, protegiendo sus operaciones, su reputación y su contribución vital a la economía regional y nacional.

# REFERENCIAS


AWS. (20 de Mayo de 2021). *AWS Shield threat landscape review: 2020 year-in-review*. Obtenido de https://aws.amazon.com/blogs/security/aws-shield-threat-landscape-review-2020-year-in-review/

Bocayuva, M. (2021). Cybersecurity in the European Union port sector in light of the digital transformation and the COVID-19 pandemic. *Springer Nature*, 173-192.

Bures, M., S. Ahmed, B., Rechtberger, V., Klima, M., Trnka, M., Jaros, M., . . . Herout, P. (2021). PatrIoT: IoT Automated Interoperability and Integration Testing Framework. *EE Conference on Software Testing, Verification and Validation*, (pp. 454-459).

CISA. (2021). *Cybersecurity and Physical Security Convergence.*

Committee on National Security Systems. (6 de Abril de 2015). *Glossary.* Obtenido de https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

CSIRT. (25 de Octubre de 2021). *RFC 2350 del CSIRT de Gobierno.* Obtenido de https://www.csirt.gob.cl/media/2021/10/RFC2350-final.pdf

Deloitte. (2021). *Modernizing the three lines of defense model.* Obtenido de https://www2.deloitte.com/us/en/pages/advisory/articles/modernizing-the-three-lines-of-defense-model.html

Demir, N., Urban, T., Wittek, K., & Pohlmann, N. (2021). Our (in)Secure Web: Understanding Update Behavior of Websites and Its Impact on Security.

ENISA. (2019). *Phishing.* Obtenido de https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl2020-phishing

ENISA. (26 de Noviembre de 2019). *Port Cybersecurity - Good practices for cybersecurity in the maritime sector.* Obtenido de https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

Henesey, L., Lizneva, Y., Philipp, R., Meyer, C., & Gerlitz, L. (2020). Improved load planning of RoRo Vessels by adopting Blockchain and Internet-of-Things. *International Conference on Harbor, Maritime and Multimodal Logistic Modeling & Simulation*, (págs. 58-65).

Hue, M. H., Debnath, J., Leung, K. M., Minaei, M., Xian, K., & Hoque, E. (2021). All your Credentials are Belong to Us: On Insecure WPA2-Enterprise Configurations. *ACM SIGSAC Conference on Computer and Communications Security*, (págs. 1100-1117).

IBM. (2022). *What is social engineering?* Obtenido de https://www.ibm.com/topics/social-engineering

IIA. (2020). *The IIA's Three Lines Model.* Obtenido de https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

IMO. (12 de Mayo de 1998). *ADOPTION OF NEW AND AMENDED PERFORMANCE STANDARDS.* Obtenido de https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/AIS/Resolution%20MSC.74(69).pdf

IMO. (7 de Junio de 2022). *GUIDELINES ON MARITIME CYBER RISK MANAGEMENT.* Obtenido de https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf

IMO. (2022). *SOLAS XI-2 and the ISPS Code*. Obtenido de https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

Jarjoui, S., & Murimi, R. (2021). *A Framework for Enterprise Cybersecurity Risk Management.*

KnowBe4. (2021). *State of Privacy and Security Awareness Report.*

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Tecnology In Society*.

NIST. (28 de Febrero de 2019). *Glossary*. Obtenido de https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary

NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations.* Obtenido de NIST Special Publication 800-53: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NIST. (2020). *Zero Trust Architecture.* Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

NPR. (19 de Diciembre de 2017). *U.S. Says North Korea 'Directly Responsible' For WannaCry Ransomware Attack*. Obtenido de https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack

OECD. (2020). *The Role of Public Policy and Regulation in Encouraging Clarity in Cyber Insurance Coverage.* Obtenido de https://www.oecd.org/finance/insurance/The-Role-of-Public-Policy-and-Regulation-in-Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf

Polatidis, N., Pavlidis, M., & Mouratidis, H. (2017). Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards & Interfaces*, 74-82.

Security, C. f. (2022). *Election Security Spotlight – Defense in Depth (DiD)*. Obtenido de https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-defense-in-depth-did

TPS. (2022). *Reporte Integrado.*

UNCTAD. (2022). *Review of Maritime Transport.* Obtenido de https://unctad.org/system/files/official-document/rmt2022_en.pdf

WIRED. (22 de Agosto de 2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Obtenido de https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Zarzuelo, I. d. (2020). Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. *Elsevier*, 3-4.

# ANEXO 1

Cuestionario de ciberseguridad

Todas las discusiones y respuestas serán manejadas de forma confidencial. No se reportarán u ocuparán los nombres de las empresas o personas entrevistadas y los resultados de estas entrevistas serán completamente anónimos.

Preguntas para los entrevistados:

1. Usando sus palabras, ¿qué es la seguridad cibernética (ciberseguridad) y los riesgos asociados a esta?

2. ¿Cuáles son, en su opinión, las brechas de seguridad más importantes en las operaciones marítimo-portuarias?

3. En su opinión y considerando su propia organización, ¿Cuáles son principales áreas en las cuales se puede pueden identificar posibles mejoras de ciberseguridad?

4. ¿Su empresa ha sido víctima o afectada negativamente por algún ciber ataque, o algún otro problema causado intencionalmente relacionado con las tecnologías de la información y comunicación (TIC)?

5. ¿Reconoce quién está a cargo de la ciberseguridad de su empresa?

6. ¿La funcionalidad e implementación de las tecnologías de información se encuentran externalizadas o son de desarrollo interno?

7. ¿Su empresa ha implementado la ciberseguridad como parte del sistema de gestión de seguridad?

8. ¿Su empresa ha realizado una evaluación y análisis de riesgos en materia de ciberseguridad?

9. ¿Qué tan alta estima la probabilidad de que su empresa enfrente un incidente de seguridad cibernética, tanto a nivel general como operativo?

10. En su opinión, ¿cuál es el nivel de conciencia y preparación del personal de la empresa sobre materias de ciberseguridad?

11. ¿Su empresa organiza simulacros enfocados a la concientización de la ciberseguridad?

12. ¿En su opinión, en qué situación se encuentra la legislación y normativa chilena para enfrentar las amenazas a la ciberseguridad?

13. El puerto de Valparaíso se encuentra conectado digitalmente a varias entidades, siendo uno de los proyectos más importantes el de SILOGPORT, en su opinión, ¿este sistema cuenta con los protocolos de continuidad operacional necesarios para la cadena logística en caso de ciberataques?