Directrices de ciberseguridad de la IAPH para puertos e instalaciones portuarias

Versión 1.0

IAPH
International Association of Ports and Harbors

WPSP
WORLD PORTS SUSTAINABILITY PROGRAM

TABLA DE CONTENIDO

LISTA DE FIGURAS

Sede Central del IAPH

Séptimo piso, Torre Sur Nuevo Muelle Takeshiba

1-16-1 Kaigan, Minato-ku, Tokio 105-0022

Japón

Teléfono: +81 3 5403 2770

Fax: +81 3 5403 7651

Correo electrónico: info@iaphworldports.org

La información proporcionada en esta publicación ha sido creada por la Asociación Internacional de Puertos y Puertos (IAPH) con el propósito de proporcionar a la industria portuaria internacional un conjunto de pautas de ciberseguridad. Estas directrices deberían considerarse directrices adicionales a los instrumentos promulgados por la Organización Marítima Internacional (OMI) y especialmente para complementar las directrices de la industria marítima compatibles con la circular MSC-FAL.1/Circ. 3, 5 de julio de 2017.

Las Directrices de ciberseguridad de la IAPH proporcionadas en este documento se basan en los éxitos logrados por puertos e instalaciones portuarias de todo el mundo y están diseñadas para ayudar a los ejecutivos de la industria portuaria en su esfuerzo por fomentar una mayor colaboración dentro de sus organizaciones, así como de manera más amplia con sus autoridades locales. socios y partes interesadas regionales, nacionales e internacionales.

Este trabajo es producto del personal y la membresía de la IAPH, junto con las contribuciones de la personal del Banco Mundial.

Derechos y permisos

AGRADECIMIENTOS

Este informe técnico fue preparado por un equipo conjunto de representantes de los miembros de la Asociación Internacional de Puertos (IAPH) y el Banco Mundial.

El equipo de la IAPH estuvo dirigido por el Dr. Patrick Verhoeven, director general de Política y Estrategia, y Pascal Ollivier, Presidente del Comité de Colaboración de Datos de la IAPH y Presidente de Maritime Street, y compuesto por Frans van Zoelen, Proyectos Especiales: Jefe Legal Emérito, Autoridad del Puerto de Rotterdam, Consejero Legal de la IAPH y Presidente del Comité Legal de la IAPH; Max Bobys, vicepresidente de HudsonCyber; Andrew Baskin, vicepresidente de HudsonAnalytix; Lance Kaneshiro, Director de Información, Puerto de Los Ángeles; Chin Beng Ong, Director de Seguridad de la Información, Autoridad Marítima y Portuaria de Singapur; Adeline Tiang, vicepresidenta adjunta de ciberseguridad del grupo, PSA International, Singapur; Mohamed Absar, Jefe de Proyectos y Soluciones, DP World; Gadi Benmoshe, Director de Información, Compañía de Puertos de Israel; Dr. Phantian
Zuesongdham, Jefe de la División de Soluciones de Procesos Portuarios, Autoridad Portuaria de Hamburgo; Lars Wentorp, Director de Información, Autoridad Portuaria de Hamburgo; Dr. Quang-Vu Pham, Jefe de Privacidad de Datos y Seguridad de la Información, Autoridad Portuaria de Hamburgo; Machiel Noijen, Asesor de Política Estratégica, División de Capitanía de Puerto, Autoridad del Puerto de Amsterdam; Peter Alkema, Asesor de Política Estratégica de la División de Capitanía Portuaria, Autoridad del Puerto de Ámsterdam; Mark de Pater, Director de Seguridad de la Información, Autoridad del Puerto de Rotterdam; Yannick Herrebaut, director de seguridad de la información, puerto de Amberes; Jerome Besancenot, Director del Proyecto de Transición Digital, Puerto HAROPA; Francis Donkoh, Director de Información de la Autoridad de Puertos y Puertos de Ghana; y Scott Dickerson, Director Ejecutivo, Sistema de Transporte Marítimo, Centro de Análisis e Intercambio de Información.

El equipo del Banco Mundial estuvo formado por Hagai Mei Zahav, especialista en cibernética, desarrollo digital, Banco Mundial, Richard Martin Humphreys, líder global para la conectividad del transporte e integración regional, y economista líder en transporte, ITRGK, y Ninan Oommen Biju, transporte portuario y marítimo senior. Especialista, IEAT.

Los autores principales agradecen a las siguientes personas por sus importantes contribuciones a la preparación de este informe: Dr. Antonis Michail, director técnico de IAPH, y Victor Shieh, director de comunicación de IAPH.

El equipo en su conjunto extiende su agradecimiento especial al Sr. Santiago García-Milà, Presidente de IAPH y Director General Adjunto del Puerto de Barcelona, por su liderazgo de IAPH y en particular su apoyo inquebrantable al Comité de Colaboración de Datos que tomó la iniciativa de lanzar estos Lineamientos de Ciberseguridad para Puertos e Instalaciones Portuarias.

ABREVIACIONES Y ACRONIMOS

TERMINOLOGÍA	ABREVIATURA / ACRÓNIMO
Amenazas persistentes avanzadas	APTO
Inteligencia artificial	AI
Sistema de identificación automática	AIS
Análisis de Impacto del Negocio	ALIMENTO
Plan de negocios continuo	BCP
Equipo de respuesta a emergencias informáticas	CERTIFICADO
Equipo de respuesta a incidentes de seguridad informática	CHIRTO
Director de información	CIO
Director de seguridad de la información	CISO
Comercial listo para usar	CUNAS
Objetivos de control para tecnologías relacionadas con la información Infraestructura de	COBIT
información crítica Inteligencia sobre amenazas	CII
cibernéticas Seguridad cibernética	TIC
Equipo de respuesta a incidentes DHS Agencia de seguridad	CHIRTO
de infraestructura y ciberseguridad Intercambio electrónico de datos Agencia de la	CISA
Unión Europea para la ciberseguridad Plan	ERA
de respuesta a incidentes Indicador de compromiso Sistemas de	ENISA
control industrial Internet industrial	PIR
de las cosas Tecnología de la	COI
información Infraestructura de tecnología	ICS
de la información Biblioteca Internacional	IIoT
Organización Marítima Organización	ÉL
Internacional de Normalización Código Internacional de Seguridad	ITIL
Portuaria y de Buques Sociedad Internacional de	OMI
Automatización Internet de las Cosas Sistema de Detección de Intrusiones /	YO ASI
Sistema de Protección contra Intrusiones Ventanilla Única Marítima	Código PBIP
Organización No Gubernamental Inteligencia de Código	UNO
Abierto Tecnología	IoT
Operacional Sistema de Comunidad Portuaria Controlador Lógico Programable Objetivo de	ID/IPS
Punto de Recuperación Objetivo de	RSU
Tiempo de Recuperación Información de seguridad	ONG
y gestión de eventos Centro de	OSINT
operaciones de seguridad Habilidad,	Antiguo Testamento
conocimiento y capacidad Supervisión	piezas
Control y adquisición de datos Ejercicio de mesa	SOCIEDAD ANÓNIMA
Tácticas, técnicas y procedimientos	RPO
Sistema operativo de terminal	RTO
Departamento de Seguridad Nacional de EE. UU. Instituto Nacional de	SIEM
Estándares y Tecnología de EE. UU.	SOC
Servicio de tráfico de embarcaciones/	VOLUNTAD
Sistema de gestión de tráfico de embarcaciones	SCADA
	TTX
	TTP
	Términos de servicio
	Departamento de Seguridad Nacional
	NIST
	VTS/VTMS

PREFACIO

La Asociación Internacional de Puertos y Puertos (IAPH) es una alianza global sin fines de lucro de 170 puertos y 140 organizaciones relacionadas con los puertos que cubre 90 países y tiene estatus de ONG consultiva ante varias agencias de las Naciones Unidas, incluida la Organización Marítima Internacional (OMI).

A través de su base de conocimientos y acceso a organismos reguladores, IAPH tiene como objetivo acelerar la digitalización y ayudar a mejorar la resiliencia general de sus puertos miembros en un mundo en constante cambio.

La pandemia de COVID19 ha demostrado ser el momento crucial para que los puertos pasen de los procesos manuales basados en papel al intercambio digital de información. El virus ha afectado drásticamente el contacto persona a persona entre el barco y la costa, y ha obligado a adoptar rápidamente soluciones digitales relacionadas con la seguridad para los movimientos de carga y personas hacia y desde las puertas del puerto, en las oficinas, en el muelle, junto a los atraques de los buques y más allá de la estación piloto. Sin embargo, esto también ha aumentado la vulnerabilidad de los puertos, algunos de los cuales han sido objeto de ciberataques muy eficaces.

En un llamado a la acción para acelerar el ritmo de la digitalización para hacer frente a una “nueva normalidad” posterior a la COVID19 Respaldado por toda la industria marítima, la IAPH estableció un plan de nueve puntos, que incluye:

> Revisar la orientación existente de la OMI sobre la gestión de riesgos cibernéticos marítimos sobre su capacidad para abordar los riesgos cibernéticos en los puertos, desarrollando orientación adicional cuando sea necesario.

Esta primera edición de las Directrices de Ciberseguridad para Puertos y Autoridades Portuarias de la IAPH sirve para este propósito. También sirve como un documento crucial y neutral para los altos ejecutivos que toman decisiones en los puertos que no necesitan ser técnicos ni conocedores de las últimas tendencias cibernéticas, pero que deben encontrar respuestas a las siguientes preguntas para salvaguardar la viabilidad comercial de su organización:

- ¿ Cómo puedo establecer el verdadero impacto financiero, comercial y operativo de un ciberataque?
- ¿ Qué tan preparada está mi organización para prevenir, detener y recuperarse de un ciberataque?
- ¿ Qué necesito en términos de recursos para gestionar eficazmente el riesgo de un ciberataque?

Este documento evolucionará para enfrentar el desafío de responder estas preguntas, proporcionadas por los principales expertos de la industria portuaria en este tema crítico.

Dr. Patrick Verhoeven

Director General de Política y Estrategia
IAPH

RESUMEN EJECUTIVO

Los puertos y las instalaciones portuarias de todo el mundo están informando de aumentos mensurables en las actividades de ciberamenazas, particularmente desde el estallido de la pandemia de COVID-19. Solo entre febrero y mayo de 2020, la industria marítima en general sufrió un aumento de cuatro veces en los ciberataques.
y esos ataques contra sistemas OT aumentaron específicamente en un 900 por ciento desde 2017. El riesgo de un ciberataque se ha convertido en el principal riesgo para las autoridades portuarias y la comunidad portuaria en general.

El ritmo acelerado de la digitalización en los puertos y las instalaciones portuarias no hace más que intensificar la urgencia de Los ejecutivos se centrarán en la ciberresiliencia organizacional para salvaguardar la integridad y disponibilidad de datos críticos, garantizar la prestación de servicios y proteger la infraestructura marítima. Hacerlo aumentará las capacidades generales de ciberseguridad de la cadena de suministro marítima global.

Las Directrices de Ciberseguridad de la IAPH se desarrollan para apoyar el puerto y las instalaciones portuarias globales. comunidad de manera coherente con las Directrices de la OMI sobre gestión de riesgos cibernéticos marítimos (MSC-FAL.1/ Circ.3, 5 de julio de 2017). Está destinado a ser utilizado por el Director General y los ejecutivos de alto nivel para reconocer la importancia de gestionar el riesgo cibernético e inculcar la comprensión de que es una responsabilidad que comienza en la cima de su organización, a pesar de la brecha digital entre los puertos. mundial.

Las directrices se centran principalmente en desarrollar el caso de negocio para que el comité ejecutivo determine "¿cuánto es suficiente?" como un nivel razonable de inversión en la gestión del riesgo cibernético y para obtener información sobre cómo un evento cibernético podría afectar la capacidad de un puerto o de una instalación portuaria.
funcionar, junto con el costo de la interrupción.

Estas directrices también abordan la necesidad de que los ejecutivos desarrollen una estrategia de gestión de riesgos cibernéticos y un plan para lograr y mantener una postura de defensa en profundidad, proporcionan información clave sobre el panorama de las amenazas cibernéticas del siglo XXI e incluyen información sobre los impactos de los ataques cibernéticos. contra los sistemas portuarios integrados. Las consideraciones específicas abordan las estructuras organizativas, la identificación de partes interesadas clave, los mecanismos de presentación de informes, el flujo de datos y el mapeo de redes, las caracterizaciones de las actividades críticas que se realizan y la identificación y análisis de datos, sistemas, activos e infraestructuras críticos.

Las directrices ilustran cómo los ejecutivos deberían considerar el riesgo cibernético en el contexto de sus propias operaciones, independientemente de dónde residan dentro de la brecha digital. Se proporciona información a los ejecutivos sobre cómo evaluar el riesgo y las vulnerabilidades en sus operaciones portuarias y cómo adoptar un enfoque holístico que les permitirá organizar y gestionar su programa de ciberseguridad mediante la implementación de medidas personalizadas de protección, detección y mitigación de la ciberseguridad. También se proporcionan las mejores prácticas que explican por qué el intercambio, la comunicación y la coordinación de información sobre ciberseguridad son clave para reducir los riesgos de ciberseguridad. Se proporcionan recomendaciones generales en todas partes.

Igualmente importante es el establecimiento de una conciencia cibernética organizacional para abordar lo humano como elemento fundamental. Por lo tanto, se destaca la capacitación general y técnica, que logra el diseño y la implementación del plan de gestión de emergencias, vital para que las organizaciones marítimas respondan de manera rápida y efectiva para mejorar la resiliencia de los puertos y las instalaciones portuarias, así como el ecosistema portuario en general.

Dado que la ciberseguridad representa una responsabilidad colectiva (que no se limita únicamente al departamento de TI), las directrices demuestran cómo la capacidad de ciberseguridad puede impulsar la resiliencia cibernética. Es esencial que los ejecutivos de alto nivel tomen la iniciativa en la asignación de recursos para abordar la ciberseguridad, la gestión activa de la gobernanza y la creación de una cultura organizacional para respaldar las operaciones de ciberseguridad, y el desarrollo de estrategias de liderazgo para impulsar la ciberresiliencia, incluida la creación de una fuerza laboral de ciberseguridad en el ecosistema portuario. .

Finalmente, las directrices brindan al líder de ciberseguridad designado asistencia práctica para desarrollar sus evaluaciones y planes de seguridad portuaria y de las instalaciones portuarias.

1. INTRODUCCIÓN

La industria marítima y el ciberriesgo

La industria del transporte marítimo global y las redes integradas de cadenas de suministro multimodales que respalda se benefician enormemente de las innumerables soluciones digitales introducidas por la Cuarta Revolución Industrial1. La digitalización y la integración de soluciones de automatización y aprendizaje automático dependen de una mayor conectividad entre los sistemas de tecnología de la información (TI) y de tecnología operativa (OT) en red de entidades individuales y de los extraordinarios volúmenes de datos creados, procesados, intercambiados y almacenados. Estos avances aumentan la eficiencia del sistema de transporte marítimo, lo que da como resultado un progreso año tras año que ofrece mejoras tanto cualitativas como cuantitativas a los consumidores y productores para responder en tiempo real a los requisitos comerciales.

Para seguir siendo competitivos en el apoyo a sus clientes y sus economías regionales y nacionales, los puertos y las instalaciones portuarias deben adaptarse a las demandas de un mercado global cada vez más digitalizado. A medida que se acelera la digitalización, el ciberespacio global2 en el que operan los puertos y las instalaciones portuarias, evoluciona. Con el tiempo, las desigualdades económicas, la velocidad de la inversión en infraestructura, el ritmo (y la voluntad) de adopción tecnológica e incluso las circunstancias geográficas abren fisuras tecnológicas. aunque sean “brechas digitales”, entre puertos e instalaciones portuarias. Inevitablemente, estas brechas digitales crecen, exacerbando las deficiencias de algunos puertos e instalaciones portuarias, al tiempo que resaltan las ventajas competitivas de otros.

Independientemente del nivel de adopción digital en un puerto o instalación portuaria, el lado inevitable de la digitalización es el riesgo cibernético. Ningún puerto o instalación portuaria es inmune a ello. Dado que la mayoría de los ciberataques involucran a personas y sistemas fragmentados, todos los puertos e instalaciones portuarias están en riesgo. Además, las desigualdades de la brecha digital y el papel oneroso que desempeña la industria marítima en el centro del comercio mundial y el intercambio de información subrayan la naturaleza compartida del riesgo cibernético dentro de la comunidad mundial de puertos e instalaciones portuarias.

La gestión eficaz del riesgo cibernético es fundamental para el funcionamiento adecuado de una comunidad marítima diversa donde las partes interesadas de la autoridad portuaria, los operadores de buques, las instalaciones portuarias, las agencias marítimas, las aduanas y las fuerzas del orden están todas interconectadas.
Los líderes de puertos e instalaciones portuarias deben reconocer que las amenazas cibernéticas no están limitadas por ninguna frontera, perímetro portuario o incluso cadena de suministro logístico donde cada eslabón sea crítico. Las amenazas cibernéticas pueden poner en peligro las operaciones de todo un puerto o de una instalación portuaria y están proliferando a un ritmo cada vez mayor. Con la evolución y la introducción de nuevas tecnologías de TI y OT, sistemas automatizados y procesos integrados que dependen de proveedores clave de servicios en la nube, los líderes portuarios deben reconocer la importancia de gestionar el riesgo cibernético y comprender que es una responsabilidad que comienza desde arriba.

Un creciente conjunto de pruebas subraya el creciente éxito que han tenido los ciberatacantes contra la industria marítima. Por ejemplo, entre febrero y mayo de 2020 la industria marítima en

1 La Cuarta Revolución Industrial representa colectivamente la tendencia global hacia la automatización y el intercambio de datos que abarca la fabricación, los sistemas industriales y los procesos de infraestructura, que incluyen sistemas ciberfísicos, Internet y el Internet industrial de las cosas, computación en la nube, aprendizaje automático, comunicaciones de máquina a máquina y inteligencia artificial. 2

El ciberespacio se puede definir de muchas maneras. En su forma más simple, representa la totalidad de toda la tecnología interconectada digitalmente. Una visión más amplia abarca la totalidad de todas las interacciones y comunicaciones sociales facilitadas por el medio computacional de Internet y todas las redes de TI interconectadas y la infraestructura de soporte habilitadas para Internet.

en general sufrieron un aumento de cuatro veces en los ciberataques3 y aquellos ataques contra sistemas OT, específicamente aumentó en un 900 por ciento en los últimos tres años.4 Las partes interesadas de los puertos y las instalaciones portuarias de todo el mundo están informando aumentos mensurables en las actividades de amenazas cibernéticas, y el Informe Anual 2021 del Centro de Análisis e Intercambio de Información del Sistema de Transporte Marítimo (MTS-ISAC)5
Destacó algunas de las técnicas de ataque más comúnmente reportadas. Las organizaciones marítimas suelen considerar los ataques de phishing como el principal medio para que los atacantes comprometan cuentas, redirijan pagos legítimos o faciliten de otro modo sus actividades. Además, también es común escanear la infraestructura pública de Internet en busca de sistemas sin parches y vulnerabilidades.

Dado que los puertos y las instalaciones portuarias permiten el comercio global, deben ser reconocidos como infraestructura de información crítica (ICI)6. Las consecuencias de los procesos digitales del puerto y/o de las instalaciones portuarias comprometidos podrían resultar en una interrupción operativa, afectando a los clientes, las autoridades portuarias, los sistemas de la comunidad portuaria y los servicios portuarios relacionados. Además, los ciberataques que exponen datos confidenciales a acceso, manipulación o exfiltración no autorizados pueden socavar aún más la integridad de la cadena de suministro marítimo.

Fondo

En junio de 2020 la IAPH, en colaboración con la Asociación Internacional de Coordinación de Manejo de Carga (ICHCA) y el TT Club publicó la Nota de Ciberseguridad de la Comunidad Portuaria7. Este reporte
abogó por la necesidad de acelerar la digitalización de las capacidades dentro de los puertos y las instalaciones portuarias en todo el mundo. Sin embargo, por las razones descritas anteriormente, esa defensa de la digitalización también justifica inversiones paralelas en capacidades de ciberseguridad.

En enero de 2021, la IAPH y el Banco Mundial publicaron un informe conjunto8 titulado “Acelerar las acciones críticas de digitalización para fortalecer la resiliencia de la cadena de suministro marítimo”, que se centró en la digitalización portuaria. Este informe también generó conciencia sobre el riesgo cibernético en el contexto de la digitalización. Sobre la base de trabajos anteriores con sus socios, la IAPH ha desarrollado esta primera versión de sus Directrices para la ciberseguridad en puertos e instalaciones portuarias9 (en adelante, las “Directrices cibernéticas de la IAPH”).

Las Directrices cibernéticas de la IAPH se desarrollaron para apoyar específicamente a la comunidad mundial de puertos e instalaciones portuarias de manera coherente con las Directrices de la OMI sobre gestión de riesgos cibernéticos marítimos (MSC-FAL.1/Circ.3, 5 de julio de 201710). Las directrices de la OMI ofrecen orientación no prescriptiva sobre ciberseguridad marítima.

---

3 https://www.captiveinternational.com/news/maritime-businesses-see-fourfold-increase-in-cyber-attacks-since-february-astaara-3568

4 https://www.professionalmariner.com/naval-dome-maritime-cyberattacks-up-900-percent-in-tres-years/

5 https://www.mtsisac.org/post/2020-mts-isac-annual-report

6 Según la Directiva 2016/1148 de la UE (Directiva NIS), los puertos se consideran CII para el transporte acuático y, además, los clasifica como Operadores de Servicios Esenciales. Dado que la ciberresiliencia de los ecosistemas portuarios y de las instalaciones portuarias es fundamental para respaldar la industria marítima mundial, la protección de las ICI es fundamental para diversas iniciativas de ciberseguridad portuarias específicas, como la Estrategia de Ciberseguridad de Singapur, la Agencia para la Ciberseguridad de la Unión Europea (ENISA) y la Agencia Nacional de Seguridad Cibernética del Gobierno de los EE. UU. Plan de Ciberseguridad Marítima.

7 https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf

8 https://sustainableworldports.org/wp-content/uploads/World-Bank-IAPH-joint-paper-accelerating-digitalizacion.pdf

9 Esta publicación no pretende proporcionar una base y no debe interpretarse como un llamado a una auditoría externa o una verificación del enfoque de la organización individual para la gestión del riesgo cibernético.

10https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Lineamientos%20Sobre%20Marítimo%20Cibernético%20Riesgo%20Gestión%20(Secretaría).pdf

Gestión de riesgos para mejorar la resiliencia de la ciberseguridad de la industria naviera frente a las ciberamenazas actuales y emergentes.

Público objetivo

Estas directrices cibernéticas de la IAPH están destinadas a ser utilizadas por el director general, el director ejecutivo, los ejecutivos de alto nivel y todos los altos directivos responsables de los puertos y las instalaciones portuarias que abarcan la comunidad portuaria mundial.

Este documento proporciona una descripción general de todos los temas relevantes necesarios para fortalecer la seguridad cibernética de equipos, redes, aplicaciones, sistemas e infraestructura críticos basados en TI/OT que respaldan todo el espectro de entornos administrativos y operativos portuarios e instalaciones portuarias.

Las Directrices Cibernéticas de la IAPH también reconocen la singularidad del ecosistema digital de un puerto o instalación portuaria frente a su posición dentro de la comunidad portuaria en la que reside, donde las tecnologías digitales se implementan e integran cada vez más. Colaboración entre puertos e instalaciones portuarias y las partes interesadas de la comunidad portuaria no solo se alienta sino que es necesaria para generar conciencia y elevar la resiliencia cibernética en toda la cadena de suministro marítimo a nivel local, regional y global.

Este documento reconoce además que la digitalización de los puertos y las instalaciones portuarias representa un desafío empresarial y no se limita al personal de TI. Fomentar una cultura ciberresiliente requiere cambios de comportamiento y una comprensión crítica de las consecuencias de las acciones de los individuos que conducen a amenazas cibernéticas. Los líderes de puertos e instalaciones portuarias deben comprender las interrelaciones e interdependencias que existen entre las entidades marítimas y reconocer la necesidad de analizarlas, la necesidad de colaboración interna y externa e intercambio de información, y el reconocimiento de una gestión disciplinada del cambio.

En última instancia, estas directrices tienen como objetivo ayudar a los equipos de liderazgo del puerto y de las instalaciones portuarias a comprometerse colectivamente, lograr consenso, compromiso interno y postular que la implementación de estas directrices es de hecho un esfuerzo orquestado de todas las disciplinas bajo el apoyo considerado de la máxima autoridad del entidad de que se trate. Si bien, al mismo tiempo, existe una necesidad muy real de implementación en flujos de trabajo reales para lograr con éxito operaciones eficientes y ciberseguras.

2. EL NEGOCIO DE GESTIONAR EL RIESGO

Dado que residen en el nexo del comercio mundial, los ataques cibernéticos contra puertos e instalaciones portuarias pueden ser perjudiciales y costosos. Si bien los datos intelectuales, financieros y/o personales pueden verse comprometidos y explotados, las interrupciones operativas pueden generar rápidamente consecuencias económicas e incluso políticas generalizadas. A medida que los puertos y las instalaciones portuarias adoptan nuevas tecnologías, como plataformas de automatización y sistemas IT/OT/IIoT integrados y habilitados en la nube, los líderes portuarios deben reconocer la gestión del riesgo cibernético como una responsabilidad de alto nivel, reconociéndola como un imperativo competitivo y operativo.

Dada la gran exposición a los riesgos, los ejecutivos de puertos e instalaciones portuarias se enfrentan a preguntas como: "¿Cuánta inversión es suficiente?" y "¿Cuál es mi retorno de la inversión?" son comunes. Ejemplos de tales fundamentos incluyen:

- El imperativo competitivo. Siempre se hacen concesiones sopesando la seguridad (que introduce ineficiencias) frente a las operaciones (que buscan eficiencia). Como resultado, los ejecutivos cuyo cálculo de riesgos se centra con demasiada frecuencia en TI aceptan sin querer algo de Tecnología Operacional (OT)
  exposiciones cibernéticas.
- El riesgo cibernético es omnipresente. Los factores de riesgo cibernético afectan todos los aspectos de la organización, incluidos administración y operaciones. La naturaleza global percibida del riesgo cibernético puede parecer abrumadora y tal vez incluso insuperable. Estas opiniones inhiben los esfuerzos proactivos para invertir en recursos clave (personas, procesos, herramientas y fondos).
- El riesgo cibernético es difícil de cuantificar. Si bien existen numerosas herramientas y métodos que intentan cuantificar el valor en riesgo cibernético, no existe un estándar común. Desarrollar escenarios de pérdidas para respaldar la cuantificación del riesgo cibernético implica colaboración, suposiciones y análisis subjetivo.
- Difícil cambiar el comportamiento y la cultura – No ha pasado nada, entonces ¿por qué cambiar? Este es uno de los mayores desafíos para la mayoría de las organizaciones. ¿Cómo se puede evitar que el personal abra correos electrónicos de phishing con enlaces incrustados a sitios infectados con malware o que descargue archivos adjuntos infectados con malware? ¿Cómo se mitiga la explotación de las redes sociales y al mismo tiempo se protege la privacidad y los datos? ¿Cómo se incentiva el intercambio de información crítica sobre amenazas cibernéticas?

Tales justificaciones revelan una percepción común que afecta a las suites ejecutivas: que las inversiones en ciberseguridad a menudo se consideran un centro de costos en lugar de un facilitador de las operaciones portuarias. Sin embargo, las respuestas a estas preguntas se pueden encontrar cuando quienes toman las decisiones emplean un lenguaje común y las encuadran en el contexto de las finanzas.

2.1 Desarrollar el caso de negocio para la ciberseguridad

Para determinar niveles razonables de inversión en gestión de riesgos cibernéticos, los ejecutivos primero deben comprender cómo un evento cibernético podría afectar la capacidad de funcionamiento de su organización y los costos potenciales de la interrupción, así como el impacto en las oportunidades comerciales. Esto implica determinar el impacto real en el negocio, lo que se puede lograr mediante un análisis de impacto en el negocio (BIA) y el desarrollo de escenarios realistas de pérdidas cibernéticas. Un BIA es una metodología para perfilar las posibles consecuencias de las interrupciones en la organización a través de sus procesos operativos, sistemas, aplicaciones, plataformas y/o equipos. La realización de un BIA permite a los ejecutivos identificar y

analizar funciones operativas y comerciales críticas y activos y sistemas clave, así como anticipar las posibles consecuencias de un evento disruptivo.

2.1.1 Determinar el impacto empresarial

Los BIA eficaces implican una colaboración interfuncional para permitir que diferentes partes interesadas de todo el mundo puerto o instalación portuaria para explicar cómo un evento inesperado podría afectar sus actividades comerciales y/o funciones operativas. Estos conocimientos ayudarán a priorizar funciones específicas y, cuando se identifiquen los objetivos de punto de recuperación (RPO) y los objetivos de tiempo de recuperación (RTO)11 , ayudarán a los ejecutivos a comprender mejor que dichas funciones operativas podrían verse afectadas por un ciberataque. Una BIA caracterizará los impactos operativos y financieros resultantes de la interrupción de las funciones comerciales y los procesos operativos. Los impactos que los puertos y las instalaciones portuarias deben considerar pueden incluir:

- Interrupción/pérdida de acceso a sistemas o infraestructura críticos (por ejemplo, puertas portuarias automatizadas, carga de carga, operaciones de terminales, gestión del tráfico), lo que resulta en retrasos logísticos.
- Pérdida o retraso en ventas e ingresos.
- Impactos en salud, seguridad y medio ambiente.
- Aumento de gastos (por ejemplo, horas extras de mano de obra, subcontratación, costos de agilización, honorarios legales, etc.).
- Multas incurridas por infracciones regulatorias.
- Penalizaciones contractuales o pérdida de bonificaciones contractuales.
- Insatisfacción o deserción del cliente/daño a la reputación.

2.1.2 Desarrollar escenarios de pérdidas realistas

Al calcular los costos para diversos escenarios de pérdidas, los ejecutivos de puertos o instalaciones portuarias pueden obtener información crítica sobre qué activos, datos, aplicaciones, procesos, sistemas o infraestructura podrían desencadenar las consecuencias más costosas o disruptivas, si se ven comprometidos. Si bien es difícil modelar las consecuencias financieras legales y para la reputación, el valor del análisis de escenarios de pérdidas cibernéticas puede ofrecer beneficios adicionales en la continuidad del negocio y la planificación de la recuperación ante desastres (Sección 7) por la forma en que:

- Facilita la colaboración entre diferentes partes interesadas de toda la organización (por ejemplo, TI, seguridad, operaciones, asuntos legales, seguridad, finanzas y administración, salud y seguridad).
- Obliga a los contribuyentes a reconocer que las amenazas cibernéticas pueden afectar todos los aspectos del ecosistema de la organización, incluidos clientes y socios externos de la comunidad portuaria/de carga.
- Apoya evaluaciones de controles, procesos y herramientas en el contexto de situaciones del mundo real.
- Educa a los participantes sobre el posible valor en riesgo asociado con las inversiones (o no inversiones) de la organización en los recursos necesarios para la ciberdefensa.
- Ayuda a priorizar las inversiones basándose en el análisis de los impactos empresariales.
- Informa los seguros cibernéticos (Sección 2.4.1).

El desarrollo de escenarios de pérdidas ciberespecíficas y ciberfísicas facilita el proceso de BIA para puertos e instalaciones portuarias. Los escenarios de pérdidas ilustran cómo un incidente cibernético puede resultar en una pérdida financiera calculable.
Los ejemplos incluyen la pérdida de acceso a los sistemas operativos de las terminales, equipos de manipulación de carga, controles de acceso a las puertas, dispositivos de escaneo portátiles (incluido RFID), infraestructura de generación y distribución de energía, almacenamiento y transmisión de líquidos a granel, comunicaciones, sistemas de gestión del tráfico de embarcaciones y oficinas. -computadoras en red. Los activos o personas comprometidos en entornos de oficina pueden

---

11 Los RPO describen el tiempo que dura una interrupción antes de que la cantidad de datos perdidos durante ese período supere el umbral o "tolerancia" máximo permitido de la organización. Los RTO definen la duración de tiempo y un nivel de servicio establecido dentro del cual el proceso de negocio, activo o sistema debe restaurarse después de que ocurra un evento para evitar consecuencias inaceptables. La RTO responde a la pregunta: "¿Cuánto tiempo tardó en recuperarse después de la notificación de la interrupción?"

también resultan en pérdidas financieras debido a ataques contra la integridad de los datos, como la suplantación de correo electrónico fraudulento, la manipulación de datos manifiestos y los ataques de intermediarios que redirigen los pagos.

Los escenarios de pérdidas cibernéticas se pueden desarrollar teniendo en cuenta las siguientes consideraciones (Sección 6.5):

- ▪ Definición de escenario : desarrollar escenarios en torno a eventos históricos o condiciones hipotéticas, solicitando el trabajo en equipo de las partes interesadas. Considerar eventos del mundo real para informar sobre el diseño de escenarios modificando las experiencias de otros al perfil de la organización y capacidades específicas.

- ▪ Probabilidad del escenario : la estimación de la probabilidad de un incidente cibernético debería involucrar a las partes interesadas clave de todas las áreas operativas. Utilizando incidentes pasados y/o tendencias actuales de amenazas cibernéticas como guía y aplicando una metodología consistente, caracterizar la probabilidad de cada.
- ▪ Centrarse en lo inesperado : no limitar el enfoque a lo que se consideraría inesperado, grave y sumamente disruptivo en lugar de las pérdidas esperadas, que pueden deberse a un desgaste normal o pérdidas asociadas con el costo de hacer negocios. ▪ Desarrollar una historia realista : los escenarios deben ser de alto impacto pero realistas. Considere piratas informáticos maliciosos, competidores, personas internas descontentas con privilegios administrativos, eventos accidentales causados por empleados o eventos desencadenados por proveedores debido a parches comprometidos.
- ▪ Definir los resultados : una vez definido un escenario, los resultados potenciales deben variarse y definirse claramente, con estimaciones de costos atribuidas a cada resultado. Los ejemplos incluyen: retrasos operativos, pérdida de ingresos, respuesta a incidentes y esfuerzos de mitigación, costos legales y multas.

- ▪ Definir lo que existe : identificar los controles y sistemas existentes y analizar cómo se podría utilizar cada uno para prevenir, detectar y responder a las condiciones del escenario. Además, justifique qué tan efectivo es cada uno de ellos. Considere: ¿Cómo se afectan entre sí los controles y los sistemas? ¿Existen dependencias? ¿Cuál es la probabilidad de que fracasen?
- ▪ Definir la Frecuencia – Estimar la frecuencia de los eventos, que debe ser el resultado de esfuerzos cooperativos entre los actores responsables de varias áreas operativas.
- ▪ Definir la gravedad de los resultados : caracterizar y definir la gravedad de cada resultado.
- ▪ Cuantificar todos los resultados : definir y asignar valores financieros de las pérdidas relacionadas con activos, sistemas, equipos, infraestructura, costos de recuperación o, si es necesario, reemplazo, costos de servicios de terceros prestados, pérdida de ingresos, etc.
- ▪ Ajustarse al sesgo : es parte de la naturaleza humana que las personas tengan un sesgo optimista en sus percepciones de conocimiento personal, habilidades, competencia y capacidad general para tener éxito. Para evitar sesgos, base los escenarios de pérdidas en una entidad hipotética que refleje la organización. Pregunte a diferentes grupos de personas de la organización, así como a entidades interesadas relevantes, sus juicios subjetivos.

2.2 Estableciendo un lenguaje común

2.2.1 Lenguaje y responsabilidad de las partes interesadas

Los equipos de liderazgo de puertos e instalaciones portuarias también enfrentan el desafío del lenguaje y la comunicación. La gestión exitosa del riesgo cibernético comienza y depende de una comprensión común de los términos, una base financiera y el reconocimiento de la responsabilidad compartida.

2.2.2 La importancia de los términos comunes compartidos

En respuesta a las amenazas cibernéticas, los ejecutivos de puertos e instalaciones portuarias a menudo despliegan recursos (su gente, procesos, herramientas y financiamiento) de una manera reactiva basada en diferentes suposiciones y terminologías inconsistentes. Los términos comunes a algunos pueden tener diferentes significados dependiendo del

contexto del entorno operativo específico de la organización y los roles, responsabilidades y experiencias del personal. Por ejemplo, un “incidente” cibernético para una organización puede implicar una variedad de eventos posibles, mientras que dentro de otra el término puede indicar un significado más limitado.

Es importante destacar que los términos inconsistentes pueden crear confusión, como escalada indisciplinada, alertas ad hoc e informes irregulares que pueden poner en peligro las operaciones y la prestación de servicios o, más ampliamente, poner en riesgo a los socios de la comunidad portuaria. Esto puede frustrar a las partes interesadas clave y a los socios comerciales y producir condiciones que permitan que los riesgos cibernéticos se multipliquen y afecten a otras partes interesadas.

El primer paso para instituir un idioma común requiere establecer un vocabulario común. Las partes interesadas del puerto y de las instalaciones portuarias deben acordar la terminología que se utilizará dentro de la organización, que debe usarse para facilitar comunicaciones claras e inequívocas entre los diferentes grupos de partes interesadas internas. Esto mejorará la claridad de las comunicaciones cibernéticas a nivel organizacional y comunitario y reducirá la probabilidad de malentendidos y/o faltas de comunicación. Se incluye un glosario de términos para ayudar a las partes interesadas en este proceso.

2.2.3 Gestión del riesgo cibernético en el contexto financiero

Además de establecer un vocabulario común, los debates sobre el riesgo cibernético deben basarse en el contexto financiero . Al hacerlo, se transforma el debate sobre la gestión del riesgo cibernético en concepciones estructurales y métricas de gestión financiera empresarial fácilmente reconocibles . Establecer la intersección entre riesgo cibernético y dinero en todas las áreas de un puerto o instalación portuaria ofrecerá un medio de medición para informar sobre las decisiones de inversión relacionadas con la identificación, asignación y priorización de recursos.

El análisis de escenarios de pérdidas apoya este proceso al iluminar los riesgos en términos financieros. Sin embargo, sólo representa la primera parte del concepto de ciberriesgo-dinero. Utilizando los resultados del escenario de pérdidas, las partes interesadas pueden determinar cómo priorizar mejor la apropiación de los recursos disponibles:
su gente, procesos, herramientas y financiación, que representan un costo, al comparar efectivamente el costo del riesgo (por ejemplo, escenarios de pérdidas) con el costo de los recursos. Fundamentar financieramente el riesgo cibernético
La discusión gerencial brinda a los ejecutivos y tomadores de decisiones clave el contexto comercial y los conocimientos operativos necesarios para tomar decisiones informadas de manera consistente con respecto a la planificación de inversiones y la asignación de recursos.

2.3 Otras consideraciones comerciales clave

2.3.1 Transferencia de riesgos

Los actores de las amenazas cibernéticas son implacables, creativos, persistentes y muy motivados. Los riesgos insuficientemente mitigados dejan a las organizaciones expuestas a pérdidas potenciales, responsabilidad propia y de terceros, multas y una serie de costos en cascada relacionados con los esfuerzos de mitigación, respuesta y recuperación. Es importante reconocer que los riesgos cibernéticos evolucionan constantemente y no pueden eliminarse por completo. Pero el riesgo cibernético se puede mitigar, aceptar, evitar o transferir (Sección 7).

Transferir parte del riesgo cibernético a través de seguros ofrece a los líderes portuarios y de las instalaciones portuarias una estrategia adicional de mitigación de riesgos porque el seguro cibernético puede ayudar a cubrir los costos de respuesta y recuperación en caso de un ataque cibernético. A medida que se intensifica la sofisticación tecnológica de las operaciones portuarias, y a medida que evoluciona la automatización y la infraestructura de TI/OT/IIoT, los puertos y las instalaciones portuarias que invierten en gestión de riesgos cibernéticos tal vez deseen considerar involucrar a sus corredores de seguros para discutir opciones de seguros de ciberseguridad.

Sin embargo, los ejecutivos de puertos e instalaciones portuarias deben abordar el seguro de ciberseguridad con cautela y en colaboración con asesores legales para elaborar políticas apropiadas al riesgo de la organización. La cobertura cibernética no libera a una organización de la responsabilidad de gestionar sus riesgos cibernéticos, sino que requiere que el puerto o la instalación portuaria mantenga un programa de ciberseguridad que fomente la mejora continua.

Para prepararse para el ciberseguro, un buen primer paso es evaluar las capacidades generales de ciberseguridad de la organización y su exposición al riesgo. Para lograr esto, primero la organización debe revisar las pólizas de seguro actuales para ver cómo podrían funcionar frente a un conjunto de escenarios de pérdidas realistas. A continuación, debe identificar y caracterizar las capacidades actuales de ciberseguridad organizacional que abarcan todas las áreas funcionales. Luego, debe considerar implementar un enfoque basado en la madurez de la ciberseguridad, como se analiza en la Sección 11, que muchos suscriptores utilizan para elaborar políticas y umbrales de precios en lugar de historiales actuariales relacionados con la ciberseguridad.

2.3.2 El presupuesto y el desafío del “ROI”
Las inversiones en ciberseguridad requieren decisiones presupuestarias y la pregunta “¿Cuánto es suficiente?”
Se deben considerar al implementar un programa de ciberseguridad. Los tomadores de decisiones con responsabilidades de pérdidas y ganancias examinan las inversiones en seguridad debido a la dificultad para pronosticar el retorno de la inversión (ROI). Por lo general, las inversiones en seguridad se miden en función del potencial de pérdidas basadas en escenarios hipotéticos que afectan la reputación de una organización, reclamos de responsabilidad de primera y tercera parte, pérdida de ingresos, multas regulatorias, etc. A diferencia de las inversiones en equipos y sistemas de seguridad física, Como el vídeo en red o los sistemas de control de acceso, las inversiones en ciberseguridad han tardado en consolidarse porque sus beneficios percibidos pueden parecer menos obvios para los profesionales de la seguridad desinformados.
Algunas organizaciones también podrían evaluar qué contratos y oportunidades comerciales pueden estar disponibles para ellos si cumplen con ciertos requisitos de ciberseguridad que algunas partes interesadas exigen en sus negocios.
contratos.

Las organizaciones de todos los sectores reconocen cada vez más que un presupuesto dedicado a la ciberseguridad es fundamental para la gestión del riesgo cibernético. A medida que los puertos y las instalaciones portuarias buscan comprender mejor y abordar eficazmente las amenazas cibernéticas, uno de los primeros pasos que se deben tomar debe ser establecer un presupuesto operativo dedicado y sostenible para apoyar las actividades de gestión de riesgos cibernéticos.

Con la excepción de unos pocos puertos e instalaciones portuarias importantes, las inversiones en ciberdefensa y gestión de riesgos han estado insuficientemente financiadas, han sido ad hoc en su ejecución y reaccionarias. Las inversiones desenfocadas dejan los puertos expuestos a ciberataques y explotación asimétricos.

Si bien muchos ejecutivos pueden suponer que las amenazas cibernéticas pueden abordarse aumentando los presupuestos de TI, son más efectivas cuando se organizan de manera coordinada bajo un programa de ciberseguridad.
Los presupuestos de ciberseguridad deben abordar la gestión de riesgos cibernéticos en todas las áreas operativas del negocio, incluidas TI, operaciones, seguridad, capacitación, seguridad física, salud y seguridad, administración y respuesta a incidentes.
En este contexto, la comprensión de la distinción entre Tecnología de la Información (TI) y Tecnología de Operación (OT) es crucial. TI se relaciona con productos de hardware y software que sientan las bases de su sistema de información, como servidores, servicios en la nube, componentes de redes de comunicación, sistemas de administración, software empresarial, etc. OT, por otro lado, se relaciona con hardware y software que detecta o causa un cambio, a través del seguimiento y/o control directo de equipos, activos, procesos y eventos industriales12.

Además, los comisionados portuarios y las juntas directivas y ejecutivos (especialmente aquellos que supervisan las empresas que cotizan en bolsa) enfrentan obligaciones y responsabilidades fiduciarias para asignar los fondos necesarios para ejecutar un programa de gestión de riesgos cibernéticos en toda la empresa. Para propiedad privada

12 Ver https://en.wikipedia.org/wiki/Operational_technology

Para las organizaciones, las responsabilidades son menos claras, pero estas directrices pueden ayudar a las partes interesadas a establecer estándares comunes de atención.

2.4 Organización para gestionar el riesgo cibernético

Un estudio del Foro Económico Mundial descubrió que el mayor impulsor de la capacidad de ciberseguridad organizacional (y por lo tanto de la resiliencia) era el compromiso ejecutivo. Se descubrió que esto es cierto independientemente del tamaño, el sector y la disponibilidad de recursos de una organización.13

Aunque la brecha digital puede caracterizarse por la disponibilidad de recursos que separa los puertos y las instalaciones portuarias, el término también puede aplicarse para describir las percepciones de la ciberseguridad: es decir, ¿qué es y quién es el responsable? – separar a los tomadores de decisiones dentro de la misma organización. En este sentido, la brecha digital plantea menos un desafío económico que distingue las capacidades de los puertos y de las instalaciones portuarias entre sí, que un desafío intelectual que divide a los tomadores de decisiones clave dentro de la misma organización. Por lo tanto, antes de contratar recursos técnicos, los ejecutivos del puerto o de las instalaciones portuarias primero deben organizarse para gestionar el desafío de la ciberseguridad. Esto implica identificar al personal clave, asignar tareas y definir responsabilidades, consolidar protocolos de supervisión y presentación de informes e implementar un grupo de trabajo.

2.4.1 Identificación de ciberstakeholders en el entorno portuario

Las partes interesadas cibernéticas de puertos e instalaciones portuarias incluyen a todo el personal administrativo y de operaciones que accede a activos digitales para crear, acceder, procesar, almacenar o transmitir datos electrónicos, interna o externamente, a terceros gubernamentales y comerciales. Si bien esto incluye una amplia gama de partes interesadas internas, también debe ampliarse para incluir partes interesadas externas, como proveedores y/o socios clave que acceden a la infraestructura y los activos digitales del puerto o instalación portuaria, y que dependen de la confidencialidad, integridad y disponibilidad. de datos. Dado que las partes interesadas pueden cambiar con el tiempo dependiendo de la dinámica del ecosistema portuario, se debe realizar una revisión periódica de estas partes interesadas en consecuencia.

2.4.2 Deberes, responsabilidades y autoridades

Tanto en las operaciones diarias como en las situaciones de crisis, las funciones, responsabilidades y autoridades basadas en funciones claras son esenciales para una gestión eficaz del riesgo cibernético. Esto comienza con la identificación y definición de roles y responsabilidades apropiados de las partes interesadas para acceder y supervisar actividades que involucran activos e infraestructuras conectados digitalmente. Luego se deben identificar las partes interesadas para estos puestos y asignarles las responsabilidades adecuadas y otorgarles las autoridades necesarias para
realizar eficazmente sus funciones de gestión de riesgos cibernéticos. Fundamentalmente, y como se analiza en la Sección 9,
Las autoridades deben asignarse a partes interesadas con los conocimientos, habilidades y/o habilidades (KSA) necesarios.

Las responsabilidades específicas incluyen, entre otras, garantizar que las capacidades, los controles técnicos, los procedimientos y los procesos de ciberseguridad se empleen y mantengan adecuadamente en todos los entornos operativos. Por ejemplo, se debe monitorear la seguridad física del hardware crítico (por ejemplo, servidores en áreas restringidas) y, con ello, se deben asignar tareas definidas para que esta actividad se complete y audite suficientemente. La asignación de deberes, responsabilidades y autoridades basadas en roles no es una actividad única. Las organizaciones deben revisar periódicamente las funciones, responsabilidades y autoridades para garantizar que sigan siendo apropiadas y relevantes y sigan apoyando la misión de la empresa.

13 Ver: http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

2.4.3 Establecimiento de la responsabilidad de supervisión de la gestión del riesgo cibernético

Si bien el éxito de la gestión del riesgo cibernético de un puerto o instalación portuaria requiere un esfuerzo colectivo, la organización debe definir quién tiene la supervisión general del programa. Los propietarios, accionistas e inversores institucionales (por ejemplo, capital privado) evalúan el riesgo cibernético en términos de riesgo para las inversiones.

Sin embargo, la supervisión operativa de la gestión del riesgo cibernético recae en aquellas personas que tienen la responsabilidad final de la gobernanza de la autoridad portuaria o instalación portuaria. Este es el director ejecutivo, el director general u otra persona designada, y su responsabilidad incluye informes a nivel de la junta directiva.

Para implementar la supervisión y la rendición de cuentas, y gestionar el riesgo cibernético de su organización, la organización también debe identificar y nombrar un Director de Seguridad de la Información (CISO) designado, o asignar las funciones de un CISO a un Director de Información (CIO) o similar. El CISO dirige el programa de ciberseguridad y su función incluye, entre otras, la implementación y el mantenimiento de planes, políticas, procedimientos y controles de ciberseguridad; operaciones técnicas; y comunicaciones internas/externas. Si bien el rol del CISO reporta directamente al CEO o al Director General, también se les debe otorgar un acceso "de línea de puntos" a la Junta.

2.4.4 El papel de la Junta en la gestión del riesgo cibernético

El riesgo cibernético se ha convertido en uno de los temas más importantes en las discusiones actuales en las salas de juntas. Una responsabilidad principal de la Junta es instituir la supervisión del riesgo cibernético, que puede hacerse cumplir a través de un mecanismo de auditoría (por ejemplo, un comité de auditoría) para monitorear las políticas que respaldan el programa de gestión del riesgo cibernético del puerto o de la instalación portuaria. Por ejemplo, como mínimo trimestralmente, las juntas directivas deben esperar informes de la alta dirección sobre el estado del programa de ciberseguridad de la organización. En la mayoría de los casos, los miembros de la Junta Directiva de un puerto o instalación portuaria no son expertos en ciberseguridad. Para ser eficaces, las Juntas deben estar informadas sobre los riesgos cibernéticos, los incidentes (incluidos los resultados) y las opciones para el tratamiento, aceptación y transferencia de riesgos.

Para apoyar la toma de decisiones para una adecuada planificación de inversiones y asignación de recursos, el
El lenguaje de los informes debe basarse en una terminología compartida, la utilización de indicadores clave de desempeño e incluir fundamentos financieros. Si bien esto es responsabilidad de los CISO o CIOS en las organizaciones más grandes, las organizaciones más pequeñas pueden asignar dichas responsabilidades al personal de operaciones o de TI.

Una opción rentable y de tendencia es la subcontratación del rol de CISO a asesores externos que estén contratados (por ejemplo, a tiempo parcial) para apoyar los esfuerzos de ciberseguridad dirigidos por la Junta. Para ser eficaces, las Juntas deberían:

- Esté preparado para contratar expertos externos para comprender el riesgo cibernético (si no, busque capacitación).
- Revisar los mecanismos para supervisar las actividades de gestión de riesgos cibernéticos.
- Revisar las decisiones de asignación y desarrollo de recursos.
- Tener un proceso para revisar las pólizas de seguro para garantizar que los factores de riesgo cibernético sean dirigido.
- Designar a una persona responsable de implementar el programa de gestión de riesgos cibernéticos y quien reporta directamente al Directorio al menos trimestralmente.
- Contar con un proceso para gestionar su reputación cibernética y abordar las exposiciones públicas.
- Apoyar la campaña de educación/concientización en toda la organización que aborde la ciberseguridad.

2.4.5 Impulsar la ciberseguridad en toda la organización: el comité directivo de ciberseguridad Un enfoque rentable que puede adoptar un puerto o una instalación portuaria es establecer un comité directivo interno dedicado a la ciberseguridad. Establecer uno puede convertirse en una herramienta clave en los esfuerzos de la organización para asumir la responsabilidad de la estrategia cibernética general, garantizar la coordinación en su implementación, reducir el potencial de duplicación en el gasto en seguridad, consolidar líneas de presentación de informes, control y supervisión de inversiones y/o infraestructuras complejas. agilizar las comunicaciones e impulsar el cambio cultural.

La función del comité directivo de ciberseguridad es asumir y coordinar las iniciativas a nivel de todo el puerto o de las instalaciones portuarias destinadas a reducir el riesgo cibernético. Bajo la dirección del CISO o CIO, permite a la organización optimizar la presupuestación y las adquisiciones, impulsar el consenso, asignar autoridades e instituir la responsabilidad, y servir como el principal impulsor para el intercambio de información y el compromiso interfuncional entre las partes interesadas del puerto/instalación portuaria. Los comités directivos eficaces deberían:

- Implementar un estatuto que incluya una declaración de aceptación ejecutiva.
- Definir autoridades y responsabilidades.
- Asumir la propiedad de la estrategia, el plan y las actividades de gobierno de la organización.
- Coordinar las comunicaciones a nivel de organización, incluida la respuesta previa y posterior al incidente.
- Gobernar los protocolos de intercambio de información.

Otras funciones cruciales en la gobernanza de la ciberseguridad también deberían incluir:

- Líder de ciberseguridad designado : una función gerencial para comprender, especificar los riesgos cibernéticos y proporcionar insumos para la estrategia y el plan cibernéticos, así como coordinar las medidas a nivel operativo de las acciones relacionadas con la ciberseguridad.

2.5 Estrategias de liderazgo para impulsar el cambio

La gestión del riesgo cibernético sólo tiene éxito con la participación y supervisión activa de los ejecutivos.
Los líderes eficaces implementan de forma proactiva capacidades de ciberseguridad que son multidisciplinarias e involucran a todas las áreas funcionales. Las siguientes estrategias pueden ayudar a los ejecutivos a impulsar sus organizaciones:

- Facilitar y participar en el proceso de toma de decisiones. Participar en el desarrollo, análisis y determinación de apetitos de riesgo operacional. Considere: ¿Qué está en riesgo? ¿Qué es y qué no es aceptable estar en riesgo? ¿Cuáles son las compensaciones con respecto a la exposición, aceptación, evitación, mitigación y transferencia del riesgo? ¿Cuáles son las prioridades? ¿Quién debería participar?

- Impulsar activamente la concienciación y el compromiso sobre los riesgos cibernéticos en todas las áreas funcionales. Cada individuo es un objetivo potencial para los actores de amenazas cibernéticas. Es fundamental involucrar al personal de todas las áreas funcionales, incluidas operaciones, legal, contratos, adquisiciones, ventas/marketing, relaciones públicas y administración y finanzas. Una opción adicional es integrar personas influyentes clave en la organización que ayuden a promover o educar al personal sobre la concienciación sobre los riesgos cibernéticos a nivel departamental o operativo local. Es importante incorporar consideraciones de ciberseguridad en los contratos y acuerdos de servicios. Se fomenta la colaboración mediante el empleo de grupos de trabajo internos con superposiciones operativas.

- Cambiar comportamientos. Dado que el cambio nunca es fácil, las organizaciones deberían comenzar con pasos simples. Patrocine capacitación periódica sobre concientización cibernética e implemente una campaña de concientización por correo electrónico que destaque las vulnerabilidades asociadas con el correo electrónico o utilice la gamificación para la capacitación sobre riesgos cibernéticos como una forma alternativa de atraer el interés de las personas. No limite las tareas y responsabilidades al personal de TI o de Seguridad. Incluir responsabilidades, métricas e incentivos de ciberseguridad en las revisiones de desempeño en toda la organización. Teniendo en cuenta la cultura de la comunicación, se deben tomar iniciativas que sean adecuadas y adaptables y que puedan medirse por su efectividad.

- Enfoque dinámico. Al reconocer la naturaleza siempre cambiante del panorama de las amenazas cibernéticas, los esfuerzos de gestión del riesgo cibernético deben reevaluarse continuamente, lo que también debe tener en cuenta el perfil de riesgo cibernético de la organización desde la perspectiva del atacante.
- Implementar gobernanza y rendición de cuentas. Los humanos naturalmente buscan atajos. Algunos eludirán activamente las políticas y controles de ciberseguridad, por muy rigurosos que sean. Considere formalizar las responsabilidades de ciberseguridad en todos los roles, definir las autoridades apropiadas y reforzarlas con procedimientos de presentación de informes para permitir el seguimiento de los objetivos definidos. Hacer cumplir las políticas y compromisos y responsabilizar a las personas.
- Responsabilidad. Los especialistas legales deben participar activa y regularmente en las actividades de planificación previa a la vulneración para garantizar que la organización pueda responder y recuperarse adecuadamente de un ciberataque que pueda implicar riesgos para los propios y terceros.

3. CIBERSEGURIDAD Y GESTIÓN DE RIESGOS

3.1 Riesgo cibernético en la industria marítima

Según la OMI, el riesgo cibernético marítimo se refiere a una medida del grado en que un activo, sistema, aplicación o infraestructura conectada podría verse amenazado por una posible circunstancia o evento, que puede resultar en fallas operativas, de seguridad o de protección relacionadas con el transporte marítimo. como consecuencia de la corrupción, pérdida o compromiso de información o sistemas14.

La OMI define además la gestión del riesgo cibernético como el proceso de identificar, analizar, evaluar y comunicar un riesgo relacionado con el ciberespacio y aceptarlo, evitarlo, transferirlo o mitigarlo a un nivel aceptable, considerando los costos y beneficios de las acciones tomadas para las partes interesadas.

Muchas plataformas integradas de TI, OT y IIoT en el sector marítimo siguen dependiendo de tecnologías y sistemas heredados que no fueron diseñados originalmente para cumplir con requisitos sólidos de ciberseguridad. La implementación de eficiencias operativas en los puertos y las instalaciones portuarias ha dado como resultado aplicaciones y plataformas independientes, equipos e infraestructura en red habilitados para OT que se integran con redes Wi-Fi y con ellos se conectan a Internet a través de sistemas administrativos. Si bien algunos esfuerzos han sido cuidadosamente planificados, otros son el resultado de esfuerzos ad hoc impulsados por las necesidades del negocio.

Si bien las plataformas integradas de TI, OT y IIoT ofrecen eficiencias mensurables, también introducen nuevas vulnerabilidades de ciberseguridad de formas nunca antes previstas. Algunas empresas optan por no integrar estos sistemas (IT, OT e IIOT) en su red, mientras que otras los integran en una red perfecta. Los riesgos involucrados dentro de la integración de estos sistemas deben evaluarse antes de realizar la integración.

El alcance de la integración ad hoc está tan extendido en la comunidad mundial de puertos e instalaciones portuarias que no es inusual descubrir conexiones de red de TI y OT desconocidas que abandonan sus
Organizaciones vulnerables a los ciberataques.

La realidad de la economía global conectada de hoy es que las operaciones marítimas dependen de la conectividad a Internet, y la creciente dependencia de los proveedores que acceden a activos en red, proveedores de servicios basados en la nube y cadenas de suministro en red no hacen más que subrayar el potencial de un riesgo cibernético en cascada. Si bien los ataques cibernéticos contra partes interesadas marítimas ocurren a diario, dos víctimas notables portuarias/instalaciones portuarias incluyen:

- AP Moller-Maersk. Originario de Ucrania y disfrazado de ransomware en 2017, el malware NotPetya se propagó por todo el mundo tan rápidamente a través de conexiones a Internet que organizaciones que abarcaban una variedad de industrias fueron atacadas indiscriminadamente y vulneradas con éxito. El impacto fue rápido y severo, y el impacto en la naviera danesa AP Moller-Maersk fue global. Las revelaciones públicas indicaron que el ataque interrumpió 17 terminales de contenedores en todo el mundo, interrumpió las operaciones globales y obligó a las partes interesadas a volver a procesos manuales para gestionar y rastrear los envíos. Los retrasos en los camiones crecieron
  miles.

14 https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx#:~:text=Maritime%20cyber%20risk%20refers%20to,siendo%20corrupto%2C%20lost%20or%20comprometido

- El Puerto de Shahid Rajaee. En mayo de 2020, el puerto de Shahid Rajaee en Irán sufrió un ciberataque que dio lugar a una serie de acciones disruptivas.15 El ataque provocó el cierre de los sistemas informáticos del puerto que controlaban el flujo de embarcaciones, vehículos y mercancías.
  Las actividades de carga y descarga de mercancías se paralizaron, aumentaron los atascos de tráfico fuera del puerto y los buques no pudieron atracar. Las partes interesadas de la autoridad portuaria se vieron obligadas a volver a los procesos de carga y descarga manuales, lo que afectó gravemente a la eficiencia.

Estos eventos sirven como continuas llamadas de atención para los ejecutivos de los puertos y las instalaciones portuarias. Independientemente de si un ciberataque tiene como objetivo una víctima en el otro lado del mundo, la naturaleza integrada de la economía marítima global deja a todos los puertos e instalaciones portuarias a ambos lados de la brecha digital. vulnerables a ataques e interrupciones operativas del sistema de transporte marítimo global.

3.2 Definición de ciberseguridad

¿Qué es la ciberseguridad?

¿Qué es la ciberseguridad?

La ciberseguridad se refiere a la protección de los sistemas de TI, OT y IIoT (hardware, software e infraestructura asociada), las redes y los datos que contienen, y los servicios que brindan, contra el acceso no autorizado, el daño, el uso indebido o la destrucción. Esto incluye daños causados por causas intencionales o no intencionales. Además, respalda la preservación de la confidencialidad, integridad y disponibilidad de la información, e incluye atributos adicionales de autenticidad, responsabilidad, no repudio y confiabilidad. Cuando los entornos ciberfísicos se cruzan, su propósito es evitar que se produzcan acciones físicas no deseadas. Las mejores prácticas de ciberseguridad abordan controles de personas, procesos y tecnología para permitir una mejor resiliencia organizacional frente a los ciberataques, al respaldar las actividades de protección, detección, respuesta y recuperación.

—El conjunto de conocimientos sobre seguridad cibernética, V1.0, 31 de octubre de 2019; Ver: https://www.cybok.org

Figura 1 - ¿Qué es la ciberseguridad?

15 https://www.timesofisrael.com/6-facilities-said-hit-in-irans-cyberattack-on-israels-water-system-in-april/

3.3 Qué está en riesgo: confidencialidad, integridad y disponibilidad de los datos

Un riesgo es una situación en la que una amenaza explota una vulnerabilidad, que puede afectar negativamente a los datos, el sistema o la red. La disponibilidad, la integridad y la confidencialidad, normalmente conocidas como la "tríada de la CIA" 16 , protegen la . A cadena de suministro marítima global hiperconectada, que depende del intercambio eficiente y confiable de datos, así como de sistemas OT que permitan operaciones eficientes, los puertos y las instalaciones portuarias deben tratar de gestionar los riesgos cibernéticos dentro de sus límites aceptables definidos.

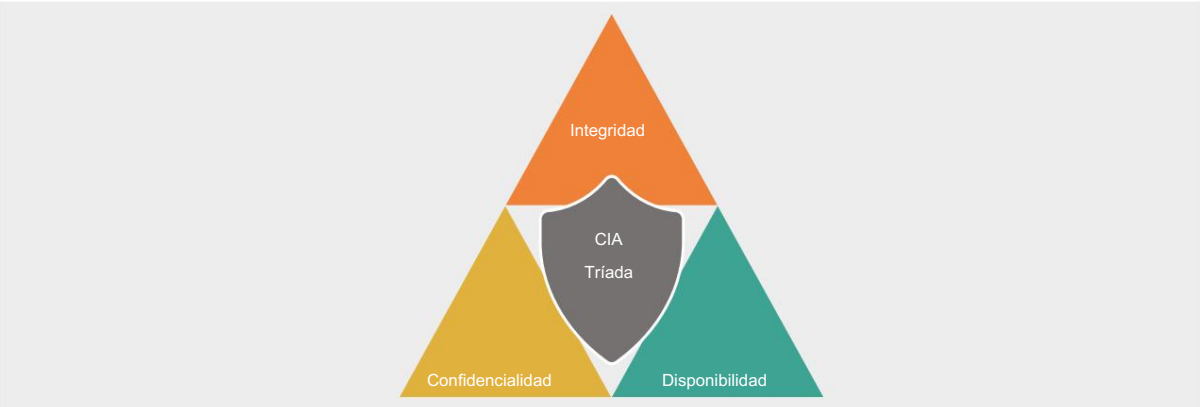

Figura 2 - Tríada de la CIA

- Confidencialidad: Garantiza que la información o los sistemas sólo sean accesibles para usuarios autorizados. Para proteger la confidencialidad de sus datos, un puerto o instalación portuaria puede agrupar la información según su sensibilidad y acceso restringido, tanto digital como físicamente. Las tácticas para garantizar la confidencialidad incluyen permisos de archivos, cifrado y listas de control de acceso.
- Integridad: La integridad se refiere a preservar la precisión de la información o del sistema; se trata de la protección de datos contra modificaciones o eliminaciones no autorizadas. Las violaciones de integridad pueden socavar la confianza en que los datos sobre bienes, clientes o finanzas ya no son confiables.

  Los puertos y las instalaciones portuarias pueden utilizar control de versiones o copias de seguridad del sistema para garantizar que se puedan revertir los cambios no autorizados en los datos.
- Disponibilidad: La disponibilidad representa la certeza de que los usuarios de un sistema o información digital pueden hacer uso de él cuando lo necesiten. Las amenazas cibernéticas dirigidas a la disponibilidad pueden causar interrupciones críticas del sistema, que incluyen sistemas operativos de terminales, operaciones habilitadas para Wi-Fi y RFID, sistemas ERP de oficina y comunicaciones habilitadas en red, como teléfonos basados en IP. Para proteger la disponibilidad, los puertos y las instalaciones portuarias pueden contar con una serie de redundancias (sistemas, comunicaciones e incluso copias de seguridad de datos), así como protecciones contra ataques de denegación de servicio.

La Tríada de la CIA se utiliza ampliamente para guiar el desarrollo de políticas de seguridad de la información. Para los puertos y las instalaciones portuarias, ofrece consideraciones importantes sobre los pasos que se pueden tomar para mejorar la resiliencia cibernética.

16 A veces también denominada “Tríada AIC” para evitar confusión con la Agencia Central de Inteligencia de Estados Unidos.

3.4 Gobernanza

Se requiere la aceptación ejecutiva con respecto a la implementación de políticas de gestión de riesgos cibernéticos y un marco de gobernanza relacionado para cualquier puerto o instalación portuaria que busque volverse ciberresiliente.
Las políticas sólidas de gestión de riesgos cibernéticos implementadas bajo un marco de gobernanza eficaz pueden hacer que los servicios de TI de una organización marítima sean más eficientes y las operaciones habilitadas para OT más productivas.

Al introducir políticas de gestión de riesgos cibernéticos dentro de la organización, es fundamental que los ejecutivos las alineen con los objetivos operativos definidos. Con demasiada frecuencia, las áreas funcionales clave operan de forma aislada: el personal de TI se concentra en los asuntos de TI; personal de operaciones enfocado en operaciones de carga; personal de seguridad centrado en la seguridad; etcétera. En el marco de un marco integrado de cibergobernanza, que puede coordinarse en el marco del comité directivo de ciberseguridad (Sección 2.4.5),
Los planes y documentos de políticas deben revisarse y actualizarse periódicamente a medida que evolucionan las estructuras organizativas, se ajustan las autoridades, se adoptan nuevas tecnologías y/o procesos y cambian las amenazas y vulnerabilidades. Más importante aún, lo esencial de estos documentos debe traducirse en mensajes integrales para una comunicación en toda la organización.

Para respaldar los esfuerzos de gobernanza del riesgo cibernético de la organización, se deben considerar las siguientes actividades de gestión del riesgo cibernético, que se tratan a lo largo de esta guía:

- La identificación de activos y redes críticos, incluidos entornos de TI, OT y IIoT.
- Un análisis de amenazas a activos críticos y vulnerabilidades.
- Comprensión de las implicaciones de un incidente cibernético, incluidos los costos de pérdida o reemplazo.
- Determinar las tolerancias al riesgo.
- Una evaluación de las necesidades comerciales/operativas y los riesgos relacionados.
- La priorización de proyectos relacionados con la seguridad y crear un plan basado en su exposición al riesgo.
- Determinar dónde residen sus datos.
- Implementar un medio estandarizado para analizar, medir y reportar perfiles de riesgo.
- Definir un conjunto adecuado de medidas de mitigación de riesgos con revisión periódica.

3.5 Desarrollar una estrategia y un plan de gestión del riesgo cibernético

Desarrollar una estrategia y un plan de gestión de riesgos cibernéticos requiere tiempo y planificación, y su implementación requiere la participación del liderazgo ejecutivo, como se describe en la Sección 2. Es esencial que la estrategia de gestión de riesgos cibernéticos se alinee con la estrategia operativa general de la organización. Se deben considerar cuidadosamente los requisitos comerciales específicos respaldados por actividades administrativas y los objetivos de desempeño respaldados por entornos complejos habilitados para OT.

Una estrategia de ciberseguridad debe incluir objetivos para madurar las capacidades de ciberseguridad en todos los entornos operativos. El documento de estrategia debe tener un nivel suficientemente alto y flexible para adaptarse a los cambios tanto tecnológicos como de los actores de amenazas. Según sea necesario, los requisitos regulatorios deben reconocerse e incorporarse a la estrategia. Una vez establecida la estrategia, se puede implementar un programa de gestión de riesgos cibernéticos.

Un plan de ciberseguridad reconoce y aborda las amenazas y vulnerabilidades identificadas, como redes no segmentadas; riesgos de terceros no gestionados (por ejemplo, proveedores, buques atracados); riesgos planteados por amenazas internas; y las innumerables amenazas cibernéticas descritas en la Sección 6. El plan debe incorporar mecanismos de retroalimentación para ser efectivo, seguir siendo relevante y garantizar la sostenibilidad.

Para desarrollar la estrategia y el plan, la organización debe buscar comprender sus riesgos específicos mediante la aplicación de evaluaciones de riesgos (Sección 8).

Si bien no existe una única estrategia correcta de gestión de riesgos cibernéticos que se aplique uniformemente a todos los puertos e instalaciones portuarias, las consideraciones específicas incluyen:

- Identificar e incorporar controles de ciberseguridad desde un marco de ciberseguridad identificado, como los de la Organización Internacional de Normalización (ISO), el Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST) y la Sociedad Internacional de Automatización (ISA). Hay varios marcos disponibles que se pueden aprovechar para combinar controles de ciberseguridad para entornos portuarios complejos de TI, OT y IIoT y es importante que se incluya el liderazgo ejecutivo en el proceso de selección del marco.

- Adoptar un enfoque de defensa en profundidad, como el modelo de “tres líneas de defensa”.

3.5.1 Lograr una defensa en profundidad mediante el modelo de tres líneas de defensa

La defensa en profundidad aprovecha la implementación de múltiples capas de controles de seguridad en un entorno operativo en red que depende de los sistemas de TI. La defensa en profundidad se logra mediante la superposición de varios controles de seguridad de una manera que ofrece redundancia de seguridad. Estos controles cubren áreas distintas, incluidas las físicas (por ejemplo, seguridad perimetral, CCTV), técnicas (por ejemplo, hardware y software como cifrado, autenticación de dos factores) y administrativas (por ejemplo, políticas y procedimientos).

La primera línea de defensa es responsable de implementar los controles y medidas de seguridad basados en los principios y mejores prácticas de ciberseguridad descritos en el marco de gestión de riesgos adoptado por la organización. Por ejemplo, estos pueden incluir parámetros que los usuarios deben cumplir al configurar contraseñas. El Líder Designado de Ciberseguridad garantiza que los usuarios sigan los protocolos establecidos de acuerdo con la política de ciberseguridad.

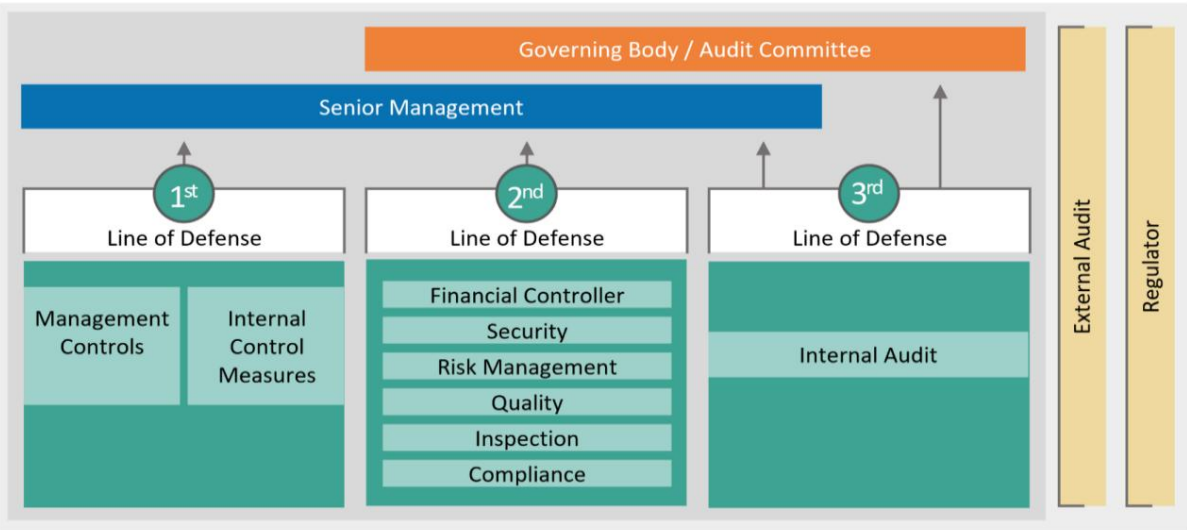

Figura 3 - Modelo ICAS 3LoD
La segunda línea de defensa

La segunda línea de defensa aprovecha las mejores prácticas que respaldan la gestión de riesgos y las actividades basadas en el cumplimiento. Estos tienen como objetivo desarrollar, facilitar y monitorear la efectividad de los controles de la primera línea de defensa. Si bien estas pueden variar según los puertos e instalaciones portuarias, una organización puede tener múltiples funciones de cumplimiento que abarcan la seguridad (por ejemplo, el Código PBIP), la confidencialidad de los datos (por ejemplo, el RGPD), las financieras (por ejemplo, PCI-DSS) y la cadena de suministro (por ejemplo, la OMA).

La tercera línea de defensa es el departamento de auditoría interna que puede comprobar con la 2ª línea dependiendo de las directrices (de acuerdo con la tolerancia al riesgo, etc.) y si estas son implementadas por la primera línea. Esta tercera línea puede ser opcional para organizaciones más pequeñas que carecen de un departamento de auditoría interna. Al adoptar este modelo, las áreas de responsabilidad de las partes interesadas pueden definirse claramente.

3.5.2 Estrategia de defensa en profundidad basada en un marco de confianza cero

Las mejores prácticas de defensa en profundidad se basan en el principio de crear múltiples capas de defensa para hacer más difícil que un atacante tenga éxito. Estas capas brindan múltiples oportunidades para que la organización proteja, detecte y responda a un ataque. Cuando una capa defensiva falla o es superada por un atacante, las capas restantes garantizan que la organización aún pueda detener el ataque. Por ejemplo, el firewall y el IDS/IPS perimetral proporcionan una capa de defensa para una organización, ya que el firewall prohíbe ciertos accesos y garantiza que se monitoree la comunicación. En caso de que un atacante

viola con éxito el firewall y el IDS/IPS, una segunda capa de defensa, como una capacidad de protección de endpoints, proporciona otro obstáculo que el atacante debe superar.

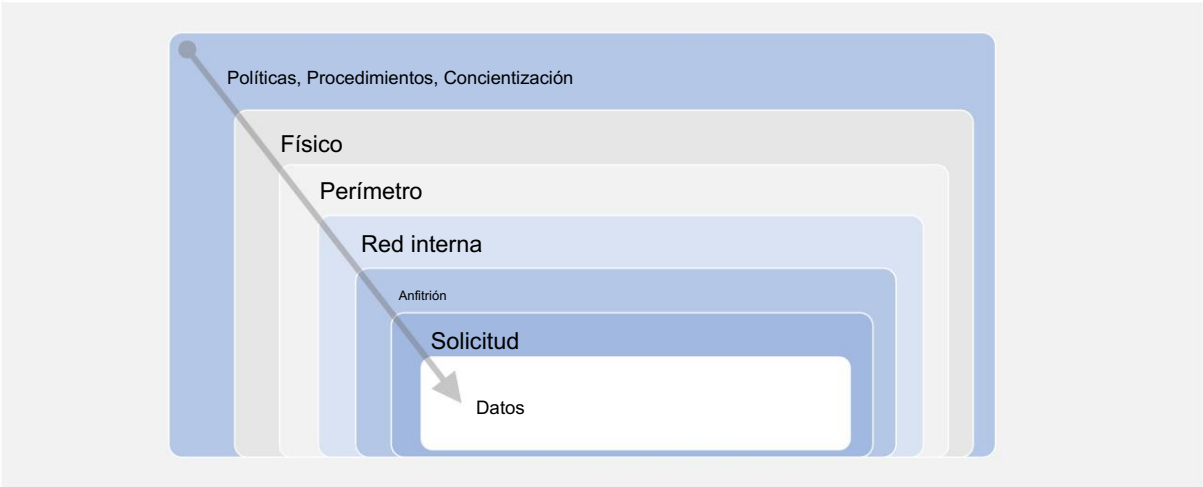

Figura 4 - Capas de defensa

3.6 Comprender la intersección “ciberfísica”

Los sistemas OT se definen como hardware y software que cambia, monitorea y controla directamente dispositivos físicos, equipos industriales, activos, procesos y eventos. Un ejemplo de OT es el Control de Supervisión y Adquisición de Datos (SCADA), que recopila y analiza datos en tiempo real con el fin de monitorear los sistemas de control en plantas, maquinaria y sistemas de infraestructura. Muchos sistemas OT dependen de controladores lógicos programables (PLC) que reciben datos de sensores, procesan datos y realizan tareas específicas basadas en protocolos predefinidos. Los Sistemas de Control Industrial (ICS), que frecuentemente son administrados por sistemas SCADA, representan otro tipo de OT que controlan y monitorean procesos, como los sistemas de cintas transportadoras. Cada vez más, los sistemas OT se conectan, gestionan y monitorean de forma remota a través de Internet y los sistemas IIoT también se conectan a estos.

redes. Cada vez con mayor frecuencia, las nuevas tecnologías ICS comparten protocolos TCP/IP comunes17 y permiten una conectividad cada vez mayor.

Los sistemas de TI se refieren a tecnologías basadas en computadora, que incluyen software, hardware, tecnologías de comunicaciones y servicios de procesamiento de información relacionados. Los sistemas de TI se han expandido al mundo de la OT al proporcionar al personal de los puertos y de las instalaciones portuarias información en tiempo real sobre el estado de las infraestructuras y los sistemas de OT. Lo que distingue a la OT de los sistemas de TI es que los dispositivos de OT controlan los sistemas físicos . Los sistemas de TI gestionan los sistemas que gestionan los datos.

En cuanto a la ciberseguridad, los sistemas OT y TI son diferentes
Los sistemas de OT y de TI son diferentes, especialmente en los resultados de los ataques. Un ciberataque exitoso contra un activo de TI, como un servidor de aplicaciones en una red administrativa, podría resultar en el robo de datos, mientras que un ataque a sistemas OT podría provocar lesiones o la muerte, daños al activo o daños al medio ambiente.

Un factor que impulsa tanto la evolución como la complejidad del riesgo cibernético para los puertos y las instalaciones portuarias es la convergencia y la conectividad entre los sistemas de TI (es decir, control de acceso, aplicaciones de planificación de recursos empresariales, etc.), sistemas de conocimiento de dominio (es decir, vídeo, RADAR, AIS, etc.) y sistemas OT (ICS, sistemas SCADA de almacenamiento y distribución de combustible, grúas pórtico, etc.). A medida que más y más puertos e instalaciones portuarias conectan sus sistemas OT a redes de TI y adoptan y emplean IoT/IIoT
tecnologías y, por implicación, a la red mundial más amplia, surgen nuevas vulnerabilidades que los actores de amenazas pueden explotar.

Históricamente, las plataformas y redes críticas para misiones específicas estaban segregadas y no conectadas físicamente. Esta segregación o separación ayudó a aislar los sistemas de control de las cambiantes amenazas cibernéticas. Se pensaba que los ciberatacantes no podrían cruzar esta división física hasta Stuxnet18.
Disipó el mito. A medida que más sistemas se habilitaron para la red, se conectaron redes de TI y OT que antes eran independientes, a menudo de forma ad hoc, sin tener en cuenta la seguridad. Hoy en día, a pesar de las mejores prácticas de segmentación de redes, muchas partes interesadas marítimas continúan conectando TI. redes habilitadas que soportan sistemas empresariales o de seguridad para controlar redes de sistemas utilizando diseños de red planos 19 .

Con el tiempo, los actores de las amenazas cibernéticas han capitalizado la convergencia TI-OT. Con el auge de la automatización plataformas en operaciones de carga, la tendencia continúa. Y con los sistemas de IoT, que con demasiada frecuencia se diseñan teniendo en cuenta poca o ninguna seguridad, se están sentando rápidamente las bases para un panorama de riesgos cibernéticos cada vez más complejo y dinámico para el que la mayoría de los puertos e instalaciones portuarias no están preparados.

Contextualizando la seguridad de TI frente a la de OT a través de la tríada de la CIA

17 TCP/IP (Protocolo de control de transmisión/Protocolo de Internet) es un estándar que define cómo los dispositivos (y por lo tanto los sistemas) y las aplicaciones transmiten datos entre ellos y permite el intercambio de comunicaciones a través de redes e Internet.

18 Lanzado en 2009, Stuxnet es un gusano informático que fue diseñado originalmente para atacar las instalaciones nucleares de Irán. El ataque original tuvo como objetivo los controladores lógicos programables (PLC) de Siemens utilizados para automatizar centrifugadoras que apoyaban el enriquecimiento de uranio. Cruzó el espacio de aire de las instalaciones a través de memorias USB y se propagó a través de computadoras con Microsoft Windows. Una vez que el gusano identificó el equipo objetivo, envió comandos que provocan daños al equipo electromecánico. Durante el ataque, el gusano envió información falsa al controlador principal, induciendo así a los ingenieros a una falsa sensación de seguridad mientras dañaba las centrífugas.

19 Grupo de Trabajo sobre Convergencia Física/Cibernética, “Informe final y recomendaciones del Consejo”, National Consejo Asesor de Infraestructura, 16 de enero de 2007, https://www.dhs.gov/xlibrary/assets/niac/niac_physicalcyberreport.pdf

Una forma de distinguir entre la seguridad basada en TI y la seguridad basada en OT es verla a través de la "lente" de la Tríada de la CIA. La CIA-Triad está diseñada para ofrecer información a una organización basada en datos confidencialidad, integridad y disponibilidad: efectivamente, el punto de referencia de TI. El punto de referencia OT, sin embargo, es control, disponibilidad, integridad y confidencialidad (CAIC). La principal diferencia entre la CIA y la CAIC es que esta última se centra más en la seguridad y el control que en la protección de datos.

Proteger los sistemas y redes OT requiere un sólido enfoque basado en el diseño CAIC. Al proteger los sistemas OT, los objetivos principales son garantizar la disponibilidad y la seguridad del sistema y que los controles del sistema funcionen correctamente y no estén sujetos a ataques cibernéticos. Las medidas de seguridad de OT deben incluirse en los procedimientos diarios de primera línea de defensa.

4. AMENAZAS Y CONSECUENCIAS CIBERNÉTICAS MARÍTIMAS

4.1 Comprender el panorama de las ciberamenazas del siglo XXI

Los puertos y las instalaciones portuarias desempeñan un papel central en el apoyo a las economías nacionales. Frente a la creciente complejidad de las cadenas de suministro del transporte marítimo, un factor clave para mantener la competitividad reside en las capacidades de la infraestructura de TI y OT de una organización marítima no solo para dar cabida a nuevos sistemas de automatización y TI, OT e IIoT, sino también para procesar procesos de rápido crecimiento. conjuntos de datos que permiten el movimiento de mercancías, pasajeros y barcos. Los sistemas, aplicaciones y datos deben mantenerse disponibles y mantenerse su integridad. Estos factores hacen que el sector marítimo sea atractivo para los actores de amenazas cibernéticas.

A medida que los puertos y las instalaciones portuarias adoptan la automatización habilitada por los sistemas de TI, OT y IIoT, que ofrecen ahorros mensurables y eficiencias operativas, están surgiendo nuevas vulnerabilidades que pueden ser explotadas por los actores de amenazas. Las actividades de procesamiento de datos se basan en gran medida en el intercambio electrónico de datos.
(EDI) y en muchos entornos se procesan a través de Port Community Systems (PCS). Dado que los volúmenes de transacciones de datos ascienden a millones, las organizaciones que buscan agilidad operativa aprovecharán cada vez más la adopción de soluciones analíticas de Big Data, automatización y tecnologías de inteligencia artificial (IA). Si se combinan estas capacidades con vehículos autónomos e inalámbricos y conectados en red, así como con sistemas de sensores habilitados para IoT/IIoT, la complejidad operativa se amplía, presentando oportunidades para que los actores de amenazas cibernéticas exploten vulnerabilidades o entornos poco seguros.

La gente de mar como vector de ciberamenaza

Los marineros modernos a menudo viajan hoy con múltiples dispositivos de TI personales (es decir, computadoras portátiles, tabletas y teléfonos). A menudo se conectan a una variedad de redes mientras realizan compras o se comunican con familiares y amigos durante el permiso en tierra en las áreas portuarias. De regreso a bordo, conectar estos sistemas a la red del barco puede introducir malware en el medio ambiente, incluso si simplemente se conecta para cargar el dispositivo. Incluso cuando la gente de mar adopta buenas prácticas de ciberseguridad, muchos pueden depender de sistemas operativos heredados que no han sido parcheados o actualizados adecuadamente, o que ya no cuentan con el soporte del fabricante. El uso de tales sistemas, incluido el uso casi endémico de dispositivos de almacenamiento móviles (por ejemplo, "memorias USB") en los buques, sirve como vector para que el malware acceda a los sistemas críticos de los buques y, a través de ellos, a los puertos mediante el intercambio de información o sistemas conectados. Los programas de educación y concientización sobre ciberseguridad son ahora un elemento crítico para que las empresas reduzcan los riesgos potenciales que los navegantes pueden representar, aunque tal vez sin querer, para los sistemas y datos críticos.

Figura 5: La gente de mar como vector de ciberamenaza

Los actores de amenazas cibernéticas que apuntan a múltiples sectores de infraestructura crítica, incluido el marítimo, no están limitados por la geografía o el idioma. Cualquier entorno de red, incluidos los que se encuentran en todos los puertos o instalaciones portuarias del mundo, podría ser vulnerable a ataques cibernéticos, compromisos y explotación.
Exclusivo de las operaciones portuarias, por ejemplo, los buques representan conductos potenciales de riesgo cibernético para los puertos que visitan, las empresas que los administran y la cadena de suministro que respaldan. Los barcos pueden ser riesgosos si sus entornos a bordo están ligeramente gobernados y tienen poca o ninguna supervisión. Cuando un barco está amarrado, puede introducir riesgos cibernéticos en una instalación portuaria a través de conexiones entre el barco y la costa.
La principal motivación de la mayoría de los actores de amenazas cibernéticas es el beneficio económico. La última tendencia es el uso cada vez mayor de ataques de ransomware propagados a través de correos electrónicos de phishing. Los ciberdelincuentes seguirán evolucionando

sus tácticas, técnicas y procedimientos (TTP) a lo largo del tiempo, lo que requiere que los profesionales de la ciberseguridad también ajusten sus tácticas defensivas, pero las motivaciones y objetivos de los ciberatacantes siguen siendo consistentes.

Otras motivaciones para los actores de amenazas incluyen la ideología (hacktivismo) y el ciberespionaje (actores-estado-nación). Las amenazas internas incluyen empleados potenciales que buscan tomar medidas contra una organización o un individuo. Una vez más, los TTP específicos utilizados por los atacantes evolucionan constantemente, con campañas y esfuerzos específicos que a veces duran un período de semanas e incluso años. La sección 8 describe cómo el intercambio de información sobre amenazas cibernéticas puede permitir a las organizaciones marítimas mantenerse al tanto de las últimas amenazas.

GRUPO	MOTIVACIONES	OBJETIVOS
Estados nacionales / Patrocinado por el estado Organizaciones (Persistente Avanzado Amenazas)	▪ Ganancia política ▪ Ganancia financiera ▪ Espionaje (incluido comercial e industrial) ▪ Ganancia comercial ▪ Contrabando	▪ Obtener datos, inteligencia e información ▪ Disrupción de las economías y crisis nacionales críticas. infraestructura ▪ Proporcionar ventajas a sus empresas comerciales nacionales en el mercado. ▪ Financiero/económico para compensar las sanciones
criminales	▪ Ganancia financiera ▪ Espionaje comercial/industrial ▪ Fraude ▪ Contrabando ▪ Soborno	▪ Vender datos robados ▪ Rescatar datos robados ▪ Operatividad del sistema de rescate ▪ Organizar transporte o contrabando fraudulento o ilegal de carga y/o personas ▪ Recopilar inteligencia para soluciones más sofisticadas delitos, ubicación exacta de la carga, planes de transporte y manipulación de buques, etc.
Insiders	▪ Venganza ▪ Involuntario	▪ Buscar venganza por el daño percibido ▪ Realizar funciones (riesgo de accidente)
Activistas	▪ Daño reputacional ▪ Interrupción de las operaciones	▪ Destrucción o cambio inadvertido de datos ▪ Publicación de datos sensibles ▪ Atención de los medios ▪ Denegación de servicio (DoS)
Oportunistas	▪ El desafío	▪ Superar las defensas de seguridad cibernética ▪ Autocumplimiento, aventura ▪ Ganancia financiera y reputacional
Terroristas	▪ Ideológico ▪ Político	▪ Interrupción o destrucción ▪ Atención de los medios ▪ Influir en las agendas políticas ▪ Ganancia financiera para apoyar sus actividades.

Figura 6 - Tipos de atacantes generales

Al evaluar el riesgo para su organización, los puertos y los líderes de las instalaciones portuarias deben tratar de identificar perfiles de actores de amenazas relevantes y anticipar sus motivaciones y objetivos. Esto permite mejorar la capacidad de desarrollar estrategias de ciberseguridad que puedan evolucionar para contrarrestar las tácticas empleadas por los actores de amenazas. Estas estrategias pueden respaldarse a través de mecanismos de intercambio de información descritos en la Sección 8.

4.2 Comprender los posibles impactos físicos de un ciberataque

Un ciberataque contra infraestructuras portuarias críticas representa un riesgo no sólo para las organizaciones responsables de dichos activos, sino también para sus socios, proveedores, clientes y todas las empresas e individuos potencialmente afectados. Los ataques ciberfísicos contra sistemas portuarios críticos podrían tener como objetivo sistemas de TI, OT y/o IIoT que administran o están conectados a una amplia gama de equipos, como sistemas operativos de terminales, grúas, sistemas de puertas, esclusas o puentes, sistemas de cámaras, sistemas de combustible. , sistemas de energía eléctrica, sistema de gestión de tráfico o cualquier otro sistema que soporte las operaciones portuarias diarias.

Desafíos que probablemente serán aprovechados por los actores de amenazas cibernéticas dirigidas a la industria marítima

- Costos laborales y escasez de habilidades. A medida que se acelera la digitalización en todo el sector marítimo, las habilidades necesarias para respaldar y proteger sistemas complejos aumentarán en valor y demanda. Puede surgir escasez de mano de obra, lo que presionará aún más a las organizaciones y brindará oportunidades para que los atacantes identifiquen sistemas inseguros.
- Debilidades en la arquitectura de seguridad IT/OT/IIoT. Las arquitecturas portuarias están evolucionando para soportar un mayor intercambio de datos digitales, particularmente para su uso en operaciones de la cadena de suministro en tiempo real. El monitoreo, la presentación de informes y los nuevos procesos comerciales portuarios, como el gemelo digital, requieren flujos de comunicación abiertos entre las tecnologías de TI, OT y IIoT. Como resultado, los diseños vulnerables pueden dar lugar a nuevas infracciones críticas.
- Desarrollo de software inseguro. Los atacantes seguirán explotando las vulnerabilidades del software, ya sea software comercial listo para usar (COTS) o desarrollado internamente. Esto podría deberse a vulnerabilidades de software comercial publicadas periódicamente o vulnerabilidades menos conocidas en software personalizado.
- Soporte indisciplinado del ciclo de vida/gestión de cambios. Desafortunadamente, cuando los sistemas clave son desconectado temporalmente para realizar mantenimiento o aplicar parches de seguridad, actualizaciones o mejoras, las operaciones se suspenden temporalmente, lo que afecta las operaciones portuarias. Como resultado, las actualizaciones a menudo se posponen, lo que deja a los sistemas críticos de TI/OT/IIoT vulnerables a ataques.
- Relaciones integradas de uno a muchos. El sector marítimo cuenta con el respaldo de una serie de aplicaciones de uso común. Por ejemplo, la expansión global de las Ventanillas Únicas Marítimas (RSU) puede potencialmente actuar como multiplicadores de fuerza para los actores de amenazas que buscan explotar el acceso a plataformas electrónicas integradas.

Figura 7: Desafíos que probablemente serán aprovechados por los actores de amenazas cibernéticas

Las consecuencias físicas de un ciberataque podrían ser de gran alcance y podrían afectar gravemente a la actividad portuaria y/o de las instalaciones portuarias, junto con sus cadenas de suministro dependientes, durante días o incluso semanas.

Aunque la integración de TI, OT y IIoT tiene buenas intenciones, un ciberataque contra sistemas integrados podría resultar en un incidente ambiental o de seguridad importante. Ejemplos de impactos de ataques físicos-cibernéticos incluyen:

- Un sistema de bloqueo comprometido podría resultar en un incidente de seguridad importante si los controles del nivel de agua no son adecuados. manipulado. Por ejemplo, drenar una cuenca de marea podría poner en peligro la presión del agua que mantiene el equilibrio de un muelle, lo que generaría problemas de seguridad y daños graves al puerto.
- Un puente podría maniobrarse cuando un barco o barcaza pasa por debajo de él, provocando una colisión.
- El mantenimiento no autorizado y/o no supervisado de equipos, sistemas o infraestructuras (por ejemplo, en tierra, grúas pórtico, carretillas pórtico, transportadores) podría generar vulnerabilidades que amenacen la seguridad o el medio ambiente.

- Las ayudas a la navegación podrían verse comprometidas (por ejemplo, alterando los colores de las señales) o dañadas, lo que podría afectar al tráfico y a la seguridad de los buques.
- Los sistemas RADAR y AIS podrían verse comprometidos, comprometiendo la información batimétrica y/o del canal de navegación, lo que podría provocar encallamientos de embarcaciones.
- Los controladores PLC comprometidos podrían provocar una sobrepresurización de la infraestructura de tuberías de líquidos a granel, lo que podría aumentar el riesgo de explosiones.
- Los sistemas de monitoreo de contenedores comprometidos (por ejemplo, Smart Container) pueden resultar en manipulación ilícita de datos, lo que puede dificultar el seguimiento de las ubicaciones de cargas peligrosas o el cambio de detalles de la carga, lo que resulta en un mayor riesgo para el medio ambiente y la seguridad o permite la liberación no autorizada de personas. carga, liberación de buques o transferencia intermodal de carga para facilitar las actividades de contrabando.

- Los archivos EDI comprometidos relacionados con los planes de carga podrían socavar las distribuciones de peso de los contenedores, lo que socavaría el equilibrio de carga de los barcos. Una carga inadecuada puede socavar la navegabilidad del buque, poniendo en riesgo el buque, el medio ambiente y la seguridad de la gente de mar.
- Los despachos aduaneros, de carga o de buques comprometidos podrían resultar en congestión portuaria y podrían comprometer la actividad de la cadena de suministro, lo que resultaría en pérdidas económicas locales, regionales y/o nacionales.

4.3 Comprender los posibles impactos no físicos de un ciberataque

Se pueden caracterizar ejemplos de impactos no físicos siguiendo el modelo de la Tríada de la CIA (Sección 3.3).

Confidencialidad

Los puertos y las instalaciones portuarias crean, procesan, reciben, administran, almacenan y transfieren grandes volúmenes de datos, que incluyen, entre otros, transacciones de pago, actividades de servicios, datos de manifiesto y detalles bancarios. Los actores de amenazas cibernéticas podrían utilizar cualquiera de estos datos para obtener ganancias ilícitas que podrían afectar a la organización:

- Reputación, mediante la divulgación pública de pruebas del ataque o de una variedad de información sensible.
- Competitividad, al vender información a un competidor.
- Cumplimiento normativo, en caso de que el atacante publique/venda parte/todos los datos y contengan información sensible, la organización podría ser declarada culpable de violar las leyes de privacidad, como, por ejemplo, el Reglamento General de Protección de Datos de la Unión Europea (GDPR).).

Integridad

La mayoría de los trámites de facturación se realizan de forma digital y automática. Un actor de amenaza cibernética podría alterar la información, lo que podría afectar al puerto o a la instalación portuaria:

- Ingresos
    - Cambiar datos para reducir los cargos a los clientes.
    - Cambio de datos para incrementar los pagos a proveedores.
    - Cambiar datos para transferir fondos a la cuenta bancaria del atacante.
    - Hacerse pasar por un ejecutivo de nivel C para dar órdenes a un empleado para transferir fondos a la cuenta bancaria del atacante.
- Cumplimiento normativo
    - Cambiar datos, como información de emisiones, para indicar un problema regulatorio o informes de formalidad falsos (aduanas, salud, agricultura, etc.).
- Seguridad
    - Alterar los datos de la cuenta para ocultar actividades no autorizadas o comprometer los sistemas.
    - Crear credenciales falsificadas o cuentas no autorizadas.

Disponibilidad

Al socavar la disponibilidad de datos o sistemas, los actores de amenazas cibernéticas pueden crear impactos como:

- Anular el cumplimiento de la Ventanilla Única Marítima Nacional (si los datos administrativos no pueden ser intercambiado).
- Retrasar o interrumpir el intercambio de datos operativos para coordinación de tráfico, carga u otros los procesos operativos.
- Retrasar los esfuerzos laborales relacionados con la información electrónica para estadísticas y análisis de datos para marketing, servicio al cliente u otras operaciones comerciales.
- Proporcionar datos históricos necesarios para las investigaciones de accidentes de embarcaciones.
- Retraso en la presentación de los documentos requeridos por los declarantes (autorizaciones, facturas…).
- Socavar la capacidad de las partes interesadas para procesar pedidos, rastrear carga, etc.
- Efectuar una interrupción operativa del servicio que resulte en un paro laboral.

5. EL CIBERECOSISTEMA DE LA ORGANIZACIÓN

5.1 Identificar, inventariar y clasificar actividades críticas y partes interesadas

Cada puerto e instalación portuaria es único. Uno de los desafíos clave que enfrentan los líderes en sus esfuerzos por gestionar su riesgo cibernético es la complejidad distintiva de las operaciones integradas de TI/OT/IIoT que es específica de sus procesos comerciales y portuarios industriales. Para gestionar el riesgo cibernético, los líderes de los puertos y de las instalaciones portuarias deben primero comprender cuáles son las actividades operativas más críticas y quiénes son las partes interesadas individuales que las respaldan.

5.1.1 Actividades críticas

Si bien la gama de actividades que ocurren en los puertos es diversa y única para cada entorno operativo, se puede identificar un conjunto común de actividades críticas. La infraestructura portuaria y de las instalaciones portuarias está compuesta por cualquier variación de edificios administrativos, infraestructura de carga y distribución de carga, almacenes, áreas e instalaciones de almacenamiento, tuberías de líquidos a granel y servicios públicos relacionados (agua, electricidad, etc.). Las autoridades portuarias a menudo confían la gestión de áreas específicas a operadores de terminales comerciales, que asumen la responsabilidad de supervisar, operar y mantener áreas específicas.
infraestructuras (grúas, silos, vallas específicas, instalaciones de control, terminales de pasajeros, etc.). Además,
Los puertos suelen proporcionar servicios clave, proporcionar controles de seguridad y facilitar las inspecciones de buques, mercancías, pasajeros y operaciones portuarias.

Además, los entornos PCS apoyan las operaciones portuarias integrando y racionalizando el intercambio de información y las actividades de coordinación de servicios críticos entre las entidades portuarias participantes.

Un puerto o instalación portuaria puede clasificar actividades clave por servicios básicos y sus infraestructuras de información críticas de apoyo, proporcionadas por:

- Actividades vinculadas al transporte marítimo y al transporte interior (contenedores, carga general, graneles líquidos o secos, etc.) con infraestructura y servicios dedicados para acomodar buques de carga y gestionar operaciones relacionadas (por ejemplo, descarga y carga, almacenamiento, inspección aduanera, controles sanitarios, etc.).

- Actividades relacionadas con el transporte de pasajeros y vehículos con infraestructura y servicios dedicados para acomodar pasajeros y vehículos a bordo de buques y operaciones relacionadas con los gestores (por ejemplo, puentes de pasajeros, estacionamiento, restaurantes y bares, control fronterizo, etc.). Esto también puede incluir buques Roll-on/ Roll-off (RoRo).
- Actividades relacionadas con la pesca con infraestructura y servicios dedicados para acomodar buques pesqueros y gestionar operaciones relacionadas (por ejemplo, descarga/carga de pescado, inspección de pescado, almacenamiento refrigerado de pescado, etc.).
- Actividades relacionadas con la coordinación del tráfico con infraestructura dedicada, equipos técnicos (cámara de videodetección, estación AIS, semáforo o señal, etc.) y servicios para garantizar una gestión segura del tráfico dentro del área portuaria en la vía navegable, así como en la infraestructura terrestre. .

- Actividades industriales cuyas operaciones están vinculadas a la logística portuaria, como plantas donde se encaminan productos desde la zona portuaria para su procesamiento (refinería, petroquímica, energía, etc.).
  Aunque estos sitios suelen estar designados como áreas restringidas, están cada vez más interconectados cibernéticamente.

5.1.2 Actores críticos

Después de identificar las actividades críticas en 5.1.1, los puertos y las instalaciones portuarias también deberían identificar las partes interesadas portuarias, marítimas e industriales críticas correspondientes. El panorama de partes interesadas involucradas en las actividades portuarias y los procesos comerciales (dependiendo del tamaño, alcance y complejidad del entorno operativo) puede ser extenso. Esto puede llegar a varios cientos o miles de procesos diferentes en los grandes puertos). Es crucial involucrar a todas las partes interesadas identificadas en la iniciativa de ciberseguridad, y estas pueden incluir:

- Transporte marítimo: navieras, armadores, gestoras de buques, tripulaciones. agencias de dotación, capitanes de barco.
- Proveedores de servicios portuarios: operadores de remolcadores, prácticos, linieros, recolectores de residuos, servicios de abastecimiento.
- Autoridades: administración marítima, aduanas, inmigración, policía, ejército, marina, guardacostas, autoridad sanitaria, autoridades de administración portuaria, agricultura, veterinaria, control estatal del puerto, estadísticas y administraciones comerciales.
- Cadena de suministro: agentes de carga, operadores de almacenes, transitarios, camioneros, operadores de trenes, operadores de barcazas.
- Industrial: sectores de automoción, energía, químico, petroquímico, aeronáutico, proveedores de energía como electricidad de alta tensión, petróleo/gas, agua industrial, vapor, empresas de tratamiento de residuos.

- Operadores de terminales: estibador, operadores de terminales de cruceros, operadores de terminales de líquidos y graneles, operadores de terminales químicos, ferries, roll on/roll of, operadores de clinker, operadores de referencia.
- Operadores de PCS: empresas gestoras de PCS.
- Actores intersectoriales: proveedores de servicios esenciales que apoyan a los actores portuarios primarios.

5.2 Identificar, inventariar y clasificar activos críticos

La complejidad y diversidad de los ecosistemas portuarios y de las instalaciones portuarias y la singularidad de cada puerto se reflejan en su implementación específica de sistemas IT/OT/IIoT. Para identificar con precisión las amenazas cibernéticas al ecosistema de un puerto o de una instalación portuaria, es esencial identificar los sistemas, activos e infraestructuras habilitados digitalmente del ecosistema. Las partes interesadas deben crear en colaboración un inventario de los sistemas portuarios clave, los flujos de datos y las interacciones con las dependencias del sistema externo identificadas para desarrollar una línea de base.20

Los sistemas operativos portuarios interactúan con una amplia gama de tecnologías automatizadas, como interfaz de máquina a máquina (vía EDI) y/o interfaces manuales (interfaces web, teléfonos inteligentes, correos electrónicos, papel o fax). Los datos intercambiados se pueden clasificar de la siguiente manera:

- Declaraciones obligatorias, como informes electrónicos que las compañías navieras, transitarios u otras partes interesadas deben presentar a las autoridades portuarias u otras autoridades, de conformidad con las regulaciones nacionales e internacionales.
- Control y autorización otorgada por las autoridades a los actores comerciales tales como autorizaciones de operaciones portuarias, de embarcaciones, de mercancías, despachos aduaneros o de manipulación de carga.
- Datos operativos relacionados con servicios y procesos portuarios tales como remolcadores, servicios de amarre o practicaje, abastecimiento de combustible, servicios de recolección de desechos y programación de fletes.
- Datos financieros y comerciales, como facturación, procesamiento de pagos, estadísticas.

20 En el contexto de las comunidades portuarias, las partes interesadas pueden acordar identificar de manera colaborativa servicios clave sin proporcionar detalles específicos de activos o sistemas.

- Datos de navegación y gestión del tráfico, como posición GPS de embarcaciones en zona portuaria, datos AIS, datos GNSS, herramientas de navegación (faro electrónico, sistema de monitoreo de tráfico, automatización de sistemas de esclusas y puentes).

Las actividades portuarias se pueden identificar según los siguientes servicios:

- Los servicios de navegación (en particular la navegación electrónica) apoyan el intercambio de datos relacionados con la navegación electrónica utilizando sistemas AIS, GNSS y radar, o incluso radiotelecomunicaciones. Los sistemas de navegación se utilizan cada vez más para la planificación de la llegada de buques y la optimización de las operaciones portuarias.
- Los servicios de atraque de buques se basan en el intercambio de datos entre buques (comerciantes, de pasajeros, pesqueros) en el mar, el tráfico dentro del puerto a través de sistemas PCS y VTS y las interfaces buque-tierra.
- Los servicios de intercambio de información sobre carga intercambian datos entre el puerto y la instalación que almacena y almacenamiento de mercancías.
- Los servicios de distribución y transferencia proporcionan interconexión con actores logísticos e industriales, asegurando la conectividad de los intercambios de datos con actores multimodales (vías navegables interiores, ferrocarril, carreteras), controles de mercancías o pasajeros. Estas cadenas de intercambio son clave para la eficiencia de los servicios de entrega previos y posteriores al enrutamiento. Estos cubren una gran cantidad de interfaces.
- Los intercambios de datos con autoridades competentes, Ventanilla Única Marítima, servicios de salud, control fronterizo, servicios fotosanitarios a nivel nacional e internacional, incluidos los documentos administrativos requeridos por la OMI y otras autoridades pertinentes, deben realizarse electrónicamente de acuerdo con la normativa establecida. Este intercambio de datos se intensificará en los próximos años. ▪ Los servicios de carga y descarga de buques implican el intercambio de datos vinculados a los servicios de carga. Estos intercambios, a menudo muy automatizados, son posibles mediante sistemas operativos de terminal (TOS) o PCS.

- Los servicios de apoyo también pueden incluir a las partes interesadas responsables del puerto y la infraestructura. Servicios de mantenimiento.
- Los servicios de seguridad y vigilancia involucran datos relacionados con la protección perimetral y las capacidades de vigilancia, que a menudo involucran tecnologías de video, control de acceso y teledetección, pero también las herramientas que permiten el monitoreo remoto, así como garantizar la seguridad del puerto y las operaciones.

Como paso siguiente, los líderes de puertos e instalaciones portuarias deben identificar todos los sistemas críticos de terceros para comprender completamente su ecosistema operativo y determinar sus objetivos de resiliencia en materia de ciberseguridad. Estos se pueden organizar según las siguientes líneas:

- Sistemas utilizados por las partes interesadas marítimas (gente de mar, consignatarios, capitanes y tripulación del barco, etc.).
- Sistemas utilizados por otros actores del transporte para compartir información sobre carga o pasajeros y permitir el transbordo (transporte por vías navegables, empresas de carreteras, empresas ferroviarias, etc.).

- Sistemas utilizados por las autoridades a nivel local, nacional o regional.
- Sistemas utilizados para vigilancia vía satélite y marítima.

Para terminar, los ciberecosistemas portuarios y de las instalaciones portuarias son dinámicos y sus partes interesadas son altamente interdependientes. Por lo tanto, se recomienda revisar periódicamente el ecosistema y sus actividades críticas, y realizar los ajustes apropiados, para ofrecer una mejor resiliencia a los ciberataques y de manera transversal en todos los procesos comerciales del puerto.

6. EVALUACIÓN DE RIESGOS Y VULNERABILIDADES

6.1 Evaluación de vulnerabilidades

El propósito de una evaluación de la vulnerabilidad de la ciberseguridad es identificar y evaluar las vulnerabilidades de la ciberseguridad dentro del complejo entorno operativo de un puerto o instalación portuaria.
La evaluación de la vulnerabilidad requiere aportes de todas las partes interesadas críticas e incluye la identificación de opciones de mitigación prioritarias en las que la organización podría invertir.

Las evaluaciones de vulnerabilidad de la ciberseguridad no son uniformes, pero la mayoría incluye un conjunto similar de actividades, tales como: identificación de activos; clasificar el valor y la importancia de los activos; definir las vulnerabilidades de los activos; e implementar tácticas de mitigación basadas en riesgos. Los puertos y los entornos de las instalaciones portuarias frecuentemente implican algunos grados de integración, por lo que se deben identificar y revisar los sistemas de TI/OT/IIoT. Además, como las vulnerabilidades en un área funcional podrían, si se ven comprometidas, poner en peligro otra área, se deben identificar todos los datos, conexiones de red y sistemas y procesos OT habilitados por TI. Por ejemplo, las redes no segmentadas, la falta de software antivirus actualizado, los sistemas mal configurados y la falta de disciplina en materia de contraseñas representan vulnerabilidades comunes a los puertos y a las instalaciones portuarias.

6.2 Evaluación del impacto

El impacto se refiere al daño potencial que una amenaza cibernética podría causar a un puerto o instalación portuaria. El impacto se basa en los criterios clave que afectan las funciones u operaciones comerciales de la organización, la seguridad de las instalaciones, la seguridad del personal y el riesgo ambiental. El análisis de escenarios de pérdidas (Sección 2.1.2) respalda esta actividad. Por ejemplo, en 2017, el ataque NotPetya interrumpió las operaciones de AP Moller-Maersk, lo que provocó pérdidas reportadas de alrededor de 300 millones de dólares (sección 3.1).

6.3 Evaluar el riesgo

El objetivo principal de una evaluación de riesgos de ciberseguridad es que el puerto o la instalación portuaria obtenga información sobre los riesgos cibernéticos para sus operaciones. El riesgo puede definirse generalmente como una medida del grado en que un puerto o una instalación portuaria se ve amenazado por una circunstancia o evento potencial, y generalmente se deriva de los impactos adversos que surgirían si ocurriera una circunstancia o evento; y la probabilidad de que eso ocurra.

Por ejemplo, el NIST CSF21 proporciona un marco sobre cómo un puerto o una instalación portuaria podría lograr esto:

- Identifique y documente las vulnerabilidades de los activos, así como las amenazas internas y externas.
- Adquirir información sobre amenazas y vulnerabilidades de fuentes externas.
- Identificar y analizar el impacto empresarial; determinar la probabilidad de factores de riesgo revisando las amenazas, las vulnerabilidades y la probabilidad de sus impactos.
- Definir y priorizar las actividades de respuesta a riesgos.

Los riesgos de ciberseguridad son aquellos riesgos derivados de la pérdida de confidencialidad, integridad o disponibilidad de la información, como la pérdida de datos relacionados con manifiestos de carga, declaraciones de mercancías peligrosas o datos procesados por sistemas informáticos (Sección 3.3), y que podrían generar efectos adversos. impactos a un puerto o puerto

21 Marco del Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. para mejorar la ciberseguridad de infraestructuras críticas (Versión 1.1), también conocido comúnmente como “NIST CSF”.

operaciones de la instalación (por ejemplo, operaciones de carga, programación) o activos, individuos, terceros clave o incluso infraestructura nacional crítica. 22

Las evaluaciones de riesgos identifican y cuantifican los riesgos aplicables al entorno operativo del puerto o de la instalación portuaria. Los pasos clave en una evaluación de riesgos son la identificación de riesgos, el análisis de riesgos y la evaluación de riesgos.

6.4 Identificación de riesgos

6.4.1 Identificación de activos

Para identificar el riesgo, un puerto o instalación portuaria debe identificar sus activos y amenazas clave y crear escenarios de riesgo. en busca de formas en que amenazas potenciales podrían afectar sus activos.

La visibilidad de los activos es fundamental para garantizar que los dispositivos no autorizados no estén conectados al entorno de red de un puerto o de una instalación portuaria y permite a las partes interesadas distinguir entre activos, sistemas, plataformas y equipos autorizados y no autorizados. Un puerto o instalación portuaria debe establecer y mantener una lista de activos y sistemas físicos y lógicos que estén autorizados para conectarse al entorno de red, incluidos todos los equipos, sistemas y aplicaciones de TI/OT/lioT. Además, algunos de los activos pueden estar ubicados en varios lugares del puerto que no son fáciles de monitorear.

Además, también deberían implementarse medidas de protección física y vigilancia para evitar el acceso no autorizado.

Los equipos críticos son equipos o sistemas cuya falla directa conducirá a una situación potencialmente peligrosa o un accidente, causando potencialmente lesiones, pérdida de vidas o daños a la propiedad o al medio ambiente marino. Se deben identificar todas las dependencias de equipos críticos (por ejemplo, servicios de terceros prestados para respaldar el equipo) relacionadas con la seguridad operativa, la salud y la protección ambiental, junto con el impacto en las operaciones y el negocio. Ejemplos de sistemas críticos habilitados para TI/OT/IIoT podrían incluir sistemas de declaración de mercancías peligrosas, sistemas de recepción y manipulación de carga, sistemas de gestión de la cadena de suministro, sistemas de despacho de aduanas y/u operaciones en puertos deportivos.

Haciendo referencia a los inventarios de activos, la organización también debe desarrollar diagramas de arquitectura de red y flujo de datos. Dichos diagramas pueden ayudar a las partes interesadas a identificar posibles puntos de acceso que los atacantes podrían explotar para obtener acceso a activos primarios y secundarios, y también deben indicar puntos de conexión a otras redes y/o Internet.

6.4.2 Entender los datos como un activo

Los líderes de puertos e instalaciones portuarias deben reconocer que los datos que sus organizaciones generan, procesan, transmiten y almacenan son activos que vale la pena proteger. Los ejecutivos de puertos e instalaciones portuarias deben recordar que siempre que se procesan o transmiten datos, son vulnerables. Los datos confidenciales incluyen registros de clientes, instrucciones de envío, manifiestos, conocimientos de embarque, información bancaria, información de contacto y dirección e historiales de compras. También incluye información logística clave, como características de la carga, datos de carga de buques, manifiestos de pasajeros, notificaciones de inspección aduanera e información de recaudación y desembolso de impuestos nacionales, etc.

---

22 NIST SP 800-53 (Revisión 4); Ver también: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, y Guía para evaluaciones de riesgos de ciberseguridad para infraestructuras de información crítica, CSA Singapur (diciembre de 2019) https://www.csa.gov.sg//media/Csa/Documents/Legislation_Supplementary_References/Guide-a-Realización-de-Evaluación-de-Riesgos-de-Ciberseguridad-para-CII---Feb-2021.pdf

Aunque no todos los empleados pueden tener acceso a los datos de la organización, el robo de datos puede afectar a individuos específicamente, así como a la organización en general. La pérdida de datos23 de los empleados puede resultar en violaciones de la privacidad, fraude financiero y/o daño emocional a un individuo. El robo o la manipulación de datos comerciales pueden provocar pérdidas financieras derivadas del fraude.

Para identificar y priorizar activos de datos clave, los ejecutivos y las partes interesadas clave deben colaborar para responder las siguientes preguntas:

- ¿Qué datos son más críticos para las operaciones de mi organización? ¿Qué es no crítico?
- ¿Qué datos son más valiosos y para quién son valiosos?
- ¿Cómo se gestionan los datos de mi organización? ¿Quién tiene acceso a qué datos?
- ¿Cómo se protegen los datos de mi organización? ¿Cómo se realiza una copia de seguridad?
- ¿Puede mi organización recuperarse de un ataque si todos los datos se perdieron y son irrecuperables? Y cómo ¿rápido?

6.4.3 Evaluación de amenazas

Las evaluaciones de riesgos y amenazas están diseñadas para identificar qué activos, sistemas, operaciones y procesos requieren protección. Determinan su valor, junto con las consecuencias de la perturbación; También identifican amenazas y vulnerabilidades que los afectan, así como acciones de mitigación. Un evento de amenaza es cuando un agente de amenaza actúa contra un activo y potencialmente podría resultar en daño a ese activo. Para determinar posibles eventos de amenazas que podrían explotar las vulnerabilidades de los activos, fuentes de terceros (por ejemplo, proveedores de información sobre amenazas cibernéticas) pueden ayudar a identificar amenazas a los puertos y las instalaciones portuarias. Estos eventos de amenaza se pueden aplicar a cada activo que presente un punto de entrada por vector de ataque al sistema. Los eventos de amenazas aplicables que afectan los activos están documentados. Las etapas de ataque de los actores de amenazas cibernéticas también pueden incorporarse a dicho análisis24.

6.4.4 Crear escenarios de riesgo

De acuerdo con el análisis de escenarios de pérdidas (Sección 2.1.2), el propósito de desarrollar análisis de riesgo precisos escenarios es detallar cómo una amenaza cibernética podría afectar los activos críticos de un puerto o instalación portuaria y Proporcionar un análisis de riesgo razonable basado en el contexto operativo, la complejidad del sistema y las amenazas potenciales. Los escenarios de riesgo también pueden facilitar la comunicación con las partes interesadas y el análisis sistemático de factores de riesgo clave.

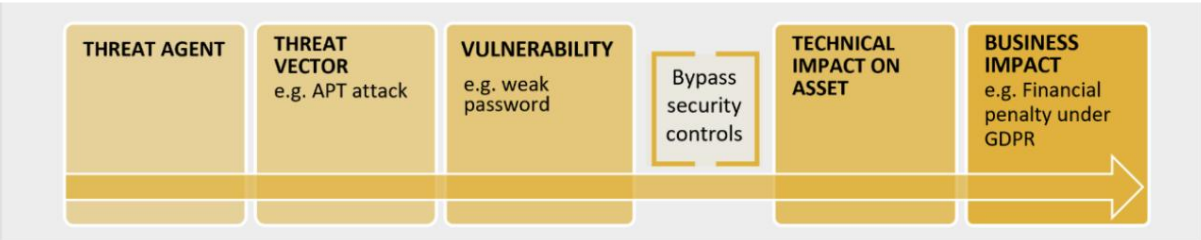

Figura 8 - Diseño del escenario de riesgo

23 También conocida como Información de Identificación Personal o “PII”.

24 Los ejemplos incluyen los modelos Cyber Kill Chain® y MITRE ATT&CK de Lockheed Martin .

6.4.5 Análisis de riesgos

El análisis de riesgos evalúa la probabilidad de que ocurra un escenario de riesgo y sus posibles consecuencias (es decir, impacto). Utilizando la metodología de análisis de escenarios de pérdidas detallada en la Sección 2.1.2, los puertos y las instalaciones portuarias deben considerar los siguientes parámetros al determinar la probabilidad de riesgo:

- Explotabilidad – Caracteriza el grado de dificultad de explotar la vulnerabilidad de un activo.
  Esto afecta a factores como la sofisticación de las herramientas, las habilidades técnicas para ejecutar el ataque, los derechos de control de acceso, los controles de seguridad vigentes, etc.
- Descubrimiento: caracteriza el grado de dificultad para descubrir la vulnerabilidad de un activo, que podría estimarse en función de la exposición del activo (por ejemplo, a través de Internet).
  conectividad) y si la información sobre vulnerabilidad está fácilmente disponible.
- Reproducibilidad: se refiere al grado de dificultad de recrear la vulnerabilidad para comprometer un activo. Dependiendo de las medidas de defensa de una organización (por ejemplo, monitoreo y detección), un actor de amenazas cibernéticas puede necesitar diseñar exploits de diversa complejidad.
  objetivo de un activo y las condiciones operativas existentes.

Al aplicar este enfoque, un evaluador de riesgos podría asignar un esquema de puntuación a cualquiera de los factores anteriores (por ejemplo, entre 1 y 5) y luego calcular una puntuación promedio. La puntuación resultante caracteriza la probabilidad del escenario de riesgo.

La realización de cualquiera de los escenarios de riesgo podría interrumpir las operaciones comerciales de un puerto o instalación portuaria, dañar su reputación o provocar pérdidas financieras. Para determinar mejor el impacto del riesgo, los puertos y las instalaciones portuarias deberían considerar desarrollar una tabla de evaluación con descriptores específicos de la organización (por ejemplo, objetivos comerciales o métricas de desempeño) para la calificación del impacto y luego asignar una puntuación de impacto. Luego se pueden aplicar calificaciones de impacto a cada escenario de riesgo para medir el riesgo de confidencialidad, integridad y disponibilidad.

6.5 Evaluación de riesgos

Una vez que se desarrolla un escenario de riesgo, el puerto y las instalaciones portuarias deben determinar la importancia del escenario de riesgo. priorizando y documentando el riesgo. Las priorizaciones de riesgos se derivan de los resultados del análisis de probabilidad e impacto, y las consecuencias de las infracciones cibernéticas se pueden asignar a una matriz de riesgos.

LEVEL OF PROBABILITY	LEVEL OF CONSEQUENCE				
	1	2	3	4	5
A: Highly Likely	MEDIUM	HIGH	VERY HIGH	CRITICAL	CRITICAL
B: Probable	MEDIUM	HIGH	VERY HIGH	CRITICAL	CRITICAL
C: Possible	LOW	MEDIUM	HIGH	VERY HIGH	VERY HIGH
D: Improbable	LOW	LOW	MEDIUM	HIGH	HIGH
E: Unlikely	LOW	LOW	LOW	MEDIUM	MEDIUM
	1: Insignificant	2: Minor	3: Moderate	4: Major	5: Catastrophic

Figura 9 - Matriz de riesgo para determinar el nivel de riesgo para el escenario de riesgo individual

Todos los resultados de la evaluación de riesgos deben documentarse en un Registro de Riesgos que relacione los escenarios de riesgo con los niveles de riesgo. El Registro de Riesgos ayuda a la comunicación con las partes interesadas y debe mantenerse y revisarse periódicamente para garantizar que el liderazgo esté consciente de los riesgos cibernéticos relevantes. Los elementos del Registro de Riesgos incluyen:

- Escenario de riesgo: un escenario que describe cómo un actor de amenaza cibernética podría explotar con éxito una vulnerabilidad potencial para acceder a un activo que podría tener como resultado un impacto debilitante.
- Fecha de identificación – La fecha de identificación del escenario de riesgo.
- Controles y procesos existentes: controles y/o procesos necesarios para mitigar un riesgo. guión.
- Riesgo inicial: el nivel de riesgo (es decir, función de probabilidad e impacto) del escenario de riesgo individual después de la evaluación de los controles y procesos existentes.
- Riesgo residual: exposición al riesgo que permanece después de la implementación de medidas de mitigación. control S.
- Plan de tratamiento: las acciones (por ejemplo, implementación de nuevos controles y procesos) y el cronograma requerido para reducir el riesgo grave a un nivel considerado tolerable para el liderazgo de un puerto o instalación portuaria.

6.6 Tolerancia al riesgo

La tolerancia al riesgo se refiere al nivel de asunción de riesgos aceptable para lograr objetivos comerciales específicos, y las determinaciones de tolerancia al riesgo permiten a los ejecutivos identificar límites de riesgo aceptables. Al definir la tolerancia al riesgo, se deben definir los objetivos de desempeño, identificar las opciones de mitigación y establecer los umbrales de aceptación del riesgo. Los riesgos específicos deben compararse con el riesgo definido
umbrales de tolerancia. Se debe priorizar el tratamiento de los escenarios de riesgo con clasificaciones de riesgo que excedan los umbrales de tolerancia definidos hasta que dichos riesgos caigan dentro de los límites de tolerancia aceptables. Se deben definir plazos para el tratamiento de riesgos. La Figura 10 destaca cómo los líderes de puertos e instalaciones portuarias pueden abordar las determinaciones de tolerancia al riesgo.

RISK RATING	RISK TOLERANCE AND RESPONSE
CRITICAL (Avoid)	Critical risks should be avoided. They should be prioritized for immediate treatment. Otherwise, update business continuity plans / develop work around solutions.
VERY HIGH (Transfer)	Treat risks at this level within three months, following completion of critical risk treatment treated. Otherwise, consider transferring via insurance.
HIGH (Mitigated)	Risks in this level should be treated in the short term (within 12 months).
MEDIUM (Mitigated)	Treat risks in this level opportunistically (e.g. at the next system refresh; introduction of new technologies). Future analysis will assess viability and need for upgrades.
LOW (Accepted)	Risks in this level can be accepted and monitored, or when deployment of additional countermeasures and/or mitigation controls is not deemed as cost -effective.

Figura 10 - Muestra de tolerancia al riesgo

7. MEDIDAS DE PROTECCIÓN, DETECCIÓN Y MITIGACIÓN

Los puertos y las instalaciones portuarias a través de la brecha digital deben adoptar un enfoque holístico para gestionar su riesgo cibernético, como se describe en la Sección 3. Dado que es imposible lograr una seguridad perfecta, establecer la capacidad de proteger activos e información críticos, identificar amenazas, detectar infracciones e iniciar Es fundamental adoptar contramedidas adecuadas en una acción de respuesta coordinada. Desafortunadamente, las capacidades de detección de intrusos han sido durante mucho tiempo un área que ha sufrido una inversión insuficiente. Por ejemplo, una organización promedio tarda 280 días en detectar una brecha de ciberseguridad e iniciar el proceso de mitigación.25

Para desarrollar medidas efectivas de ciberseguridad, el puerto o instalación portuaria debería:

- Identificar todos los activos críticos, dependencias relevantes y diagramas de flujo de datos y redes (Sección 6.4). Los inventarios de activos y los diagramas de flujo de datos y redes brindan a las partes interesadas información clave relacionada con todas las aplicaciones y sistemas, equipos e infraestructura habilitados para TI, OT y IIoT, así como los activos digitales (datos) que requieren protección.
- Identificar, evaluar y priorizar todas las vulnerabilidades de ciberseguridad que deben abordarse para mitigación (Sección 6).
- Identificar, caracterizar y revisar periódicamente todas las amenazas a la ciberseguridad de la organización, evaluando cómo cada una podría impactar las operaciones de la organización (Sección 4).
- Identificar un marco de seguridad apropiado para adaptarlo al entorno operativo específico de la organización26. Las medidas de seguridad deben estructurarse para impulsar un proceso de mejora continua (Sección 11) que debe mantenerse para gestionar el riesgo cibernético organizacional dentro de tolerancias de riesgo aceptables. ▪ Comprender cómo se pueden aprovechar diversos marcos de análisis

de amenazas cibernéticas para comprender cómo se pueden aprovechar los ataques y los indicadores de compromiso (IOC) para ayudar a proteger, detectar y responder a los ataques cibernéticos.

7.1 Medidas de protección

La identificación de activos críticos, datos, diagramas, dependencias y amenazas informará el alcance, alcance, estrategias y profundidad de las medidas de protección apropiadas.

La mayoría de las partes interesadas en puertos e instalaciones portuarias a ambos lados de la brecha digital con frecuencia asumirán que se puede confiar en las cuentas, las aplicaciones y los sistemas integrados de TI, OT y IIoT. Si bien estas percepciones continúan persistiendo, la creciente interconexión y la adopción acelerada de servicios en la nube conspiran para desdibujar los límites entre los derechos y privilegios de acceso externos e internos.
Desafortunadamente, las debilidades que inevitablemente surgen de las relaciones de confianza a menudo son explotadas por los actores de amenazas cibernéticas después de obtener la entrada inicial al entorno operativo de red confiable de la organización. Esto permite que lo que sería un problema relativamente pequeño se propague rápidamente.

25 Véase: https://www.ibm.com/security/data-breach

26 Los recursos disponibles que ofrecen orientación sobre medidas de protección se pueden obtener de ENISA, NIST e ISO.

Debería abandonarse el concepto de "red confiable" dentro del perímetro de un puerto o instalación portuaria en favor de la adopción del concepto de "confianza cero". Esto se debe a las complejidades de las operaciones marítimas modernas que requieren una amplia gama de conexiones internas y externas (usuarios, socios, vendedores, clientes, proveedores, etc.). En su forma más simple, el concepto de confianza cero significa que no se debe confiar en ningún usuario, dispositivo o aplicación sin verificación, independientemente de si el usuario, dispositivo o aplicación reside dentro o fuera del entorno de red de la organización.

Además, los ejecutivos de puertos e instalaciones portuarias pueden proteger su organización contra actores de amenazas cibernéticas considerando el empleo de medidas de seguridad dentro del contexto de las siguientes categorías:

- Organización : se debe organizar un equipo de seguridad interno (o contratar servicios de terceros) para anclar las medidas de ciberseguridad del puerto o de la instalación portuaria. Responsabilidades claras y se deben definir y asignar responsabilidades. Además de identificar al personal clave para supervisar la ciberseguridad (Sección 2), se debe identificar claramente a todos los propietarios de activos digitales críticos, así como a los propietarios de los riesgos cibernéticos.
- Procesos : utilizando las medidas básicas de ciberseguridad descritas en estas directrices, las partes interesadas del puerto y de las instalaciones portuarias deben integrar medidas de control de ciberseguridad en procesos específicos de la organización que también respalden los objetivos de desempeño definidos. Los ejemplos incluyen incorporar requisitos de seguridad con actividades de gestión de riesgos basadas en el cumplimiento, políticas de gestión de riesgos empresariales y contratos con proveedores. Las revisiones de los acuerdos con proveedores deben realizarse con un enfoque específico en las cláusulas de ciberseguridad (por ejemplo, requisitos de notificación de incumplimiento).

- Personas : si bien las personas representan el eslabón más débil del programa de ciberseguridad de un puerto o instalación portuaria, también representan la primera línea de defensa. Por lo tanto, se deben establecer medidas de protección para todo el personal al que se le concedan derechos de acceso a activos, sistemas y/o infraestructuras digitales. Estos incluyen verificaciones de antecedentes previas al empleo, capacitación inicial en concientización sobre ciberseguridad (Sección 9), definición de compromisos de ciberseguridad durante el proceso de incorporación y actividades periódicas de capacitación en concientización sobre ciberseguridad (por ejemplo, phishing). Se deben emplear prácticas de desaprovisionamiento durante el proceso de baja. Cuando se producen cambios de personal, los permisos de acceso físico y lógico deben revisarse y/o retirarse (y coordinarse entre las partes interesadas de TI y seguridad) de manera oportuna para evitar la acumulación de credenciales y prevenir la posibilidad de acceso no deseado.

- Tecnología – Las medidas tecnológicas representan la mayor parte de las medidas de protección e incluyen control de acceso, monitoreo de redes, comunicación y protecciones para sistemas, equipos, datos, aplicaciones e infraestructuras en red. Las medidas tecnológicas están destinadas a bloquear el acceso no autorizado y el tráfico de datos (control de acceso), prevenir ataques y malware, y proteger los sistemas y los datos para que no se vean comprometidos o se pierdan.

ÁREA	EJEMPLOS
Control de acceso	▪ Gestión de identidad y acceso. ▪ Gestión de cuentas privilegiadas ▪ Acceso basado en roles y privilegios mínimos ▪ Convenciones de contraseña ▪ Autenticación multifactor ▪ Revisiones periódicas de cuentas y derechos de acceso.
punto final y Red Seguridad	▪ Segmentación de la red (por ejemplo, separación de las redes operativas y administrativas de la TI de la oficina) ▪ Firewalls (tradicional y Firewall de Aplicaciones Web – WAF) ▪ Aislamiento de sistemas críticos o vulnerables ▪ Acceso remoto, VPN

	▪ Control de acceso a la red (NAC) ▪ Protección contra malware ▪ Refuerzo del sistema
Seguridad de datos	▪ Cifrado para proteger datos en sistemas portuarios/instalaciones portuarias, en reposo, en tránsito y en uso. ▪ Clasificación de datos. ▪ Controles de medios extraíbles ▪ Eliminación de equipos, incluida la destrucción de datos. ▪ Usar mecanismos de verificación de integridad para verificar el software y el firmware. ▪ Prevención/protección de fuga de datos – DLP
Operacional Seguridad	▪ Gestión de cambios y actualizaciones ▪ Gestión de parches ▪ Separación de funciones ▪ Gestión de vulnerabilidades ▪ Prevención de fraude ▪ Fortalecimiento del sistema ▪ Ciberinteligencia

Figura 11 - Ejemplo de medidas de protección

Medidas de protección física

La protección contra amenazas físicas, como el acceso no autorizado, el sabotaje o el espionaje de la información, se logra mediante el empleo de medidas de seguridad física adecuadas. Los sistemas de seguridad física y sus prácticas de apoyo a menudo quedan relegados a prácticas y procedimientos de gestión tradicionales destinados a cumplir con estándares internacionales, como el Código PBIP de la OMI. A nivel organizacional, las partes interesadas en ciberseguridad y seguridad física deben colaborar y comunicarse periódicamente. Por ejemplo, los informes de actividades sospechosas deben compartirse, notificando a ambos grupos de partes interesadas sobre posibles eventos que podrían afectar una o ambas áreas de responsabilidad.

Las capacidades de seguridad física permiten la ciberseguridad, por ejemplo, al controlar el acceso a los sistemas OT y a los equipos e infraestructuras habilitados para redes que frecuentemente residen en áreas restringidas.
Dichos sistemas y componentes también suelen depender de redes habilitadas para TI, que también pueden incluir puntos de integración que conectan TI, OT y IIoT y plataformas de automatización que a menudo pueden verse fácilmente comprometidas, lo que resulta en efectos catastróficos en la seguridad portuaria (Sección 3.7).

7.2 Medidas de detección

Las medidas de detección son fundamentales para determinar cuándo han fallado las medidas de protección, y hay varias formas en que las partes interesadas del puerto y de las instalaciones portuarias pueden determinar si ha ocurrido un evento o si se está produciendo un ataque cibernético. El más obvio es cuando un activo o sistema deja de funcionar, como en el caso de un ataque de ransomware. En otros casos, un activo o sistema puede exhibir comportamientos inusuales o irregulares. Sin embargo, lo más preocupante son los ataques que no arrojan resultados inmediatos u obvios y que a menudo pasan desapercibidos a menos que se adopten medidas de detección adicionales. En el caso de equipos, plataformas o infraestructuras de OT/IIoT habilitados para TI, los resultados podrían amenazar la seguridad del personal o el medio ambiente. De manera similar, los actores de amenazas no detectados en los sistemas administrativos podrían afectar las actividades financieras.

Los ejecutivos de puertos e instalaciones portuarias deben garantizar que se implementen niveles adecuados de protección para detectar actividades anómalas o nefastas que, si no se abordan, podrían dejar a sus organizaciones vulnerables a ataques cibernéticos. Las capacidades específicas que deben implementarse

Depende de los requisitos específicos de la organización. Dependiendo de la disponibilidad de recursos y la tolerancia al riesgo, los ejecutivos de puertos e instalaciones portuarias deben considerar soluciones y actividades técnicas tales como:

- Sistemas de detección de intrusos / sistemas de protección contra intrusos (IDS/IPS).
- Sistemas de Monitoreo de Eventos e Información de Seguridad (SIEM).
- Escaneo de vulnerabilidades.
- Caza de amenazas.
- Monitoreo continuo, servicios de seguridad administrados y/o detección y respuesta administradas.

Medidas organizativas

Se necesitan responsabilidades y procesos de las partes interesadas claramente definidos (Sección 2) para respaldar una detección eficaz de cibereventos. Los empleados son fundamentales para el proceso de detección y deben recibir la capacitación adecuada para reconocer incidentes de ciberseguridad e informarlos al personal designado. Dependiendo del tamaño y madurez del puerto o instalación portuaria, se debe considerar la organización de un Equipo de Respuesta a Incidentes de Ciberseguridad interno (Sección 10), el desarrollo de un Centro de Operaciones de Seguridad (SOC) o incluso la subcontratación de estas capacidades. Además, establecer relaciones formales con organizaciones CERT/CSIRT nacionales y/o internacionales, así como el fomento de proveedores de servicios externos clave, puede resultar útil independientemente del nivel de madurez, por ejemplo, para el intercambio de información sobre amenazas cibernéticas.

Medidas técnicas

Para respaldar las capacidades de detección técnica, los puertos y las instalaciones portuarias deben asignar recursos dedicados tanto para identificar como para evaluar eventos sospechosos de ciberseguridad. Esto se puede lograr empleando una plataforma SIEM, que recopila, agrega y coteja de forma centralizada datos de registro, correlaciona eventos de seguridad y alerta sobre anomalías. A continuación se enumeran ejemplos de eventos relevantes sobre los que alertan los SIEM:

- Intentos fallidos de inicio de sesión.
- Cambios de permisos, como grupos de usuarios privilegiados.
- Comportamiento inusual del usuario, por ejemplo, intentos de inicio de sesión incorrectos, horas de inicio de sesión.
- Intentos de acceso inusuales, por ejemplo, a áreas confidenciales o a sistemas honeypot.
- Creación de nueva cuenta.
- Patrones de ataque detectados (detección de intrusiones), indicadores de compromiso (“IoC”) o códigos maliciosos (detección de malware) en el flujo de datos o en los sistemas.
- Actividad anormal de la red (puntos finales nuevos/desconocidos, comunicación o datos inusuales). volumen).
- Cambios en la configuración relacionada con la seguridad, como escáneres de virus desactivados.
- Es importante que se puedan detectar todas las fases de un ciberataque para poder identificarlo rápidamente. El marco MITRE ATT&CK®27 se puede establecer para facilitar la clasificación de los ciberataques y está estructurado en fases (Figura 12).

27 Ver: https://attack.mitre.org/

FASE	EXPLICACIÓN
Reconocimiento	Encontrar información sobre el objetivo para preparar un ataque, por ejemplo, mediante escaneo activo, phishing o inteligencia de código abierto (OSINT).
Recurso Desarrollo	Preparar el ataque creando los recursos necesarios, como infraestructura, cuentas o capacidades.
Acceso inicial	Técnicas utilizadas para obtener acceso inicial a las estructuras internas del objetivo, como la explotación de vulnerabilidades, el compromiso drive-by o el phishing.
Ejecución	Ejecución de código malicioso que permite a los atacantes realizar un ataque.
Persistencia	Crear acceso persistente a los recursos del objetivo, por ejemplo, instalando puertas traseras o modificando las credenciales de autenticación.
Privilegio Escalada	Ampliar privilegios dentro de las redes y sistemas del objetivo, por ejemplo, explotando vulnerabilidades o configuraciones erróneas.
Evasión de defensa	Tomar medidas para evitar la detección y las defensas, por ejemplo, cambiando la configuración de seguridad o desactivando el software de protección.
Acceso a credenciales	Acceder a datos de autenticación, como contraseñas, por ejemplo, intentándolo (fuerza bruta), leyendo contraseñas de almacenes de contraseñas o utilizando registradores de teclas.
Descubrimiento	Explorar el entorno del objetivo, por ejemplo, observando el tráfico de la red, leyendo directorios de usuarios o repositorios de archivos.
Lateral Movimiento	Ampliar el acceso a todo el entorno de destino (por ejemplo, a través de servicios remotos, distribución de software, uso de credenciales robadas para comprometer activos o explotar vulnerabilidades).
Recopilación	Recopilar datos que puedan ser de interés para el atacante, por ejemplo, repositorios de archivos, bases de datos, datos de correo electrónico y navegador, o tomar capturas de pantalla y registrar las pulsaciones de teclas.
Comando y Control	Control remoto de los sistemas comprometidos de la víctima, generalmente haciéndose pasar por tráfico discreto para evitar la detección.
Exfiltración	Exfiltración de datos recopilados, por ejemplo, en forma cifrada o comprimida, para evitar la detección.
Impacto	Manipulación de sistemas, interrupción o destrucción de datos (por ejemplo, eliminando permisos de acceso, cifrando o eliminando archivos).

Figura 12 - Clasificación de ciberataques

7.3 Medidas de mitigación

Una respuesta adecuada a un incidente de ciberseguridad solo es posible si se identifica y asigna personal capacitado y se le proporciona las autoridades, procesos, procedimientos y tecnologías necesarios para realizar actividades de mitigación. Si bien la Sección 10 cubre específicamente la respuesta a incidentes de ciberseguridad, las actividades de planificación previa al incidente representan elementos críticos de protección y defensa.

Planes de continuidad del negocio/recuperación ante desastres

Garantizar la continuidad del negocio o volver a un estado adecuado de operación dentro de un período de tiempo aceptable es el objetivo de un plan de continuidad del negocio y recuperación ante desastres, independientemente de la causa.

Los planes de continuidad del negocio/recuperación ante desastres (BC/DR) especifican las medidas de precaución anticipadas que se deben tomar, así como las acciones específicas que se emplearán tras un incidente cibernético.

(Sección 10.6).

La planificación efectiva de BC/DR requiere que los ejecutivos de puertos e instalaciones portuarias y los tomadores de decisiones clave comprendan los problemas críticos que surgirán en caso de que la organización sufra un incidente cibernético y estén conscientes y capacitados adecuadamente en los procedimientos de recuperación apropiados.

La planificación de BC/DR comienza con una evaluación de las fortalezas de la capacidad de ciberseguridad de la organización (Sección 8) y los riesgos cibernéticos a los que se enfrenta la organización si sus sistemas de TI, OT o IIoT ya no funcionan. Específicamente, las partes interesadas responsables deben conocer las funciones críticas de OT o IIoT que pueden verse afectadas en caso de que sistemas de TI específicos queden inoperables. Una evaluación de riesgos con medidas de mitigación identificadas puede ayudar a aclarar cómo la organización podría verse afectada. Además, los escenarios de pérdidas (Sección 2.1.2) que abordan los riesgos ciberfísicos pueden ofrecer información específica sobre los tiempos críticos de recuperación.

Copia de seguridad/recuperación de datos

La copia de seguridad de datos es un elemento crítico tanto de la gestión de riesgos cibernéticos como de la planificación de recuperación ante desastres y representa la capacidad de acceder a copias de seguridad de datos funcionales y restaurar dichos datos dentro de los plazos requeridos. Si los datos de la organización se ven comprometidos, robados o destruidos, o incluso borrados accidentalmente por un empleado, una copia de seguridad facilitará la recuperación y puede permitir volver a las operaciones normales.

Los puertos y las instalaciones portuarias deben implementar políticas de respaldo, que describan todas las actividades de respaldo y definan la frecuencia de las copias de seguridad (por ejemplo, diariamente). Identifique en la política las funciones, responsabilidades y autoridades de las personas responsables de las actividades de respaldo. Identifique dónde y cómo se almacenan las copias de seguridad.
Considere implementar las siguientes mejores prácticas:

- Realice copias de seguridad de toda la información y pruebe copias de seguridad : cree, administre y pruebe periódicamente los esfuerzos de copia de seguridad, garantizando que las copias de datos, software e imágenes del sistema sean coherentes con las políticas de ciberseguridad.
- Proteger las instalaciones de almacenamiento de respaldo : identificar todos los equipos o software de respaldo necesarios para restaurar las funciones clave y garantizar que todas las áreas de almacenamiento (por ejemplo, casilleros/armarios) tengan la seguridad adecuada, como cerraduras y controles ambientales, como deshumidificadores o cierres resistentes al agua. para proteger equipos electrónicos. Las copias de seguridad deben conservarse fuera del sitio (instalación alternativa si es posible) y, si es necesario, almacenarse fuera de línea.
- Cifrar datos en tránsito : utilice software para proteger los datos en tránsito mediante cifrado. ▪ Cifrar datos de copia de seguridad : cifra todas las copias de seguridad. Cree múltiples copias de seguridad para que, en caso de una infracción, la restauración se puede realizar con una versión anterior a la infección.
- Considere la nube : los costos de almacenamiento en la nube continúan cayendo y son una opción viable para los puertos e instalaciones portuarias que buscan ahorros de costos y al mismo tiempo logran una mayor escalabilidad y disponibilidad de la red.

- Establecer redundancias : garantizar que se establezcan redundancias para sistemas clave de TI, OT e IIoT. Identificar necesidades operativas y de seguridad para sistemas con requisitos de alta disponibilidad.

- Capacitación y ejercicio : Capacite al personal para que participe en procesos manuales para restablecer operaciones críticas. Ejercer planes de recuperación para incidentes cibernéticos que comprometan TI, OT y/o IIoT sistemas.

8. INTERCAMBIO DE INFORMACIÓN, COMUNICACIONES Y COORDINACIÓN

8.1 Intercambio de información, comunicación y coordinación

El intercambio, la comunicación y la coordinación de información sobre ciberseguridad representan un componente amplio, pero esencial, de todo programa de ciberseguridad, como se describe en la Guía del NIST para el intercambio de información sobre amenazas cibernéticas28. Este capítulo no repite la documentación del NIST ni otras referencias de intercambio de información técnica, sino que presenta consideraciones de C-Suite para el intercambio de información de ciberseguridad, incluido por qué, qué y cómo el intercambio de información de ciberseguridad puede reducir los riesgos de ciberseguridad para los puertos y las instalaciones portuarias.

8.2 ¿Por qué compartir información sobre ciberseguridad?

El concepto de intercambio de información a menudo se ve a través de dos lentes: “compartir es dar” y “compartir es intercambiar”. El enfoque de “dar” a menudo se percibe negativamente como unidireccional, de poco o ningún beneficio y un camino para exponer las propias faltas. Alternativamente, el enfoque de “intercambio” fomenta un ambiente de comunicación bidireccional, responsabilidad mutua, sentimiento de comunidad, generación de confianza y creación de valor mutuo. Este último enfoque se recomienda para puertos e instalaciones portuarias.

Beneficios del intercambio de información cibernética

- Alineamiento Estratégico a través de estrategias integradas de negocio y ciberseguridad.
- Mayor Cumplimiento de la normativa existente y emergente.
- Mensajes consistentes con todas las partes interesadas que resulten en un entendimiento completo y común.
- Resiliencia mejorada con mayor conocimiento colectivo, experiencia y recursos de intercambio comunidad.

Figura 13: Beneficios del intercambio de información cibernética

Por encima de todo, el intercambio de información sobre ciberseguridad permite la toma de decisiones informadas para los puertos, las instalaciones portuarias y sus partes interesadas. El intercambio de información sobre ciberseguridad representa más que Cyber Threat Intelligence (CTI) para la prevención y respuesta a incidentes técnicos; El intercambio de información sobre ciberseguridad también incluye el intercambio de información no técnica sobre riesgos cibernéticos (CBRI) para la coordinación interna de los esfuerzos cibernéticos. El intercambio eficaz tanto de CTI como de CBRI proporciona una comprensión holística que puede mejorar la alineación estratégica, los recursos, el cumplimiento, los mensajes y la resiliencia.

28 Publicación especial (SP) 800-150 del NIST: Guía para el intercambio de información sobre amenazas cibernéticas; Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

Se pueden aplicar componentes básicos basados en el conocimiento para iniciar el intercambio de información sobre ciberseguridad entre las partes interesadas clave y empoderarlos con una comprensión fundamental de las mejores prácticas necesarias a partir de las cuales se puede crear un programa de ciberseguridad eficaz.

Niveles de intercambio de información

Los puertos disponen de muchos niveles de comunidades de intercambio de información sobre ciberseguridad. A continuación se presentan consideraciones de diferentes comunidades.

- Puerto o instalación portuaria (interna) : intercambio interno de CTI y CBRI, incluidos los servicios técnicos. información para la prevención y respuesta a incidentes, e información no técnica para evaluar riesgos empresariales.
- Comunidad portuaria (externa) : compartir CTI entre las instalaciones portuarias y otras cadenas de suministro. socios en un complejo portuario. Esto puede incluir amenazas cibernéticas contra la comunidad portuaria, investigaciones conjuntas, informes y análisis posteriores a incidentes, ejercicios y mejores prácticas.
- Puerto a puerto (o comunidad a comunidad) – Fomentar la cooperación bilateral compartiendo CTI directamente entre puertos conocidos o comunidades portuarias. Esto puede incluir información acordada sobre amenazas cibernéticas, informes y análisis posteriores a incidentes, ejercicios y mejores prácticas.
- Sector portuario : una entidad de análisis e intercambio de CTI específica del sector para compartir información relevante sobre amenazas cibernéticas que es común a los puertos en general. Esto sirve como una opción para puertos grandes o pequeños que pueden tener objetivos de seguridad comunes para respaldar las relaciones de intercambio de información de puerto a puerto.
- Sector marítimo : similar a una entidad compartida del sector portuario, una entidad compartida del sector marítimo comparte CTI relevante para la industria marítima. Dicha entidad goza de una perspectiva de riesgo más amplia que afecta al sector marítimo y también tendrá CTI directamente relevantes para los puertos o instalaciones portuarias, así como para los propietarios y operadores de buques y otras partes interesadas marítimas.
- Nacional : el sector marítimo debe contar con el apoyo de un centro de respuesta de ciberseguridad a nivel nacional, generalmente el Equipo de Respuesta a Emergencias Informáticas (CERT) nacional, el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) o equivalente. Los CERT nacionales suelen estar expuestos a inteligencia clasificada sobre amenazas cibernéticas y pueden proporcionar a los puertos e instalaciones portuarias información clave sobre incidentes, amenazas, alertas, análisis, directivas y disposiciones. Algunos CERT nacionales operarán un portal o plataforma de información para intercambiar información con sus electores.

- Internacional : se realiza en múltiples niveles, incluyendo puerto a puerto, comunidad a comunidad, unidad sectorial a unidad paralela, ministerio a ministerio y/o gobierno a gobierno. La información compartida depende de las políticas establecidas y puede verse afectada por las tendencias políticas. En algunos casos, la información compartida, y su intensidad, está sujeta a acuerdos bilaterales firmados entre los países u otros grupos de actores.

- Público en general : algunos países exigen notificaciones públicas de incumplimiento. Los puertos y las instalaciones portuarias en estos entornos deberían considerar procedimientos de notificación pública predefinidos.

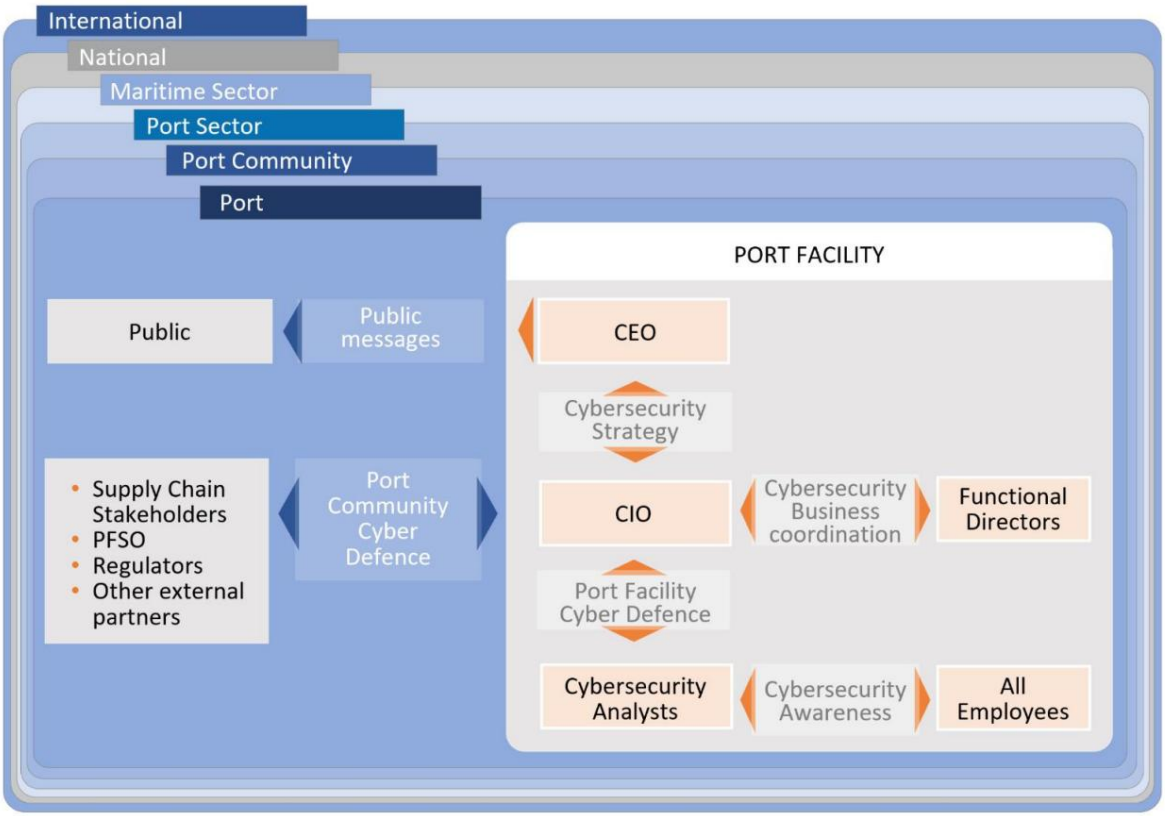

Figura 14 - Modelo de intercambio de información cibernética para puertos e instalaciones portuarias

8.4 Establecer un sólido programa de intercambio de información sobre ciberseguridad

Esta sección presenta consideraciones clave para que los ejecutivos de puertos o instalaciones portuarias establezcan un programa eficaz de intercambio de información sobre ciberseguridad. En particular, las prácticas de intercambio de información sobre ciberseguridad dependen en gran medida de las leyes específicas de cada país, el despliegue operativo e institucional de ciberseguridad, las interdependencias entre entidades y la cultura de intercambio de información en la comunidad.

Declarar la ciberseguridad como una prioridad organizacional

La declaración de un CEO o director general de la ciberseguridad como máxima prioridad será efectiva para defender una cultura cibernética y alinear las áreas funcionales de la organización, incluidas áreas clave como operaciones, TI, legal, gestión de riesgos, finanzas, relaciones con los medios y relaciones con los clientes. , asuntos gubernamentales, recursos humanos y adquisiciones. Sin dicho apoyo, la ciberseguridad puede seguir considerándose una responsabilidad exclusiva del Departamento de TI y limitar las comunicaciones.

Designar un líder de ciberseguridad

El Líder Designado de Ciberseguridad será responsable de implementar el programa de intercambio de información de ciberseguridad29. El liderazgo es el papel central, ya que actúa como coordinador de todas las actividades cibernéticas clave. Este rol debe ser capaz de traducir la estrategia comercial organizacional en una estrategia técnica de ciberseguridad, coordinar los esfuerzos de ciberseguridad en diferentes áreas funcionales, interactuar con partes interesadas externas y cumplir con los requisitos de cumplimiento. Esta función suele estar codificada bajo el título de CIO, CISO u otro título, y para puertos o instalaciones portuarias más pequeñas puede incluso contratarse o subcontratarse. Quienquiera que sea el líder de ciberseguridad designado, debe reunirse periódicamente con el puerto.

29 Como se describe en NIST SP 800-150.

o Liderazgo Ejecutivo de la instalación portuaria respecto de la estrategia de ciberseguridad de la organización. Este rol también debe iniciar la comunicación a nivel de la empresa para comprobar la comprensión y ejecución de las medidas derivadas de la estrategia.

Establecer relaciones para compartir información.
El intercambio de información sobre ciberseguridad implica comunicaciones fuera de la organización, incluidas las comunicaciones obligatorias y voluntarias con las partes interesadas. Aunque el líder de ciberseguridad designado implementará el programa, generalmente se necesita el director ejecutivo u otro liderazgo ejecutivo designado para asegurar el compromiso de sus pares en otras organizaciones para que compartan su información de ciberseguridad.

Participar en compartir relaciones.
La participación ejecutiva demostrará la importancia de compartir información sobre ciberseguridad y maximizar su valor. Esto puede incluir el monitoreo periódico de la eficacia del intercambio de información de ciberseguridad, continuar dedicando recursos a los esfuerzos, participar en la gobernanza comunitaria y comunicarse interna y externamente.

Mejorar continuamente
A medida que la comunidad de intercambio de información sobre ciberseguridad madure, debería intentar autoevaluarse continuamente. También se recomiendan revisiones periódicas de los riesgos cambiantes y el perfeccionamiento de los objetivos y protocolos compartidos. Además, otras comunidades de intercambio de información, incluidas las de otras industrias, pueden ser una fuente de aprendizaje de mejores prácticas30 que pueden mejorar el intercambio de ciberseguridad en puertos e instalaciones portuarias.

30 Documento de ciberseguridad de la comunidad portuaria de la IAPH, 2021, Guardia Costera de EE. UU., Carta de política CG-5P, 12 de diciembre de 2016, The
El Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos ha desarrollado la Publicación Especial 800-150, Reino Unido
Centro Nacional de Seguridad Cibernética, Asociación para el Intercambio de Información sobre Seguridad Cibernética (NCSC CiSP), Información sobre Seguridad Cibernética
Ley de intercambio de 2015

9. ENTRENAMIENTO

9.1 La importancia de establecer una conciencia cibernética organizacional

9.1.1 Lo Humano como riesgo

Los comportamientos de los empleados (curiosidades, descuidos, prejuicios y deseos) representan colectivamente eslabones débiles en el programa de ciberseguridad de un puerto o instalación portuaria. Los puertos y las instalaciones portuarias a ambos lados de la brecha digital enfrentan un desafío universal en materia de ciberseguridad: la gestión de lo humano. El error humano por sí solo genera una amplia gama de riesgos cibernéticos, y se estima que el 95 por ciento de las violaciones de seguridad cibernética son el resultado de errores humanos, en lugar de fallas relacionadas con TI[31].

Muchas de las estrategias más exitosas de los actores de amenazas cibernéticas aprovechan la psicología y el comportamiento de las personas en sus interacciones con la tecnología digital. La variedad de profesiones, habilidades, idiomas y culturas de las personas que interactúan con un puerto o los activos de una instalación portuaria hace que la tarea de abordar el error humano sea un desafío recurrente. Los actores de las amenazas cibernéticas buscan constantemente penetrar los activos e infraestructuras de TI/OT/IIoT, que controlan procesos esenciales u otros sistemas involucrados en la creación, el procesamiento, el almacenamiento y la transmisión de datos. Buscan errores humanos o adaptan sus ataques para explotar comportamientos, prejuicios, conexiones sociales y/o afiliaciones culturales. Estos errores ofrecen puntos de apoyo en las redes, lo que permite a los actores de amenazas cibernéticas penetrar más profundamente en las redes y a través de ellas.

Aunque las inversiones en diversos recursos técnicos (por ejemplo, sistemas de control de acceso, cortafuegos, etc.) mejoran las defensas cibernéticas, dichos esfuerzos pueden resultar inútiles cuando una persona con las credenciales apropiadas (nombre de usuario/contraseña) ejerce una mala higiene cibernética al hacer clic en un correo electrónico. archivo adjunto o un enlace URL a un sitio web infectado con malware. El desafío que enfrenta el liderazgo portuario es cómo proporcionar recursos adecuados para brindar la capacitación necesaria para desarrollar la conciencia, monitorear el progreso y gestionar los recursos e inversiones necesarios para lograr la resiliencia cibernética operativa.

Tipos de errores humanos

- El empleado comprometido introduce dispositivos infectados en (y se conecta a) la TI/OT de una organización. redes.
- El empleado descuidado se apresura a completar una tarea, a menudo sin malas intenciones. Sus errores son el resultado de violando las políticas de seguridad.
- El empleado malintencionado crea daño deliberado al comprometer un sistema de TI/OT o al robar datos. Sus motivos pueden ser económicos, de insatisfacción o simplemente maliciosos.

Figura 15 - Tipos de errores humanos

9.1.2 Reconocer al Humano como primera línea de defensa

En última instancia, se requiere patrocinio ejecutivo para garantizar el éxito de cualquier programa de capacitación. Los líderes de puertos e instalaciones portuarias deben comunicar expectativas claras sobre la capacitación al personal no relacionado con TI en todos los entornos operativos funcionales de la organización.

[31] https://www.cybintsolutions.com/cyber-security-facts-stats/

Aunque el riesgo cibernético es generalizado, la capacitación es una inversión de bajo costo y alto valor agregado. Para que la formación en ciberseguridad sea eficaz, no puede relegarse a una actividad anual de "marcar casillas" ni únicamente al personal de TI.
Aunque el personal de TI es directamente responsable de garantizar la integridad de los datos y la seguridad de la red, y la obligación de patrocinar una cultura cibernética recae en los ejecutivos del puerto y de las instalaciones portuarias, la responsabilidad de mantener la resiliencia cibernética a través del compromiso y la concientización continuos es, en última instancia, compartida. El Humano representa la primera línea de defensa de la organización. Esto involucra a todos los directivos y tomadores de decisiones clave de TI, seguridad, administración, gestión de riesgos, recursos humanos, adquisiciones, contratos, capacitación, salud y seguridad, marketing y comunicaciones.

Los puertos y las instalaciones portuarias con personal con conciencia cibernética posicionan ventajosamente a sus organizaciones dentro de la comunidad portuaria local y la industria marítima global. Específicamente, una fuerza laboral más consciente de lo cibernético se traduce en una organización más competitiva y ciberresiliente. Cuando las personas están capacitadas para reconocer las ciberamenazas y comprender cómo responder a los incidentes, la organización puede recuperarse más rápidamente de las ciberdisrupciones.

9.2 La capacitación es una parte integral de un programa de gestión de riesgos cibernéticos

9.2.1. Desarrollo y gestión de la fuerza laboral.

A medida que los puertos y las instalaciones portuarias invierten e implementan cada vez más tecnologías habilitadas para TI/OT/IIoT en sus entornos operativos, enfrentan el desafío de cultivar una fuerza laboral cibernética y cibercompetente. Los puertos y las instalaciones portuarias deberían requerir tanto capacitación general en concientización cibernética para que todo el personal mantenga la atención, como capacitación más avanzada para el personal de TI/OT para mantener habilidades y desarrollar nuevas competencias. Este programa podría desarrollarse respetando una perspectiva del ciclo del personal desde la incorporación hasta la jubilación o salida de las personas.

Desarrollar la capacidad de la fuerza laboral como parte de un programa a largo plazo requiere acciones coordinadas que incluyen identificar los requisitos portuarios, adaptar la capacitación a personal específico, establecer objetivos, identificar y encargar a las partes responsables la entrega de productos de capacitación y asignar deberes y responsabilidades apropiadas (que incluyen la gestión y vigilancia). Deben establecerse presupuestos para sostener las inversiones en materiales de capacitación; Las tecnologías y actividades de implementación relacionadas deben organizarse para áreas funcionales clave. El contenido de la capacitación debe presentarse de manera que refuerce
planes establecidos, políticas, procedimientos y tecnologías implementadas. Toda la capacitación debe ser monitoreada y las brechas de conocimiento (incluidas las tendencias) deben identificarse de manera consistente y periódica. Las competencias del personal deben mapearse en todas las áreas funcionales. Las prácticas de reclutamiento y contratación deben abordar las brechas identificadas en la fuerza laboral. Se deben diseñar estrategias de capacitación para mitigar las deficiencias en cualquier área de conocimiento y habilidades. Cuando sea posible, se deben explorar y aprovechar asociaciones con instituciones académicas locales para desarrollar la capacidad de la fuerza laboral. La comunicación de consejos útiles y prácticos y una campaña de sensibilización pueden respaldar estas medidas de formación de forma más eficaz. Los empleados pueden aplicarlos en su rutina diaria, lo que influye en su cambio de comportamiento y su sensibilidad a los problemas relacionados con la cibernética.

Individuos sujetos a capacitación en concientización cibernética

- Todos los ejecutivos y altos directivos.
- Finanzas, contabilidad y administración.
- Operadores de seguridad, operaciones y equipos.
- Ventas, marketing y comunicaciones.
- Recursos humanos y gestión de personal.
- Salud, seguridad y formación.
- Adquisiciones, contrataciones y asuntos legales.
- Terceros: proveedores, contratistas y socios.

Figura 16 - Individuos sujetos a formación en sensibilización cibernética

9.2.2 Capacitación en sensibilización general

Independientemente del tamaño, la ubicación o la complejidad de un puerto o instalación portuaria, se debe exigir capacitación en concientización sobre ciberseguridad a todo el personal que acceda a los sistemas en red. Siempre que sea posible, la formación en materia de concienciación cibernética debe adaptarse a la organización. Esto involucra:

- Capacitación para todo el personal administrativo que accede a sistemas habilitados para TI, como computadoras de escritorio, que debe abordar cómo reconocer correos electrónicos maliciosos, adherirse a políticas definidas como condición para acceder a dispositivos habilitados para red, emplear fuertes controles de contraseña y mantener credenciales seguras.

- La capacitación del personal de operaciones debe incluir amenazas cibernéticas a los sistemas habilitados para OT/IIoT, como equipos de manejo de carga, sistemas de almacenamiento y transferencia de líquidos a granel y transportadores.
  sistemas.
- La capacitación de los oficiales de protección de las instalaciones portuarias debería facilitar una mayor comprensión de las amenazas cibernéticas y cómo colaborar eficazmente con el personal de TI. La formación debería abordar cómo reconocer las interconexiones ciberfísicas. Por ejemplo, la instrucción debe cubrir cómo reconocer un peligro para la seguridad de TI, como activos de TIC no seguros, y cómo informar y/o investigar actividades sospechosas observadas.

9.2.3 Formación técnica en ciberseguridad

Los líderes de puertos e instalaciones portuarias con personal técnico responsable de las tareas y responsabilidades de seguridad de la información (por ejemplo, CISO, CIO o gerentes de TI) deben fomentar la capacitación continua en ciberseguridad avanzada. La capacitación debe permitir las operaciones de ciberseguridad, estar estructurada para respaldar objetivos de desempeño definidos y contar con los recursos adecuados. Como mejor práctica, los puertos y las instalaciones portuarias deberían definir habilidades, educación y/o requisitos de capacitación en ciberseguridad antes de contratar personal de TI. Además, parte del personal técnico, como los desarrolladores de software, puede requerir niveles mínimos definidos de conocimientos sobre ciberseguridad, como un conocimiento práctico de las mejores prácticas del ciclo de vida del desarrollo de software seguro.

Los puertos y las instalaciones portuarias que buscan capacitación especializada en ciberseguridad (incluidas certificaciones) para su personal técnico pueden considerar una amplia gama de organizaciones de desarrollo profesional que ofrecen certificaciones reconocidas mundialmente y programas de capacitación recurrentes32.

9.2.4. Implementación de capacitación

9.2.4.1 Actividades de formación personalizadas

El primer paso para aumentar la conciencia cibernética en un puerto o instalación portuaria es implementar una serie de eventos para todo el personal, como conferencias y seminarios web, patrocinados por la dirección ejecutiva, que enfaticen la concienciación sobre los riesgos cibernéticos. Los puertos y las instalaciones portuarias pueden entonces reforzar los objetivos de aprendizaje a través de opciones adicionales de capacitación en concientización sobre ciberseguridad, como cursos de capacitación en concientización sobre ciberseguridad basados en computadora (CD/DVD) y/o en la web, diseñados para la industria marítima. Dado que los proveedores y terceros realizan cada vez más monitoreo administrativo y de contenido

32 Instituto SANS (www.sans.org), Asociación de Control y Auditoría de Sistemas de Información (ISACA) (www.isaca.org), Consorcio Internacional de Certificación de Seguridad de Sistemas de Información (ISC2) (www.isc2.org), Asociación de la Industria de Tecnología de Computación (www.comptia.org)

tareas de gestión, los líderes de capacitación deberían considerar instituir una capacitación obligatoria en concientización cibernética como un requisito previo para las partes interesadas externas, a quienes se les puede exigir que accedan a sistemas críticos de TI/OT/IIoT.

Los puertos y las instalaciones portuarias deberían considerar enriquecer la conciencia sobre la ciberseguridad a través de programas de capacitación en ciberseguridad in situ o virtuales, que pueden adaptarse para satisfacer necesidades específicas. Los materiales de capacitación pueden diferenciarse para adaptarse a una comunicación integral para diferentes grupos objetivo de fuerza laboral. Los puertos o instalaciones portuarias que participan en sistemas comunitarios portuarios o en intercambios de información locales también podrían considerar la posibilidad de aunar recursos para desarrollar y mantener materiales de capacitación localizados.

9.2.4.2 Simulacros

Los puertos e instalaciones portuarias sujetas a regulaciones, como el Código PBIP, ya realizan simulacros trimestrales. Los escenarios de simulacros deben revisarse y ampliarse para adaptarse a situaciones de ciberseguridad que ponen a prueba la preparación del personal del puerto o de las instalaciones portuarias. Los simulacros deben diseñarse como un esfuerzo de colaboración entre el personal de ciberseguridad, seguridad y operaciones.

La incorporación de factores de riesgo cibernético en los simulacros trimestrales refuerza la conciencia de cómo una amenaza cibernética puede afectar directa o indirectamente las operaciones. Los riesgos cibernéticos se pueden inyectar en muchos escenarios de simulacros para probar procedimientos multifuncionales de alerta, escalamiento y comunicaciones de incidentes. Los escenarios de perforación también deben incluir aspectos de información y de intercambio de amenazas en tiempo real (Sección 10), o escenarios que involucren dependencias de terceros y cadenas de suministro portuarias. Los simulacros ponen a prueba la conciencia cibernética de todos los participantes en los simulacros con respecto al conocimiento de la respuesta a incidentes (Sección 10), la efectividad de los deberes y responsabilidades asignados, los comportamientos de respuesta y la efectividad general. Los resultados deben analizarse para determinar su impacto y considerarse para la revisión de la estrategia o los planes de seguridad cibernética, según sea necesario.

9.2.4.3 Ejercicios

Los ejercicios de mesa (TTX), realizados anualmente, tienen como objetivo comprobar la eficacia del entrenamiento.
Deben reflejar el entorno operativo de los participantes para determinar cómo la organización podría responder a desafíos hipotéticos.
Deben poner a prueba la conciencia general, validar planes y procesos y evaluar los sistemas y procedimientos para la respuesta a incidentes y las acciones de recuperación. Se pueden revelar desafíos, consecuencias y brechas de capacidad imprevistos para resaltar las vulnerabilidades. Los resultados deben analizarse para determinar el impacto directo para la organización, así como para cualquier tercero potencialmente afectado.

El personal de capacitación, seguridad, operaciones y TI debe colaborar para revisar los planes de respuesta y seguridad existentes para diseñar escenarios de riesgo que incorporen amenazas físicas y cibernéticas en una variedad de sistemas y procesos. Cuando se realizan, los TTX deben medir el tiempo y los procesos asociados con la detección y alerta de un incidente cibernético e identificar si los planes, el personal, el equipo y los procedimientos de alerta y comunicación funcionan como se espera. Los escenarios integrados de amenazas ciberfísicas deberían estresar los entornos administrativos y operativos de la organización. Según corresponda, se pueden incluir terceros, como socios del sistema de la comunidad portuaria (incluidos los miembros del SOC portuario), CERT/CSIRT regionales o nacionales, proveedores especializados de respuesta a incidentes e incluso autoridades designadas.

9.2.5 La formación como medio para impulsar la mejora continua

Auditorías, inspecciones y revisiones

Los puertos y las instalaciones portuarias deberían evaluar periódicamente el desempeño y la eficacia de su programa de capacitación cibernética mediante:

- Incluir la cibersensibilización en el proceso anual de inspección y preauditoría de seguridad.
- Realizar auditorías aleatorias de áreas operativas clave para probar la conciencia y el comportamiento del personal y evaluar la eficacia de las políticas y procedimientos.
- Proporcionar capacitación y certificación actualizada al personal de seguridad de TI.

- Establecer controles de supervisión y revisión para garantizar un seguimiento regular de toda la capacitación. programas, contenidos y actividades.

Al implementar estas estrategias, se identificarán las brechas de conocimiento del personal y se desarrollarán acciones correctivas posteriores. Estos incluyen contenidos y estrategias de capacitación, nuevas herramientas y/o tecnologías, controles, políticas y procedimientos, cambios presupuestarios e incluso nuevas contrataciones.

Desarrollar lecciones
aprendidas. Documentar las brechas identificadas, las actividades de respuesta y las recomendaciones de mitigación en informes posteriores a la acción ayudará a los líderes a identificar oportunidades de mejora. Por ejemplo, se deben identificar, caracterizar y describir claramente las fallas en la cadena de mando, la confusión sobre responsabilidades y autoridades y los impactos de los ciberataques en las operaciones. Además, se deben identificar, definir y priorizar claramente las mejoras en el contenido de la capacitación, los requisitos de recursos y las habilidades requeridas.

10. RESPUESTA Y RECUPERACIÓN A INCIDENTES

10.1 Planificación y preparación de la respuesta a incidentes

En el lenguaje de respuesta a incidentes cibernéticos, la máxima “más vale una onza de protección que una libra de cura” es cierta33, y los líderes actuales de puertos e instalaciones portuarias deberían asumir que su organización algún día sufrirá una violación de ciberseguridad. Desafortunadamente, el crecimiento continuo de los esquemas de ransomware y phishing por correo electrónico, junto con la incipiente adopción de la IA por parte de redes criminales, desafiarán a los puertos y las instalaciones portuarias a ambos lados de la brecha digital. Bajo tales presiones, es menos cuestión de si
en lugar de cuándo se violará un puerto o una instalación portuaria.

Para prepararse para tales contingencias, los ejecutivos de puertos e instalaciones portuarias deben tomar las medidas necesarias para preparar proactivamente a sus organizaciones para responder y recuperarse de un incidente de ciberseguridad.
Hacerlo servirá para proteger los intereses de su organización, madurar su capacidad de responder y recuperarse de un incidente, y avanzar no solo en su resiliencia operativa, sino también fortalecer una resiliencia cibernética más amplia de la comunidad portuaria en la que residen y de la industria marítima global en general.

Si bien las circunstancias de los incidentes cibernéticos varían, existen dos tipos de incidentes. El primero es de naturaleza empresarial , que afecta a numerosas áreas de una organización. Desde el nivel empresarial
Los incidentes pueden amenazar a toda la organización, a menudo requieren la movilización de varios miembros del personal.
de diferentes áreas funcionales (incluido el director ejecutivo y la junta directiva), así como expertos técnicos externos que pueden contratarse fácilmente para realizar análisis de expertos y tomar acciones correctivas.

Tipos de incidentes cibernéticos

- Incumplimiento físico : robo físico, la pérdida involuntaria de un activo (su función se ve interrumpida o perdido), o el compromiso físico de un activo que permite facilitar el robo de datos, compromete la confidencialidad e integridad de los datos, o permite el acceso a un activo que ha sido eliminado de la organización y que no ha sido desmagnetizado adecuadamente.
- Violación de datos : la exposición, divulgación o pérdida intencional o no intencional a una persona que no es de confianza. entorno de datos clasificados como confidenciales, privados o sensibles.
- Violación de la seguridad de la red y/o del sistema : cuando una computadora, enrutador de red, firewall o cualquier componente de la red se ve comprometido por una infección de malware o usuarios autorizados o no autorizados acceden a él con intenciones maliciosas.

Figura 17 - Tipos de incidentes cibernéticos

El segundo tipo puede limitarse a un sitio, activo, sistema o proceso operativo discreto. Aunque inicialmente está físicamente localizado o limitado, un incidente de este tipo que no se detecta puede tener un impacto significativo con consecuencias inmediatas y/o en cascada. Dependiendo de la gravedad, las acciones de respuesta a incidentes pueden requerir el mismo nivel de recursos movilizados para la respuesta y la recuperación. Por lo tanto, los esfuerzos de planificación y preparación de respuesta a incidentes deben armonizarse con las actividades de gestión de la seguridad operativa del puerto o de la instalación portuaria.

33 A menudo se atribuye a esta cita a Benjamín Franklin, quien regularmente advertía a los habitantes de Filadelfia sobre el riesgo de incendio.

10.2 Componentes clave de la respuesta a incidentes de ciberseguridad y pasos de implementación

La planificación de la respuesta a incidentes cibernéticos comienza a nivel ejecutivo porque gestionar adecuadamente un esfuerzo de respuesta a una infracción no es simplemente una cuestión técnica. La respuesta adecuada a incidentes implica una variedad de disciplinas, que abarcan todas las áreas de operaciones del puerto o de la instalación portuaria, y debe incluir a las partes interesadas responsables de diversas áreas funcionales y áreas de responsabilidad superpuestas.

Las personas asignadas a la responsabilidad de la respuesta a incidentes pueden consultar recursos disponibles gratuitamente. y mejores prácticas para ayudar a guiar sus esfuerzos de planificación, organización, implementación y mantenimiento para un programa apropiado de respuesta a incidentes. Por ejemplo, el NIST y la Comisión Europea ofrecen recursos gratuitos para las partes interesadas34.

Al planificar cualquier respuesta a incidentes para un puerto o una instalación portuaria, los ejecutivos del puerto o de la instalación portuaria deben colaborar con sus equipos de liderazgo para considerar los siguientes pasos:

Paso 1: crear una política y un plan de respuesta a incidentes

- La alta dirección debe comprometerse a establecer requisitos de desempeño específicos y asignar responsabilidades. Las políticas deben describir el alcance, definir acciones e identificar a los miembros del equipo de respuesta a incidentes de seguridad cibernética.
- Implementar un Plan de Respuesta a Incidentes de Ciberseguridad (CIRP) y asignar partes interesadas clave para desarrollarlo, mantenerlo y ejecutarlo. Los CIRP deben incluir escenarios relevantes para el entorno operativo real del puerto o de la instalación portuaria. En este caso la clasificación de las instalaciones portuarias ayudaría a diseñar los escenarios. Por ejemplo, un CIRP que solo aborde escenarios basados en oficinas no será útil para instalaciones portuarias con entornos complejos de TI/OT/IIoT. Los CIRP deben incluir criterios de escalada de incidentes cibernéticos, como umbrales y factores desencadenantes para contactar e interactuar con recursos internos y externos.

Paso 2: Desarrollar procedimientos claros para el manejo de incidentes, incluidas las respuestas a ataques comunes.

- Además del CIRP, definir y documentar qué procedimientos se siguen en caso de un incidente cibernético. Esto incluye clasificación de eventos, análisis y declaración de incidentes. También debería incluir procedimientos que guíen la declaración, clasificación y priorización de incidentes.
- Para acelerar el proceso de toma de decisiones durante la respuesta a incidentes, prepare las decisiones clave estratégicas con anticipación y manténgalas en formato impreso. Dependiendo de los objetivos operativos de la organización, dichas decisiones pueden definir cómo la organización gestiona en general un incidente cibernético, lo que debe incluir una estrategia de comunicación, decisiones legales clave y una lista de partes interesadas esenciales, incluido el equipo ejecutivo, que deben participar (con contacto información).

- Definir y documentar cómo la organización contendrá un incidente declarado. Definir procedimientos para la erradicación, mitigación y recuperación de amenazas. Los procedimientos deben estar claramente definidos y ser flexibles. Los directivos de puertos e instalaciones portuarias deberían fomentar la redacción de procedimientos para manejar tipos específicos de incidentes, tales como los siguientes:

  - Ataque de phishing exitoso
  - Malware, incluido ransomware, troyanos, gusanos, droppers, etc.
  - Ataque de denegación de servicio
  - Ataque a aplicaciones web (scripting entre sitios, falsificación de solicitudes entre sitios, inyección SQL)
  - Suplantación de DNS

34 NIST SP 800-61 (R2), Guía de manejo de incidentes de seguridad informática es una guía de uso común; y el conjunto de herramientas de ciberseguridad del transporte de la CE; Ver: https://ec.europa.eu/transport/themes/security/cybersecurity_en

Paso 3: Establecer requisitos de notificación de incidentes

- Dentro del plan de respuesta a incidentes, identifique a las personas responsables de informar a terceros, como organismos de gobernanza nacionales y/o internacionales (por ejemplo, reguladores), autoridades policiales, control estatal del puerto, aseguradoras, clientes, socios y otras partes interesadas.
- Al responder a un incidente cibernético, gestionar la comunicación interna con las partes interesadas es clave. Es importante que los ejecutivos reconozcan que no todos dentro de la organización pueden comprender las implicaciones de un incidente cibernético en el contexto de su trabajo o departamento específico. Se deben desarrollar planes de comunicación para la gestión de incidentes que identifiquen claramente quién debe ser notificado e involucrado (Capítulo 10). Se deben identificar los miembros del equipo de crisis y del equipo ejecutivo, incluidos protocolos para notificar e involucrar a los propietarios de activos, sistemas, equipos e infraestructura relevantes y a aquellos que dependen de sus funciones.

- Gestionar la comunicación con las partes interesadas externas es fundamental. La primera reacción podría ser cerrar cualquier comunicación saliente o actualización de información. Sin embargo, los ejecutivos deben reconocer que terceros dentro de la comunidad portuaria pueden enterarse rápidamente de una infracción. Si un puerto o una instalación portuaria ya no puede operar, se recomienda encarecidamente la comunicación y la participación proactivas. ▪ Las comunicaciones con los medios deben ser

consistentes, coordinadas y disciplinadas, y todas

Los mensajes deben entregarse a través de un representante designado. Plantillas de notificación
Debe prepararse con antelación para permitir modificaciones rápidas y notificaciones externas.

Paso 4: Establecer y capacitar a un Equipo de Respuesta a Incidentes de Ciberseguridad (CsIRT)

- Es fundamental para la planificación y preparación eficaz de la respuesta a incidentes el establecimiento de un Equipo de Respuesta a Incidentes de Ciberseguridad (CSIRT). El CSIRT debe contar con un grupo dedicado de personas específicamente capacitadas para responder a incidentes cibernéticos y comprender cómo realizar todas las fases de un esfuerzo de respuesta y recuperación.
- Al organizar el CSIRT, asegúrese de que las personas asignadas estén facultadas para tomar decisiones con el fin de actuar para responder rápidamente a los eventos. Se debe asignar al CSIRT un miembro del equipo de liderazgo ejecutivo (por ejemplo, CISO o CIO). Debe incluir personal de TI, seguridad, legal, comunicaciones/relaciones públicas y operaciones funcionales del puerto o instalación portuaria. Cada departamento debe estar representado para garantizar la participación durante una
actividad de respuesta. En algunos casos, un CSIRT podría organizarse en torno a un equipo de respuesta a crisis existente que esté estructurado para hacer frente a una variedad de incidentes importantes.
- Nominar a un miembro del CSIRT que tenga más experiencia en liderar la organización a través de las complejidades y el estrés de las actividades de recuperación de crisis. Designarlos formalmente como Presidente del CSIRT. Este individuo debe ser percibido como un unificador, centrándose
sobre la colaboración y facilitar comunicaciones claras entre otros miembros de la organización y el personal ejecutivo.

- Identificar suplentes del Presidente del CSIRT y todos los representantes clave del CSIRT. Dado que las acciones de recuperación de incidentes cibernéticos pueden ser complejas, es importante que el puerto o la instalación portuaria mantenga una nueva participación de las partes interesadas durante todo el esfuerzo, y se pueden involucrar alternativas para apoyar las actividades de recuperación extendidas.

Paso 5: Identificar recursos clave

- Es fundamental para la planificación de la respuesta a incidentes la necesidad de identificar la experiencia necesaria para volver a poner en línea los sistemas, equipos y/o infraestructura. El manejo de sistemas IT/OT/IIoT requiere habilidades técnicas especiales y, cuando se necesitan con urgencia, los desafíos pueden resultar abrumadores dependiendo de la disponibilidad del personal o de la experiencia de terceros. Los puertos y los operadores portuarios tal vez deseen considerar identificar e involucrar a una organización externa que se especialice en la respuesta a incidentes de ciberseguridad que involucren entornos de TI/OT/IIoT. Comprometerse con los nacionales

Las organizaciones de ciberseguridad, como los CERT o los CSIRT nacionales, es otra opción recomendada que vale la pena considerar (Sección 8.3).

Paso 6: Probar los planes de respuesta a incidentes y las capacidades del CSIRT

- Probar el CIRP en simulacros regulares para garantizar que las capacidades del CSIRT se mantengan actualizadas y que los miembros del equipo estén familiarizados entre sí, lo que debe incluir conocimiento de las fortalezas y debilidades individuales. Dado que lo más probable es que la organización trabaje con otras entidades dentro de la comunidad portuaria, invite a terceros interesados a participar en los simulacros. Estas personas pueden ser de otras terminales u organizaciones de servicios, así como de organizaciones de emergencia o de aplicación de la ley.

- Probar el CIRP al menos una vez al año en un ejercicio integral. Los ejercicios no deben centrarse en y peores escenarios, pero deben diseñarse para probar específicamente cómo se desempeña la organización , CSIRT en general durante una crisis. Los ejercicios pueden dar como resultado experiencias y hallazgos clave que son bastante diferentes de las actividades típicas del día a día. Asegúrese de que los ejercicios estén diseñados para expresar una interrupción de los sistemas de TI y de los servicios habilitados por TI que resulten en estrés operativo. Incorporar deliberadamente desafíos que afecten a los sistemas IT/OT/IIoT en los ejercicios para obligar al equipo CSIRT a colaborar con personal de diferentes áreas operativas. También es valioso asignar a una persona o un grupo de observadores para obtener una visión general de los procesos ejecutados en el ejercicio y de las lecciones aprendidas junto con las experiencias de las personas involucradas en el escenario de prueba.

- Establecer protocolos para que el CSIRT obtenga acceso rápido a sistemas y conjuntos de datos clave en caso de un incidente. Como mejor práctica, el CSIRT debería tener fácil acceso a información como registros de seguridad, que probablemente serán necesarios para respaldar el análisis, la selección, la clasificación, la priorización y las decisiones de mitigación. Los registros deben almacenarse y mantenerse periódicamente en un entorno separado (por ejemplo, segmento de red o entorno de nube) independiente del entorno de red principal del puerto o de la instalación portuaria. Dicha separación permitirá al CSIRT determinar rápidamente qué tan extendida puede haber penetrado una amenaza cibernética e identificar qué sistemas pueden haberse visto afectados y cuáles podrían permanecer operativos.

10.3 Detección y análisis

Como la detección de eventos basada en TI se cubrió en la Sección 7, aquí la atención se centrará en los sistemas OT.
Los ciberataques no sólo se limitan a los sistemas de TI, sino que también pueden lanzarse contra sistemas OT vulnerables. Las consecuencias de un sistema OT comprometido pueden poner en peligro la salud y la seguridad del personal, dañar el medio ambiente y/o destruir equipos e infraestructura. Peor aún, el impacto en cascada de un ciberataque OT exitoso puede afectar la cadena de suministro marítima en general. Por ejemplo, la falla de los sistemas informáticos a bordo de sensores remotos o sistemas instrumentados de seguridad puede provocar una falla del sistema, lo que resulta en interrupciones operativas y copias de seguridad de la cadena de suministro.

Los sistemas habilitados para OT operados desde una o más ubicaciones remotas o automatizadas pueden ser vulnerables a los ataques cibernéticos. El análisis de los eventos detectados debe centrarse en los sistemas OT más críticos para las operaciones del puerto o de las instalaciones portuarias, el manejo de carga, las infraestructuras críticas, los equipos (es decir, grúas), así como para los sistemas de instrumentos de seguridad y el monitoreo de protección. En algunos casos, una autoridad portuaria podría actuar como organismo coordinador en acciones de respuesta y recuperación cuando múltiples instalaciones, incluidas instalaciones remotas, puedan haber sido afectadas.

Se debe realizar un análisis de un incidente cibernético que resulte en la posible ruptura de la cadena de suministro marítimo y compartir los hallazgos clave con las partes afectadas. Para algunos puertos e instalaciones portuarias, compartir dicha información podría parecer contradictorio, ya que la reacción inicial podría

ser mantener la confidencialidad del incidente cibernético. Sin embargo, dado que todos los puertos y las instalaciones portuarias contribuyen a la cadena de suministro marítima global, se alienta a los ejecutivos a reconocer que una de las mejores prácticas en ciberseguridad es compartir ideas clave extraídas de ciberataques exitosos. La Sección 8 ofrece información detallada y orientación sobre las mejores prácticas para compartir información.

10.4 Contención y recuperación

La contención y la recuperación implican actividades necesarias para limitar los efectos de un incidente y los pasos necesarios para que la organización vuelva a sus operaciones normales.

Los planes de continuidad del negocio (BCP) son fundamentales para restaurar las operaciones después de un incidente importante. Dado que los activos y sistemas de TI/OT/IIoT integran cada vez más todos los aspectos de los procesos operativos de un puerto o de una instalación portuaria, los BCP en puertos e instalaciones portuarias suelen estar dominados por contenido técnico que aborda sus sistemas de TI/OT/IIoT.

Los BCP comparten cuatro componentes generales:

- Respuesta a emergencias : se centra en las personas, la comunicación, la responsabilidad del personal y evacuación y transición al equipo de gestión de crisis.
- Gestión de crisis : se centra en los procesos de decisión relacionados con la contención, el comando, el control y la colaboración de incidentes.
- Reanudación del negocio : se centra en restaurar los procesos de negocio y su continuidad.
- Plan de recuperación de desastres de TI : se centra en la recuperación de sistemas de información y la disponibilidad de Activos tecnológicos para la prestación de servicios empresariales.

Figura 18: Los BCP comparten cuatro componentes generales

Si bien un BCP es un plan de base amplia que orienta los esfuerzos de recuperación operativa, un puerto o una instalación portuaria El plan de respuesta a incidentes debe proporcionar instrucciones específicas sobre cómo responde la organización a un incidente. El CIRT de la organización debe identificar las acciones específicas necesarias para restaurar la funcionalidad comercial y técnica de los activos y sistemas clave que respaldan su entorno operativo de TI/OT/IIoT.

Con un plan de respuesta a incidentes bien desarrollado y probado, un puerto o instalación portuaria puede aprovechar un marco de gestión de riesgos de ciberseguridad mediante la implementación de funciones de contención, erradicación y recuperación aplicables. Cada uno de estos elementos, dependiendo del tamaño y la complejidad de las operaciones de un puerto o instalación portuaria, puede resultar completo y técnicamente complejo. Un objetivo principal de la respuesta proactiva a incidentes es escalar rápidamente la postura general de seguridad de la organización con una serie de cambios relativamente rápidos y de alto valor diseñados para evitar incidentes posteriores. Más específicamente:

- Es esencial implementar estrategias de contención antes de que un incidente abrume a las autoridades internas. recursos, la perturbación se expande y/o se producen daños a los activos.
- Erradicación de los componentes de un incidente de todos los hosts afectados para que puedan ser remediados.
- La recuperación implica restaurar los sistemas a sus operaciones normales y remediar la vulnerabilidad para evitar incidentes similares.

10.5 Contención y erradicación

Las actividades coordinadas de contención de incidentes son fundamentales para las operaciones del puerto o de las instalaciones portuarias. Una vez detectado un incidente, se debe contener. Las acciones de contención deben centrarse inicialmente en el impacto potencial sobre la seguridad humana, la protección y las operaciones. Durante la respuesta a incidentes cibernéticos, la seguridad física del puerto o de la instalación portuaria debe seguir siendo una prioridad, especialmente controlando el acceso a áreas restringidas, como las salas de servidores. Aquí es donde se necesita la comunicación entre el personal de TI y el Oficial de la Instalación de Protección Portuaria (PFSO). Dependiendo de la magnitud del incidente y su posible impacto en los sistemas de seguridad, es posible que se requiera que el OPIP cambie el nivel de seguridad de la instalación de conformidad con los planes de seguridad aplicables.

Para los sistemas OT, la respuesta a incidentes debe centrarse en aislar los activos y/o sistemas afectados. En algunos casos, se pueden implementar elementos o procedimientos BCP específicos para encontrar soluciones alternativas con sistemas alternativos. Al hacer esto, siempre se debe tener en cuenta la seguridad de los procesos de las instalaciones.

Una vez que se determina el alcance del incidente cibernético, los esfuerzos de respuesta al incidente deben seguir rutas de mitigación de riesgos internas y externas. Internamente, a medida que el CIRT de la organización contiene el ataque e implementa medidas de mitigación, se debe realizar un análisis de impacto para determinar las implicaciones en la "vida real" de cómo las partes interesadas internas y externas podrían verse afectadas. Para las partes interesadas responsables o dependientes de los sistemas IT/OT/IIoT, esto significa confirmar qué información permanece accesible y qué datos han conservado su integridad. Los esfuerzos de mitigación podrían implicar volver a crear imágenes o recargar sistemas de TI clave recurriendo a copias de seguridad. Si bien este enfoque podría dar lugar a una recuperación rápida, es posible que no siempre sea una opción.

La contención externa también implica mantener buenas relaciones con socios clave, clientes, socios portuarios y terceros críticos en la cadena de suministro marítimo. Al informarles sobre las medidas de respuesta a incidentes que está tomando su organización, podrán actuar en consecuencia.

10.6 Recuperación posterior al incidente

La recuperación posterior al incidente depende en gran parte de la planificación y los preparativos del incidente que se hayan realizado antes del incidente cibernético. Dependiendo del tipo de incidente, si se realizan copias de seguridad del sistema y se han establecido medidas de gestión de crisis, es posible que los esfuerzos de recuperación posteriores al incidente se logren más rápidamente. En algunos casos, puede ocurrir un incidente cibernético en el que las copias de seguridad no sean la única respuesta. En la mayoría de los casos, es esencial que las partes interesadas comprendan qué componentes organizacionales requieren secuenciación, es decir, el orden y la velocidad con la que los sistemas vuelven a estar en línea. El grado de integración de los sistemas en los entornos portuarios eleva la criticidad de esto.

10.7 Desarrollar lecciones aprendidas con las partes interesadas relevantes

Una vez que un incidente ha sido mitigado, es importante aprender de él para identificar sus causas específicas, los factores contribuyentes y el impacto. Es imperativo investigar las causas del incidente, determinar el impacto operativo en el activo o sistema de TI/OT/IIoT afectado, comprender las consecuencias (financieras, regulatorias, legales, reputacionales, etc.) y desarrollar un conjunto de de lecciones aprendidas. La realización de una investigación conducirá a una mayor comprensión del alcance total de cómo se aprovechó la vulnerabilidad, su impacto en las operaciones y las implicaciones para la confidencialidad de los datos.

integridad y disponibilidad. Es recomendable desarrollar un conjunto de lecciones aprendidas e incorporar los hallazgos en futuros simulacros y ejercicios, así como en materiales de capacitación.

Cuando corresponda, compartir lecciones entre la comunidad portuaria, así como con socios de la industria, como MTS-ISAC. Las partes interesadas de la comunidad portuaria pueden beneficiarse de esto implementando sus propias medidas de seguridad antes de posibles ataques cibernéticos. El resultado es una comunidad portuaria fortalecida y más ciberresiliente.

11. MEJORA CONTINUA Y CIBERSEGURIDAD MADUREZ

Para concluir las directrices, este capítulo resume las conclusiones clave para los ejecutivos y la alta dirección del puerto o de las instalaciones portuarias responsables de la gestión del riesgo cibernético con el objetivo de tomar medidas concretas:

- Por qué la ciberseguridad no es sólo para el "departamento de TI".
- Cómo la capacidad de ciberseguridad impulsa la ciberresiliencia.
- Estrategias de liderazgo para impulsar la ciberresiliencia.

11.1 Por qué la ciberseguridad no es sólo para el "departamento de TI"

La ciberseguridad es una preocupación esencial para todo puerto o instalación portuaria. Los ejecutivos marítimos enfrentan la tarea de garantizar que sus organizaciones comprendan los riesgos y establezcan las prioridades adecuadas. Desafortunadamente, con una experiencia limitada en ciberseguridad, muchos ejecutivos tienen conceptos erróneos sobre cómo abordar el riesgo cibernético y, como resultado, muchos perciben la ciberseguridad como un misterio gestionado por el personal de TI.

Como se destacó anteriormente, la gestión del riesgo cibernético abarca tecnologías, procesos, estructuras y prácticas que se adaptan adecuadamente para proteger mejor los activos, sistemas, sistemas y sistemas portuarios y de las instalaciones portuarias. infraestructura y datos. Sin embargo, los ejecutivos tienden a enfatizar demasiado el papel de la tecnología como solución al desafío del riesgo cibernético. Sin duda, el personal de TI desempeña un papel esencial en el apoyo a las actividades críticas de ciberseguridad porque administra y monitorea las redes y la infraestructura de TI a través de las cuales pueden surgir ciberamenazas. Pero centrarse únicamente en la tecnología presenta una promesa falsa, ya que no puede eliminar por completo el riesgo cibernético de un puerto o instalación portuaria. En este sentido, ya no es apropiado relegar la responsabilidad de la gestión del riesgo cibernético enteramente al personal de TI o, como es el caso de muchas instalaciones portuarias pequeñas y medianas, subcontratarla por completo.

Para subrayar este punto, los actores de amenazas cibernéticas comúnmente apuntan al personal que no pertenece a TI, que representa la mayoría del personal de una organización, para violar un entorno de red seguro. Por ejemplo, los actores de amenazas cibernéticas pueden explotar información de código abierto para formular y ejecutar ataques de correo electrónico dirigidos basados en ingeniería social, conocidos como phishing. Cuando tienen éxito, estos ataques eluden las defensas cibernéticas administradas por TI, haciendo que las tecnologías y protocolos de seguridad pierdan su valor.

La importancia de implementar un enfoque integral de ciberseguridad en toda la organización en el ámbito marítimo solo aumentará a medida que los puertos y las instalaciones portuarias se vuelvan cada vez más dependientes de la automatización y las tecnologías integradas de TI/OT/IIoT. La industria del transporte marítimo siempre ha enfrentado riesgos operativos y, con el tiempo, los ha mitigado exitosamente a través de cuidadosas estrategias de gestión de riesgos, regímenes de cumplimiento y participación de toda la organización. Al igual que con la seguridad y la protección, se debe aplicar la misma filosofía de gestión de riesgos al abordar el riesgo cibernético y esto se puede lograr trabajando hacia la madurez de la ciberseguridad organizacional.

11.2 Cómo la capacidad de ciberseguridad impulsa la ciberresiliencia

A medida que evolucionan las amenazas cibernéticas, los puertos y las instalaciones portuarias deben centrarse en desarrollar capacidades de ciberseguridad para lograr y mantener una postura ciberresiliente. En concreto, deberían poder anticipar, identificar, detectar, responder y recuperarse de los ciberataques. Para puertos e instalaciones portuarias a ambos lados

de la brecha digital, esto significa más que invertir en soluciones técnicas: requiere que sus líderes se apropien del riesgo cibernético y construyan un modelo eficaz para la gestión del riesgo cibernético. Requiere identificar y aplicar técnicas proactivas de gestión de riesgos; colaboración interfuncional entre el personal; cultivar y mantener una cultura de riesgo cibernético; e implementar mejores prácticas que fomenten la mejora continua.

Hay medidas prácticas que un puerto o instalación portuaria puede tomar para mejorar las capacidades de ciberseguridad de su organización. El primer paso es involucrar a la alta dirección : líderes portuarios y de instalaciones portuarias deben asumir la responsabilidad de supervisar los esfuerzos de gestión del riesgo cibernético de su organización y hacerlo de manera holística que abarque todas las áreas de su organización. Aquellas organizaciones con juntas directivas deberían incluir la ciberseguridad como un tema habitual en las sesiones informativas periódicas. Las actividades de supervisión deben incluir un seguimiento constante de las actividades en el contexto de la estrategia de ciberseguridad.

Para ser eficaces, los ejecutivos deben tener una comprensión adecuada de la capacidad de la organización y definir la dirección futura de los controles de riesgos. Para lograrlo, los puertos y las instalaciones portuarias tal vez deseen considerar realizar primero una evaluación de la madurez de la capacidad de ciberseguridad de toda su red. organización.

El análisis de madurez de la capacidad de ciberseguridad proporciona una estructura flexible para evaluar cada área funcional de una instalación portuaria y ofrece una metodología para establecer una línea de base de las capacidades actuales frente a los riesgos cibernéticos con el fin de respaldar los esfuerzos de mejora continua. Si se ejecuta correctamente, este análisis permite a los ejecutivos determinar dónde pueden existir fortalezas o debilidades de ciberseguridad dentro de sus organizaciones. Tomar decisiones bien informadas sobre cómo y dónde invertir fondos y asignar valiosos recursos es de suma importancia. Algunas capacidades pueden ser más adecuadas para invertir que otras. El empleo de un análisis de madurez de la capacidad de ciberseguridad calibra la relevancia de la capacidad, crea una base para evaluaciones comparativas recurrentes y orienta la planificación de inversiones. Una vez completado, este análisis ayudará a los ejecutivos de puertos e instalaciones portuarias a caracterizar las capacidades generales del estado actual de su organización y medir la madurez de la ciberseguridad dentro de un modelo similar al descrito en la Figura 19 [35] .

Figura 19: Creación de resiliencia cibernética

[35] Creación de resiliencia cibernética en la gestión de activos; KPMG (mayo de 2018)

El lugar en el que se encuentre un puerto o una instalación portuaria dentro de este modelo dependerá de una variedad de factores, incluida la complejidad de su entorno operativo, el grado en que se han implementado y conectado en red las tecnologías de TI/OT/IIoT y de automatización, y el alcance de las capacidades de ciberseguridad. empleados para proteger el entorno operativo. Dado que las determinaciones de madurez de la capacidad de ciberseguridad son exclusivas de los puertos individuales, un puerto pequeño con liderazgo comprometido y tecnología implementada limitada podría autoidentificarse con un mayor estado de madurez de la capacidad de ciberseguridad que un puerto grande, altamente automatizado e integrado que tal vez no haya invertido. adecuadamente en las medidas de ciberseguridad o sufre de un liderazgo no comprometido.

Los puertos y las instalaciones portuarias pueden construir sus defensas de ciberseguridad en torno a marcos industriales líderes[36], que pueden ayudar a las organizaciones a:

- Construir un entorno de confianza con sus socios comerciales.
- Incrementar la concienciación en materia de seguridad entre el personal.
- Desarrollar un enfoque organizado basado en riesgos para comprender el valor comercial de la información. y sistemas de información y sus integraciones con sistemas operativos.
- Demostrar madurez de los procesos.
- Proporcionar una estructura para la mejora continua.

11.3 Estrategias de liderazgo para impulsar la resiliencia cibernética

Para lograr una mayor resiliencia cibernética, los puertos y las instalaciones portuarias deben considerar el desarrollo de las siguientes capacidades de ciberseguridad, que son la culminación de los temas tratados en estas directrices:

- Involucrar a los ejecutivos en cuestiones de ciberseguridad: los ejecutivos deben asumir la responsabilidad y la supervisión de la gestión de riesgos cibernéticos en toda la organización. Se requiere conciencia sobre los riesgos cibernéticos para guiar la toma de decisiones, lo que se puede lograr mediante capacitación y/o sesiones informativas periódicas por parte del personal técnico o expertos externos que pueden participar, según sea necesario.
  Se deben establecer autoridades para determinar quién supervisa qué y se deben definir claramente protocolos de comunicación/información para identificar quién informa a quién y cuándo.

- Desarrollar un modelo de madurez de capacidad de ciberseguridad específico de la organización: el ejecutivo debería considerar trabajar con partes interesadas clave para definir el contexto organizacional dentro del cual se puede aplicar un modelo de madurez como el de la Figura 19. Por ejemplo, identificando y evaluando cada una de las áreas funcionales de la organización dentro de la estructura de madurez de la capacidad de ciberseguridad. Las áreas funcionales variarán según la organización, pero pueden incluir TI, administración, operaciones, seguridad, capacitación, salud y seguridad, cumplimiento/gestión de riesgos, legal, etc. La alta dirección de cada área debe participar en el análisis inicial y continuo de la capacidad de ciberseguridad y en la asignación de recursos. , y planificación de esfuerzos, así como en la coordinación de actividades de recuperación, si fuera necesario.

- Gestionar el modelo de gestión de riesgos basado en la madurez de la capacidad de ciberseguridad: para que un puerto o instalación portuaria logre una mayor resiliencia cibernética, es importante identificar y reconocer las amenazas que podrían enfrentar. Esto requiere hacer un inventario y mapear todos los activos (por ejemplo, información, datos, sistemas informáticos, etc.); realizar análisis de impacto de amenazas; determinar las personas, los procesos, las herramientas y el dinero en riesgo; identificar e implementar medidas de mitigación; definir tolerancias de riesgo para las opciones de aceptación, evitación, tratamiento y transferencia de riesgos; e informar periódicamente tanto a nivel interfuncional (en todas las áreas funcionales) como a los ejecutivos y la junta directiva.

[36] Los ejemplos incluyen los promulgados por NIST e ISO, entre otros.

- Cultivar una cultura de concientización sobre la ciberseguridad: la gestión del riesgo cibernético tiene más que ver con las personas que con la tecnología, por lo que es crucial educar, capacitar y empoderar al personal en todos los niveles. Una cultura cibersegura sólo tiene éxito cuando los altos ejecutivos patrocinan la capacitación. Comienza con una ciberhigiene básica. Todo el personal debería: 1) estar informado de los riesgos para la organización; 2) comprender lo que se espera de ellos; y 3) saber qué hacer en caso de incumplimiento. ▪
- Garantizar una gestión eficaz de terceros: la cadena de suministro de un puerto o instalación portuaria representa una fuente importante de riesgo cibernético. Las partes interesadas deben colaborar y coordinar esfuerzos para desarrollar requisitos de ciberseguridad para los procesos de adquisición, contratación (por ejemplo, cláusulas de notificación de incumplimiento), pruebas y análisis de vulnerabilidad de los servicios recién contratados. Los acuerdos de nivel de servicio deben definir estándares de respuesta a incidentes y restauración del servicio. Un puerto o instalación portuaria también debe establecer un programa de monitoreo de seguridad para proveedores basado en el análisis y
- priorización de riesgos. ▪ Implementar soluciones de ciberseguridad apropiadas para responder a incidentes de seguridad: No importa cuánto invierta un puerto o una instalación portuaria en sus defensas cibernéticas, se producirán ciberataques Es fundamental que los ejecutivos implementen las capacidades necesarias para que su organización detectar, prevenir y tratar adecuadamente que los actores de amenazas cibernéticas obtengan acceso no autorizado a sistemas clave. Algunas organizaciones pueden implementar centros de operaciones de seguridad (SOC) internos, mientras que otras pueden intentar subcontratarlos. En cualquier caso, las capacidades del SOC brindan a las partes interesadas las herramientas necesarias para detectar eventos cuando ocurren y coordinar acciones de respuesta y recuperación rápidas para limitar el impacto de los eventos. Integradas con las políticas, procedimientos, controles y mecanismos de presentación de informes adecuados, las organizaciones cibermaduradas se beneficiarán al reducir el potencial de tiempo de inactividad y mejorar su capacidad para recuperarse y reiniciar operaciones.

Siguiendo estas conclusiones clave, se pueden iniciar y establecer las bases del programa de resiliencia cibernética del puerto y de la instalación portuaria. La ambición de la IAPH es que estas directrices apoyen a los puertos, sus instalaciones y las organizaciones relevantes en un puerto en la implementación de una verdadera resiliencia cibernética.

12. ANEXOS – CIBERSEGURIDAD DE LAS INSTALACIONES PORTUARIAS

PLANTILLAS DE EVALUACIÓN Y PLAN

12.1 Introducción

El propósito de los Anexos es brindar al líder de ciberseguridad designado asistencia práctica para desarrollar su Plan de protección del puerto o de la instalación portuaria (P/PFSP). Los anexos incluyen orientación y el índice de un modelo de P/PFSP que se puede utilizar como modelo. La organización debe adaptar esta plantilla a sus requisitos específicos según corresponda.

12.2 Plantilla de evaluación de la ciberseguridad de puertos e instalaciones portuarias

▪ Antecedentes ▪
Descripción general de la metodología de evaluación ▪
Descripción general de las instalaciones ▪ Detalles de las instalaciones/Información de contacto de ciberseguridad ▪ Identificación de activos
▪ Resumen
▪ Datos
▪ Sistemas de tecnología de la información (TI)
▪ Sistemas de tecnología operativa (OT) ▪ Sistemas de Internet industrial de las cosas (IIoT) ▪ Otra infraestructura y equipo críticos ▪ Entidades/ funciones críticas de soporte externo ▪ [por ejemplo, servicios públicos]
▪ [Proveedores de servicios externos, por ejemplo ISP, etc.]

- Identificación de amenazas/vulnerabilidades y análisis de riesgos ▪ Resumen ▪ Amenazas de ciberseguridad a [Organización] ▪ Registro de riesgos
- Gobernanza
  ▪ Administración y organización de la seguridad ▪ Gestión de registros ▪ Auditorías e inspecciones
- Consideraciones de ciberseguridad para las medidas de seguridad existentes ▪ Arquitectura empresarial ▪ Entorno operativo OT [según corresponda]
  ▪ Medidas Técnicas de Protección para
    ▪ Sistemas OT – Infraestructura Fija ▪ Sistemas OT – Móviles ▪
  Procedimientos (Planes, Políticas, Procedimientos, Controles)
    ▪ Sistemas OT – Infraestructura Fija ▪ Sistemas OT – Móviles

- ▪ Entorno Operativo de TI ▪
  - Medidas Técnicas de Protección ▪
  - Procedimentales (Planes, Políticas, Procedimientos, Controles) ▪ Medidas de Seguridad
    - Física ▪ Seguridad
    - Perimetral ▪ Controles de Acceso
    - ▪ Áreas restringidas
    - ▪ Monitoreo de medidas de seguridad
    - ▪ Mantenimiento de sistemas y equipos de seguridad ▪ Comunicaciones ▪
      - Interfaz barco – costa ▪
      - Inalámbrico
      - ▪ Radio
      - ▪ Niveles de seguridad
- ▪ Operaciones de manejo de carga
- ▪ Capacitación
- ▪ Respuesta y recuperación de incidentes
- ▪ Resumen del análisis de impacto

- ▪ Resumen de hallazgos y recomendaciones priorizadas ▪ Hallazgos ▪ Recomendaciones priorizadas
- ▪ Estrategias para mejorar la ciberseguridad

12.3 Plantilla de plan de ciberseguridad para puertos e instalaciones portuarias

- ▪ Antecedentes
- ▪ Descripción general de las instalaciones
- ▪ Detalles de la instalación
- ▪ Información de contacto de ciberseguridad

Nombre del Director Designado/Oficial de Seguridad de la Información Cibernética (“CISO” o “CYSO”)	INSERTAR NOMBRE
Número de teléfono de la oficina del CISO	INSERTAR
Número de teléfono móvil del CISO	INSERTAR
Dirección de correo electrónico	INSERTAR
del CISO Nombre del CISO	INSERTAR NOMBRE
adjunto Número de teléfono móvil del CISO adjunto	INSERTAR
Correo electrónico del CISO	INSERTAR
adjunto Nombre del oficial de protección de la instalación portuaria (PFSO):	INSERTAR
Número de teléfono de la oficina de OPIP	[INSERTAR LO MISMO DEL PLAN DE SEGURIDAD PORTUARIA – “PFSP”]
PFSO Número de teléfono móvil	[INSERTAR LO MISMO DE PFSP]
Correo electrónico	[INSERTAR LO MISMO DE PFSP]
del OPIP Nombre del OPIP	[INSERTAR LO MISMO DE PFSP]
adjunto No. de teléfono móvil del OPIP	[INSERTAR LO MISMO DE PFSP]
Correo electrónico adjunto del OPIP	[INSERTAR LO MISMO DE PFSP]
Ubicación/Dirección de la Oficina de Seguridad del PFSO	[INSERTAR LO MISMO DE PFSP]
Ubicación / dirección de la oficina del CISO	[INSERTAR LO MISMO DE PFSP]

- ▪ Descripción general de la ciberseguridad

Guía:

- ▪ Proporcionar una descripción general del entorno operativo digital de la organización, que debe incluir descripciones generales de todos los entornos administrativos y operativos en red. Por ejemplo, ¿hay redes separadas que admitan sistemas administrativos de tecnología de la información (TI) y sistemas de tecnología operativa (OT)? ¿Se emplean redes inalámbricas? Identifique activos importantes (p. ej., grúas en red) o infraestructura habilitada para OT (p. ej., sistemas de control de tráfico de embarcaciones, atracaderos, puertas, grúas terminales, instalaciones de almacenamiento, sus puntos de acceso, puertas de enlace y tuberías). ¿Se emplean múltiples redes? ▪ Describir a alto nivel todas las operaciones de administración, seguridad, recepción y manipulación de carga, almacenamiento y logística, y comunicaciones que dependen de activos habilitados por TI. Enumere todos los edificios y estructuras de instalaciones en red (p. ej., administración, centros de control de gestión del tráfico de embarcaciones, centros de datos, almacenes, etc.), infraestructura lineal (p. ej., sistemas ferroviarios, transportadores, etc.), plantas y maquinaria (p. ej., grúas, barreras). , cerraduras, etc.), y otros sistemas, como seguridad electrónica, sistemas de escaneo y otras infraestructuras operativas y de comunicaciones.

- ▪ Niveles de seguridad

Orientación: Identificar las actividades de ciberseguridad realizadas para cada Nivel de Seguridad. En cada nivel, las amenazas cibernéticas deben comunicarse a los socios portuarios.

▪ Consideraciones y definiciones de ciberseguridad marítima ▪ Descripción general

▪ Confidencialidad ▪ Integridad ▪ Disponibilidad ▪ Funcionalidad ▪ Resiliencia cibernética ▪ Salud, seguridad y protección ambiental ▪ Funcionalidad ▪ Evaluación de riesgos

Orientación: Introduzca descripciones para reflejar con precisión el entorno operativo actual de la organización según los hallazgos descritos en la PFSA y cualquier evaluación complementaria de ciberseguridad realizada previamente.

▪ Amenazas ▪ Vulnerabilidades ▪ Consecuencias ▪ Estándares Referenciados ▪ Medidas de Seguridad ▪ Comité Directivo de Ciberseguridad (u otro Grupo de Trabajo Interno) ▪ Gestión de Seguridad

Orientación: Identifique al personal clave de ciberseguridad, como el Director de Seguridad de la Información (CISO), incluido cómo y cuándo el personal de seguridad física y ciberseguridad coordina las actividades y realiza notificaciones sobre actividades sospechosas, violaciones de seguridad y cambios en el nivel de seguridad.

▪ Administración y Organización de la Ciberseguridad ▪ Centro de Operaciones de Seguridad ▪ Comité de Seguridad Portuaria (Subcomité Cibernético) ▪ Cambios en el Nivel de Seguridad ▪ Deberes, Responsabilidades y Autoridades de Ciberseguridad del Personal de [Instalación] ▪ Capacitación en Ciberseguridad ▪ Simulacros y Ejercicios de Ciberseguridad ▪ Mantenimiento de Equipos del Sistema de Seguridad ▪ Puerto Revisión, modificación y auditoría del plan de seguridad de las instalaciones ▪ Evaluación y notificación de incidentes de ciberseguridad ▪ Planes de contingencia ▪ Seguridad de la información

▪ Mercancías y sustancias peligrosas ▪ Mantenimiento de registros y documentación ▪ Comunicaciones

▪ Comunicaciones entre buques e instalaciones portuarias

▪ Alerta de seguridad del barco

▪ Declaración de seguridad ▪ Notificación de incidentes y actividades sospechosas ▪ Respuesta y Recuperación de Incidentes de Ciberseguridad ▪ Medidas de Ciberseguridad ▪ Ciberseguridad para Áreas Restringidas e Instalaciones Controladas ▪ Ciberseguridad para Manejo de Carga, Entrega y Almacenamiento de Almacenes ▪ Ciberseguridad para Sistemas de Seguridad Electrónica ▪ Control de Acceso

▪ Monitoreo perimetral ▪
Centro de operaciones de
seguridad ▪ Otros requisitos de ciberseguridad

GLOSARIO DE TÉRMINOS

Término	Definición
Control de acceso	La disciplina, tecnología, proceso y/o control para limitar el acceso a las aplicaciones, sistemas, plataformas, activos críticos e instalaciones de una organización a entidades autorizadas (por ejemplo, personal autorizado, flujos de trabajo y/o intercambios de datos).
Avanzado Amenaza persistente (APTO)	Un ciberatacante o adversario que posee capacidades técnicas sofisticadas, experiencia y recursos que le permiten emplear una variedad de tácticas, técnicas y procedimientos (por ejemplo, cibernéticos, físicos, engaños, etc.) para llevar a cabo un ataque contra una víctima específica.
Anomalía	Comportamiento exhibido que es excéntrico o inconsistente o se desvía de lo que se considera normal o típico.
antivirus Software	Software especializado diseñado para detectar y, cuando sea posible, mitigar el malware antes de que ataque un sistema. Para que sea eficaz, el software antivirus debe mantenerse con las últimas actualizaciones para que pueda identificar, aislar y reparar archivos infectados de forma eficaz.
Autenticación	El proceso empleado para verificar la identidad y autenticidad de un usuario, dispositivo, sistema o aplicación designado como condición para obtener acceso a un sitio protegido. recurso.
Autorización	El proceso para aprobar o permitir que un individuo, una aplicación y/o un sistema haga algo.
Disponibilidad	La condición para facilitar el acceso oportuno y consistente a un activo, conjunto de datos o sistema o servicio basado en información.
Puerta trasera	Una brecha no documentada en una aplicación de software o sistema informático que permite el acceso a usuarios no autenticados, eludiendo los procesos de seguridad.
Respaldo	Una práctica diseñada para guardar archivos electrónicos contra pérdida, destrucción, daño o falta de disponibilidad involuntarios. Los métodos incluyen cintas de alta capacidad, discos o servicios administrados basados en la nube proporcionados por un tercero. Los esfuerzos de respaldo deben realizarse fuera del sitio, físicamente lo suficientemente lejos del sitio principal de la organización (por ejemplo, la sede administrativa) para reducir el riesgo de que factores de riesgo ambientales potenciales (por ejemplo, terremotos, inundaciones, incendios) afecten tanto al sitio principal como al sitio. sitio de respaldo.
Lista negra Software	Las listas negras de software permiten filtrar sitios web que han sido identificados y especificados como inseguros. Las empresas a veces lo utilizan para evitar que el personal visite sitios web dañinos, como aquellos que han sido identificados como abrevaderos comunes. Si bien la inclusión en listas negras es eficaz para impedir el acceso a sitios web conocidos, es menos eficaz contra sitios web con riesgos desconocidos.

Bot	Una computadora conectada a Internet que ha sido comprometida subrepticiamente con malware que dirige la computadora a realizar actividades específicas dirigidas por un administrador remoto con privilegios de comando y control.
Fuerza bruta Ataque	Un proceso metódico mediante el cual un ciberatacante emplea un enfoque exhaustivo de prueba y error para obtener acceso a información confidencial. Por lo general, el software se aplica para generar automáticamente cantidades masivas de “conjeturas” simultáneas con la esperanza de que alguna de ellas finalmente tenga éxito.
Impacto de negocios Análisis (BIA)	Un análisis cuantitativo que distingue controles, funciones, procesos y actividades organizacionales críticos y no críticos y prioriza su impacto como resultado de un compromiso o pérdida de una aplicación, sistema o plataforma. Luego se evalúan cualitativa y/o cuantitativamente la criticidad y/o sensibilidad de los activos y luego se determina la aceptabilidad del riesgo identificado, incluidos los costos de recuperación.
Común Operando (Operacional) Imagen (COP)	A menudo reflejada en una única pantalla (o conjunto de pantallas), una COP es la consolidación e integración de múltiples y relevantes actividades y tecnologías que se han configurado para recopilar, analizar, alertar, visualizar y utilizar información de ciberseguridad, incluido el estado y los eventos. Informacion de sumario. Está diseñado para proporcionar conciencia situacional, facilitar la colaboración y apoyar la toma de decisiones informadas sobre cuestiones de ciberseguridad.
Computadora Incidente de seguridad	Una violación de las políticas de seguridad informática establecidas, incluidas las políticas de uso aceptable u otras prácticas de seguridad estandarizadas según lo definido en los planes de seguridad de la organización. (Ver también Incidente)
Confidencialidad	El estado protegido logrado por un conjunto de reglas claramente definidas y restricciones autorizadas que determinan el acceso y/o divulgación de los datos. Incluye restricciones diseñadas para proteger datos relacionados con la privacidad personal y otra información de propiedad exclusiva. Para un activo administrado o basado en información, la confidencialidad se mantiene al permitir que solo personas, procesos y/o dispositivos autorizados y autenticados accedan a él.
Configuración Gestión	Un conjunto de procesos definidos y actividades controladas diseñadas para establecer y mantener la integridad de un activo, aplicación, sistema o plataforma a lo largo de su ciclo de vida. La gestión de la configuración generalmente implica especificaciones y procedimientos documentados para gestionar la tecnología de la información y los sistemas, activos o plataformas basados en tecnología operativa. También proporciona un medio común para rastrear y gestionar la inicialización, el cambio y el monitoreo a largo plazo de sus configuraciones.
Plan de contingencia	Un plan, generalmente expresado como un procedimiento de gestión, para respaldar las actividades de respuesta en caso de que la capacidad de un activo, aplicación, sistema y/o plataforma se pierda, se interrumpa o se vea comprometida. A menudo es el primer plan que utilizan las partes interesadas para caracterizar lo que sucedió, comprender por qué ocurrió e identificar las actividades iniciales de mitigación. También puede hacer referencia directa a los planes de seguridad de las instalaciones y de la empresa, así como a los planes de continuidad de las operaciones y/o recuperación ante desastres en caso de una interrupción importante.

Continuo Supervisión	Un enfoque de gestión de riesgos para lograr y mantener una conciencia continua del estado de ciberseguridad de una organización. El monitoreo continuo recopila, analiza, alerta, visualiza y respalda a los profesionales de la tecnología de la información, la tecnología operativa y la seguridad mediante la identificación de eventos anómalos, vulnerabilidades y amenazas en todo el entorno operativo de la organización. Su propósito es apoyar las actividades de respuesta a incidentes y la toma de decisiones de gestión de riesgos.
Control S	Un conjunto de políticas operativas y/o procedimientos técnicos definidos, que pueden ser manuales o automatizados, que respaldan la tecnología de la información, la tecnología operativa y los procesos comerciales en la protección de la confidencialidad, integridad y disponibilidad de los datos.
Galleta	Una cookie es un pequeño archivo descargado de un sitio web que almacena un paquete de información en el navegador del visitante. Se utilizan para almacenar datos recopilados, como información de inicio de sesión e identificación personal, comportamientos del sitio, preferencias y páginas visitadas. Aunque están orientadas a la comodidad, las cookies representan vulnerabilidades de seguridad. Los navegadores se pueden configurar para alertar sobre las cookies y los usuarios pueden aceptarlas o borrarlas.
Ataque cibernetico	Un evento que se lanza contra un objetivo con la intención de negar, interrumpir, destruir o explotar un entorno operativo habilitado para computadora. Muchos ataques cibernéticos tienen como objetivo comprometer con fines de explotación o destruir la integridad de los datos específicos, robar datos o manipularlos con fines nefastos. propósitos.
Ecosistema cibernético	La infraestructura de información interconectada de la empresa de una organización que facilita el intercambio, la comunicación y las interacciones de datos electrónicos entre usuarios, aplicaciones, sistemas, plataformas y procesos autorizados.
La seguridad cibernética	La capacidad de proteger o defenderse contra el acceso no autorizado o el uso del ciberespacio frente a ciberataques. Consiste en las medidas colectivas implementadas para defender una computadora o un sistema habilitado para computadora contra amenazas cibernéticas, como piratas informáticos, hacktivistas, servicios de inteligencia extranjeros y sindicatos del crimen organizado, entre otros.
La seguridad cibernética Arquitectura	La arquitectura de ciberseguridad, un elemento fundamental que respalda la arquitectura empresarial de una organización, consiste en la estructura y los comportamientos relacionados de tecnologías, procesos, sistemas, prácticas operativas y responsabilidades del personal centrados en la seguridad que se alinean con los objetivos definidos de la organización. Ver también: arquitectura empresarial y arquitectura de red.
La seguridad cibernética Evento	Un incidente visible que ocurre en un entorno habilitado para red o sistema informático relacionado con requisitos de ciberseguridad definidos. Un evento de ciberseguridad afecta la confidencialidad, integridad o disponibilidad de los datos. Ver también evento.
La seguridad cibernética Impacto	Las consecuencias resultantes de un evento de ciberseguridad, que también incluye el efecto sobre las capacidades y procesos de ciberseguridad actualmente implementados.
La seguridad cibernética Plan	Un documento que identifica y define los requisitos de ciberseguridad y los controles asociados necesarios para cumplir esos requisitos.

La seguridad cibernética Política	Un conjunto de principios, medidas y condiciones que se han definido para respaldar las capacidades y la planificación de la ciberseguridad en toda una organización.
La seguridad cibernética Programa	Un conjunto integrado de actividades coordinadas que incluyen gobernanza, planificación estratégica, patrocinio ejecutivo, informes y capacitación que se gestiona para cumplir con los objetivos de ciberseguridad definidos para una organización. Si bien los programas de ciberseguridad se pueden implementar a nivel divisional o de práctica, un nivel superior (empresarial) a menudo puede beneficiar a una organización al coordinar la planificación de inversiones y la asignación de recursos, alinear los procesos y procedimientos comerciales y otros recursos y capacidades, según sea necesario.
La seguridad cibernética Programa Estrategia	Un conjunto de acciones definidas adaptadas a las capacidades específicas de ciberseguridad de la organización y los objetivos de desempeño relacionados.
La seguridad cibernética Riesgo	El riesgo para la tecnología de la información y/o los activos y recursos basados en tecnología operativa de una organización, junto con sus funciones de soporte, procesos y reputación como resultado de acceso no autorizado, compromiso, explotación, interrupción, denegación o destrucción.
Filtración de datos (También “Datos Derramar")	El acceso no autorizado, la exfiltración o la divulgación de información confidencial y/o privilegiada a un tercero o entidad que no tiene autorización para acceder, ver o utilizar la información.
Negación de servicio Ataque (DoS)	Un tipo de ataque cibernético que resulta en la interrupción temporal o indefinida del acceso autorizado a una aplicación, sistema, plataforma u otro recurso. Por lo general, implica la sobrecarga de un sistema específico con una cantidad abrumadora de solicitudes innecesarias, lo que impide que se atiendan las solicitudes legítimas. Un ataque de denegación de servicio distribuido (DDoS) implica que el atacante emplee miles de direcciones IP únicas para llevar a cabo un ataque simultáneamente.
Riesgo de dependencia	El riesgo para una organización debido a un proveedor, vendedor, proveedor de servicios u otra parte externa del cual depende la prestación de un servicio crítico o función clave. Se evalúa y mide por la posibilidad y gravedad del daño que puede sufrir una aplicación, un sistema de tecnología de la información, un activo de tecnología operativa o una plataforma en caso de un compromiso.
Desaprovisionamiento	Es un proceso de gestión de riesgos que define la revocación o eliminación de la identidad de usuario de un individuo y los privilegios asociados que permiten el acceso autenticado a una instalación, aplicación, sistema o plataforma.
Digital Certificado	Una forma de credencial electrónica (por ejemplo, identificación virtual o pasaporte) que admite comunicaciones confiables y/o transacciones comerciales a través de Internet. Contiene el nombre de una persona, una identificación definida (por ejemplo, número de serie), fecha de vencimiento, una copia de la clave pública del titular del certificado (utilizada para cifrado y firmas digitales) y la firma digital de la autoridad emisora del certificado para verificar el certificado. .

Dominio Secuestro	Una forma de ciberataque que se produce cuando un atacante se hace cargo del registro de un dominio bloqueando el servidor de nombres de dominio (DNS) de la víctima y luego lo reemplaza ilegalmente por el suyo propio sin la autorización del registrante original.
Cifrado	Un método criptográfico utilizado para codificar un conjunto de información con el fin de protegerla del acceso o modificación no autorizados antes de enviarla a un destinatario específico. Luego, el destinatario decodifica el mensaje utilizando una clave de cifrado.
Empresa	El nivel organizativo más alto de una entidad definida.
Empresa Arquitectura	El plan organizacional, el diseño y la descripción de todo el entorno operativo de tecnología de la información y tecnología operativa de una organización. Identifica cómo se configuran, integran y conectan las aplicaciones, los sistemas y las plataformas a través de fronteras internas y externas. También identifica cómo se mantienen, cómo respaldan los objetivos de desempeño de la organización y cómo respaldan las capacidades de seguridad a nivel empresarial.
Evento	Un suceso observable en un activo, aplicación, sistema, red o plataforma. Los criterios de riesgo establecidos por la organización informan cómo algunos eventos se caracterizan y escalan para acciones de respuesta y mitigación.
Evento y Incidente Respuesta, continuidad de Operaciones	La organización y el mantenimiento de un conjunto integrado de planes, procedimientos y capacidades diseñados para respaldar la detección, el análisis y la respuesta a eventos de ciberseguridad. Además, están diseñados para brindar orientación para respaldar las operaciones continuas a través de un evento de ciberseguridad declarado de una manera que esté alineada y proporcional al riesgo para las capacidades y los objetivos generales de la organización.
Exfiltración	La eliminación, transferencia o reubicación no autorizada de información privilegiada de un sistema de información.
Cortafuegos	Un dispositivo de hardware o enlace de software en una red que está diseñado para inspeccionar paquetes de datos (por ejemplo, tráfico de datos) entre dispositivos, sistemas o redes. Se pueden configurar para restringir el tráfico de la red según reglas definidas.
Identidad	Un conjunto de características atribuibles u otros valores definidos (por ejemplo, un número de identificación de usuario generado aleatoriamente) que han sido asignados y pueden verificarse de manera que puedan distinguir a un individuo o entidad de otro.
Incidente	Un evento que surge de circunstancias deliberadas o accidentales, violando políticas y/o protocolos de seguridad establecidos que pueden tener consecuencias perjudiciales para activos, aplicaciones, sistemas, plataformas y/u otros elementos críticos de la infraestructura. Un incidente declarado debe justificar la activación de recursos de respuesta a incidentes para responder y contener su impacto en la organización, y limitar sus efectos en sistemas periféricos, plataformas, entornos operativos u otros activos dependientes. Véase también incidente y evento de seguridad informática .

Información Activos	Información o datos que la organización ha identificado y/o clasificado como esenciales para el funcionamiento de la misión. Esto también incluye datos operativos (por ejemplo, datos de proceso, información de comando y control), planes de seguridad, diagramas de red, diseños confidenciales, propiedad intelectual, información financiera y de clientes, y contratos.
Información Compartir y Comunicaciones	El intercambio de información implica el intercambio concienzudo de conocimientos, experiencia, datos e información sobre amenazas. Asume relaciones preexistentes entre terceros internos y externos de confianza (por ejemplo, asesores, socios, organismos encargados de hacer cumplir la ley, autoridades de control del Estado rector del puerto, etc.) con quienes compartir información de ciberseguridad, incluida cualquier información relevante sobre ciberseguridad actual o emergente. amenazas, actores de amenazas o vulnerabilidades específicas de la industria marítima, así como lecciones aprendidas y hallazgos similares.
Información Tecnología (TI)	Cualquier aplicación, activo, equipo, sistema, plataforma o sistema o subsistema interconectado que implique la creación, consumo, intercambio, difusión, procesamiento, gestión, protección y/o almacenamiento de información electrónica discreta. En el contexto de esta publicación, la definición incluye todos y cada uno de los sistemas interconectados y/o dependientes que respaldan entornos operativos en tierra y a bordo, y las tecnologías operativas que respaldan y/u operan.
Amenaza interna	Representa una amenaza maliciosa o involuntaria a la organización por parte de empleados, contratistas o proveedores de servicios que disfrutan de acceso privilegiado confiable a activos, aplicaciones, sistemas y/o plataformas controlados.
Integridad	En el contexto de la ciberseguridad, la integridad es la preservación de la autenticidad y corrección de la información. Implica la protección de la información contra alteración o destrucción inadecuada o no autenticada. La información puede presentarse en forma de archivos electrónicos, comandos, instrucciones y consultas.
protocolo de Internet (Dirección IP	La dirección IP de una computadora es una serie única de cuatro números de 8 bits, separados por puntos. Es la identificación asignada a todas las computadoras y dispositivos de red conectados a una red TCP/IP. En resumen, representa la dirección entre redes del dispositivo. Todos los sitios web también tienen una dirección IP. Las direcciones IP son administradas globalmente por la Autoridad de Números Asignados de Internet (IANA) y por cinco registros regionales de Internet.
Pulsación de tecla Inicio sesión	El registro de pulsaciones de teclas (también conocido como 'keylogging') es la grabación subrepticia de las pulsaciones de teclas del teclado de computadora que se capturan a medida que la víctima escribe. Las pulsaciones de teclas grabadas se transmiten automáticamente al atacante. Esta forma de ataque se puede lograr mediante software o hardware. Los atacantes suelen emplear el registro de teclas para capturar los nombres de usuario, contraseñas y otros datos personales de las víctimas, como la información de la tarjeta de crédito.
Privilegios mínimos	Un control establecido por una organización que permite sólo un nivel mínimo de acceso a los usuarios autorizados que lo requieren para realizar sus deberes y responsabilidades asignadas. El propósito del privilegio mínimo es mitigar los riesgos relacionados con el posible uso indebido y corrupción de privilegios autorizados relacionados con funciones, procesos y/o servicios específicos.

Inicio sesión	El mantenimiento de registros es un proceso manual o automatizado diseñado para monitorear y rastrear la actividad y el comportamiento de los usuarios. Como parte de un sistema de tecnología de la información o de tecnología operativa o un entorno de red, el registro es un proceso automatizado. Los procesos manuales incluyen la aplicación de procesos físicos (por ejemplo, inicio de sesión manual o uso de tarjetas inteligentes) empleados para controlar el acceso a entornos restringidos, como embarcaciones, instalaciones en tierra y entornos de oficina. La auditoría periódica de los registros (ya sea manualmente o mediante el uso de herramientas automatizadas) respalda un proceso crítico de gestión de riesgos cibernéticos que proporciona conciencia situacional a los profesionales de la seguridad.
malware	Término genérico para software que compromete el sistema operativo de un activo de red o de TI con diferentes tipos de código malicioso genérico o personalizado.
hombre-en-el-Ataque medio	Un tipo de ataque que involucra a un actor de amenazas que se hace pasar por un proveedor en línea o una institución financiera y alienta a la víctima a iniciar sesión utilizando sus credenciales a través de una conexión Secure Sockets Layer (SSL). Luego, el atacante utiliza las credenciales de la víctima para acceder al servidor válido con el fin de robar información específica (por ejemplo, propiedad intelectual, datos financieros, etc.)
Supervisión	El monitoreo implica la recopilación, agregación, registro, análisis y distribución de conjuntos de información específicos relacionados con la aplicación, el sistema y el comportamiento del usuario. Apoya un proceso continuo con respecto a la identificación y análisis de riesgos para los activos, aplicaciones, sistemas, plataformas, procesos y personal críticos de una organización.
Multifactor Autenticación	La aplicación requerida de dos o más factores que un usuario debe emplear para autenticarse en una aplicación, sistema o plataforma. Los factores aplicables pueden incluir: A) algo que usted sepa (por ejemplo, una contraseña única); B) algo que tenga (por ejemplo, un dispositivo de identificación); C) algo que usted es (por ejemplo, un elemento biométrico, como una huella digital); o D) usted está donde dice estar (por ejemplo, un token o dispositivo GPS).
Red	Dos o más sistemas informáticos o dispositivos en red conectados para compartir información, software y hardware.
Red arquitectura	Un marco que describe la estructura general de los activos, sistemas y plataformas de tecnología de la información y tecnología operativa (incluidos los sistemas integrados). Describe las reglas de comportamiento que respaldan las comunicaciones y la interconexión entre los activos de TI y/o OT. Véase también arquitectura empresarial y arquitectura de ciberseguridad.
Riesgo operacional	El impacto potencial en activos, aplicaciones, procesos y/o plataformas clave, incluidos sus servicios relacionados, que podría resultar de capacidades insuficientes o procesos, sistemas o tecnologías internos fallidos, o las acciones deliberadas o inadvertidas de personas, o eventos externos.
Operaciones Tecnología (TO)	Controles, sistemas o dispositivos programables que están diseñados para dirigir, monitorear o interactuar con sistemas que facilitan procesos físicos, como sistemas de control industrial, gestión de edificios, gestión de carga, seguridad, controles de motores, etc.

Contraseña	Un conjunto confidencial de caracteres alfanuméricos que se combina para usarse como medio de autenticación para confirmar la identidad de un usuario con el fin de acceder a una aplicación, sistema, plataforma o conjunto integrado de sistemas.
Parche	Una pequeña actualización de seguridad personalizada emitida por un proveedor de software para corregir errores conocidos en aplicaciones de software existentes. La mayoría de los programas de software y/o sistemas operativos se pueden configurar fácilmente para buscar automáticamente parches u otras actualizaciones.
Aprovisionamiento	La creación, mantenimiento y activación de un perfil de usuario, incluidos roles y privilegios de acceso. Una organización debe monitorear y rastrear continuamente los derechos de acceso para garantizar la seguridad de TI, OT y las comunicaciones. recursos.
Secuestro de datos	Malware informático que se instala en un sistema, cifra los datos del sistema, impide el acceso a estos datos y los mantiene como rehenes o amenaza con publicarlos hasta que se pague un rescate.
Riesgo	Una probabilidad o amenaza de una circunstancia negativa de un evento que explota una vulnerabilidad y que puede abordarse mediante una acción preventiva.
Riesgo residual	Exposición al riesgo después de que se consideren o apliquen controles para mitigar el riesgo.
Análisis de riesgo	La definición y comprensión de las posibles consecuencias para la organización si ciertos riesgos se materializaran y la determinación de los pasos apropiados para gestionar esos riesgos.
Evaluación de riesgos	Una identificación y evaluación de los riesgos potenciales que resultan de una determinada actividad y una determinación de un nivel aceptable de riesgo para la organización en cuestión.
Riesgo Gestión	La estimación y evaluación de riesgos potenciales y el establecimiento de acciones o procedimientos para aceptar, evitar, controlar, mitigar o transferir las consecuencias de dichos riesgos.
Riesgo Gestión Programa	Un plan definido para estimar y evaluar riesgos potenciales y establecer acciones o procedimientos para mitigar las consecuencias de esos riesgos.
Riesgo Gestión Estrategia	Un enfoque estructurado para estimar y evaluar riesgos potenciales y establecer acciones o procedimientos para mitigar las consecuencias de esos riesgos. Esto también incluye un procedimiento definido para revisar periódicamente el enfoque para incorporar nueva información.
Mitigación de riesgos	Acciones tomadas para reducir la ocurrencia y/o las consecuencias negativas de un riesgo.
Mitigación de riesgos Plan	Un conjunto definido y documentado de acciones a tomar para reducir la ocurrencia y/o las consecuencias negativas de un riesgo.

Registro de riesgo	Un repositorio estructurado de riesgos identificados, con información que respalda la gestión de riesgos, como la naturaleza del riesgo, las consecuencias del riesgo y la estrategia de mitigación del riesgo.
Respuesta a los riesgos	El proceso de desarrollar estrategias para reducir la ocurrencia y/o las consecuencias negativas de un riesgo. Estas estrategias pueden incluir aceptación, evitación, compartir o transferencia.
Enrutador	Un dispositivo de red conectado a dos o más líneas de datos en diferentes redes. que envía datos a la siguiente red apropiada. Esta función es similar a dirigir el tráfico de Internet.
Guion	Un archivo simple que contiene comandos programados que puede realizar una computadora sin la dirección del usuario.
Software seguro Desarrollo	El proceso de incluir las mejores prácticas de seguridad como parte integral del desarrollo de software, incluida la revisión de código, arquitecturas de seguridad y otros procesos y herramientas reconocidos. Los programadores y arquitectos de software con formación específica en desarrollo de software seguro suelen estar profundamente involucrados en este proceso.
Enchufe seguro Capa (SSL)	El sistema de cifrado estándar para proporcionar un enlace seguro para los datos intercambiados entre un sitio web y un usuario. Un sitio web cuya URL comienza con https está utilizando este sistema.
Nivel de servicio Acuerdo (SLA)	Un contrato entre un proveedor de servicios y un cliente, incluidos los servicios que el proveedor proporcionará y los estándares de desempeño que el cliente espera que cumplan estos servicios. Los estándares de desempeño deben incluir requisitos de ciberseguridad.
situacional Conciencia	La conciencia del estado actual de un sistema o entorno y la comprensión de cómo un cambio en una variable podría alterar ese estado actual. Esta conciencia surge de tener datos suficientes y precisos y de la capacidad de analizarlos adecuadamente para informar la toma de decisiones.
Social Ingeniería	La manipulación psicológica de las personas con el fin de engañar a una persona desprevenida para que eluda los controles de seguridad normales o proporcione acceso a las redes comerciales.
Social Redes Sitios web	Una plataforma en línea en la que los usuarios crean perfiles en línea y publican palabras escritas, imágenes, videos y otra información personal para compartir entre sí. Estas plataformas facilitan la conexión social entre usuarios con intereses similares.
Correo basura	El uso de mensajes masivos no solicitados y no deseados en un intento de convencer al destinatario de comprar algo o revelar información personal, como un número de teléfono, dirección o información de cuenta bancaria. El correo electrónico es el medio más típico de spam, pero el spam también se produce en otras áreas, como mensajes de texto, mensajes instantáneos y sitios web de redes sociales.

Patrocinio	El apoyo de la alta dirección a los objetivos de ciberseguridad en toda una organización a menudo se demuestra a través de declaraciones o políticas formales. El patrocinio total también implica la revisión, el seguimiento y la mejora continua de la alta dirección del programa de ciberseguridad de la organización.
suplantación de identidad	Un ataque mediante el cual un actor malintencionado intenta hacerse pasar por un actor de confianza para ocultar su verdadera identidad.
software espía	Software que se instala de forma encubierta en una computadora para permitir que un atacante robe datos y, posiblemente, información de identificación personal. Este software malicioso a menudo se combina con software que un usuario descarga voluntariamente y permanecerá en la computadora del usuario incluso si se elimina el programa descargado voluntariamente.
Cadena de suministro & Cadena de suministro Riesgo	Un conjunto secuencial de procesos, realizados por varios actores que de otro modo no estarían relacionados, que dan como resultado la creación, transporte y distribución de un producto. Por lo general, se entiende que la cadena de suministro abarca el diseño, desarrollo, producción, integración, distribución y eliminación de un producto. El riesgo de la cadena de suministro es la probabilidad o amenaza a la cadena de suministro de una circunstancia negativa de un evento causado por una vulnerabilidad y que puede abordarse mediante una acción preventiva.
Amenaza	Una acción o evento que puede, mediante la explotación de la vulnerabilidad de TI, OT o de la infraestructura de comunicaciones, causar que un riesgo se convierta en una pérdida o daño, con consecuencias negativas para las operaciones y recursos de una organización. Esto podría ocurrir, por ejemplo, mediante acceso no autorizado, denegación de servicio o suplantación de identidad.
Amenaza y Vulnerabilidad Gestión	Un enfoque estructurado para estimar y evaluar amenazas y vulnerabilidades y establecer acciones, planes o procedimientos para mitigar las consecuencias de esas amenazas y vulnerabilidades. Este enfoque debe incorporar las evaluaciones de riesgos y los planes de mitigación de riesgos de la organización.
Amenaza Evaluación	Una evaluación de amenazas potenciales, incluida su gravedad y sus posibles efectos en la infraestructura de comunicaciones, TI y OT de una organización.
Perfil de amenaza	La identificación de las características del conjunto completo de amenazas a una función determinada. Esto combina el conjunto de evaluaciones de amenazas de la organización para su infraestructura de comunicaciones, TI y OT.
Caballo de Troya	Software malicioso que engaña a las víctimas haciéndoles creer que es inofensivo. Generalmente propagados mediante algún tipo de ingeniería social, muchos caballos de Troya brindan acceso no autorizado a la computadora de la víctima, lo que permite el acceso a información personal, como información bancaria y contraseñas.
Río arriba Dependencias	Un actor externo que debe actuar o completar una tarea antes de que se pueda realizar o completar una función. Las dependencias upstream incluyen ciertos socios operativos, incluidos proveedores.
URL	Un método para indicar dónde se encuentra un recurso web específico en una red informática. También conocida como dirección web.

Virus	Un tipo de malware que se inserta e infecta otro programa informático y luego se reproduce e infecta otros programas. Debido a que un virus no puede ejecutarse por sí solo, requiere la ejecución de un programa anfitrión para poder activarse. Un virus puede propagarse a través de archivos adjuntos de correo electrónico, mensajes de texto, estafas en Internet e incluso descargas de aplicaciones móviles.
Vulnerabilidad	Una debilidad en un sistema de TI, OT o de comunicaciones que un atacante podría aprovechar para obtener acceso no autorizado a ese sistema y a la información que ese sistema almacena.
Gusano	Un tipo de malware que, a diferencia de un virus, puede ejecutarse de forma independiente, replicarse en otros hosts de una red y causar daños a una computadora y a la red, como por ejemplo, consumir como mínimo un ancho de banda significativo.